Deformaciones de grupos finitos

Manuel Jair Medina Luna
Matemático
cod. 830212

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C.
Febrero de 2010

Deformaciones de grupos finitos

Manuel Jair Medina Luna
Matemático
cod. 830212

Trabajo de Grado para optar al título de
Maestría en Ciencias Matemáticas

Director
César Neyit Galindo Martinez
Doctor en Matemáticas

Codirector
Ruth Stella Huérfano
Doctor en Matemáticas

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C.
Febrero de 2010

Título en español

Deformaciones de grupos finitos

Title in English

Deformations of finite groups

Resumen: Clasificamos las G-álgebras de Galois sobre k, donde G es un grupo finito y k es un cuerpo arbitrario. Aplicamos este resultado para clasificar los 2-cociclos de Hopf sobre el álgebra de funciones de G, los cuales a su vez caracterizan las deformaciones del grupo.

Abstract: We classify the G-Galois algebras over k, where G is finite group and k is an arbitrary field. We apply this result in the classification of Hopf 2-cocycles on the function algebra over G, which characterize the deformations of the group.

Palabras clave: Álgebra de Galois, Álgebra de grupo torcida, 2-cociclo de Hopf, Deformación de grupo finito, Grupo cuántico compacto.

Keywords: Galois Algebra, Twist group algebra, Hopf 2-cocycle, Deformation of finite group, Compact quantum group.

Nota de aceptación

Trabajo de tesis
Aprobado

Jurado
Gabriel Padilla

Director
César Neyit Galindo Martinez

Codirector
Ruth Stella Huerfano

Bogota, D.C., Febrero 10 de 2010

Dedicado

A mi familia.

A mi sol.

Agradecimientos

Quiero expresar mis agradecimientos a César Neyit Galindo Martínez gran amigo que me brindo su conocimiento de manera sincera y apasionada. Asimismo a la profesora Stella Huérfano gran maestra en el sentido apropiado de la palabra.

Índice general

Introducción

A partir de la introducción de los grupos cuánticos por Drinfeld y Jimbo en los 80, las álgebras de Hopf han sido intensamente estudiadas por matemáticos y físicos con diversos intereses y formaciones. Su estructura, que puede verse como una generalización de la estructura de grupo, se ha encontrado naturalmente ligada el estudio de las simetrías de distintos objetos matemáticos. Como ejemplos, se pueden mencionar los siguientes: en la física matemática, las álgebras de Hopf cuasi-triangulares aparecen como un instrumento adecuado para construir sistemáticamente soluciones de la Ecuación Cuántica de Yang-Baxter; en la topología, ligadas a la construcción de invariantes de nudos y 3-variedades; ciertas álgebras de Hopf semisimples aparecen como invariantes o "grupos de Galois" en el estudio de inclusiones de subfactores, a partir de ideas de Ocneanu. La literatura sobre los distintos aspectos de la teoría de los grupos cuánticos es bastante numerosa. Se citan, por ejemplo, los libros [CP95] y [Maj95]. Los libros [Kas95], [Tur94] y [BKJ01] están enfocados principalmente en el punto de vista topológico. Referencias básicas sobre las álgebras de Hopf son [Mon93], [DNR01].

La clasificación de álgebras de Hopf no conmutativas ni coconmutativas (especialmente las de dimensión finita), es un tema muy activo en la actualidad. Resultados importantes sobre clasificación se han obtenido principalmente en el caso de álgebras de Hopf semisimples y punteados, ver [Nat07a], [AS06]. Cabe aclarar que la mayoría de los resultados generales conocidos, son validos únicamente sobre cuerpos algebraicamente cerrados.

Un paso importante en todo esquema de clasificación, es la construcción de ejemplos no triviales que permitan encontrar invariantes, teoremas de estructura, etc. Para construir ejemplos no triviales de álgebras de Hopf, existen dos técnicas básicas: extensiones abelianas de álgebras de Hopf [Mas97] y deformaciones por 2-cociclos de Hopf (o en su forma dual deformaciones por twisting) [Doi93]. El teorema de clasificación de extensiones abelianas [Mas97, Proposition 5.2], es valido sobre cuerpos arbitrarios. En contraste, para los 2-cociclos de Hopf las condiciones sobre el cuerpo base son esenciales.

La teoría de deformaciones por 2-cociclos de Hopf, puede ser explicada en términos de extensiones de Hopf-Galois [Sch96]. Los resultados de Schauenburg *loc. cit.*, muestran que la clasificación de 2-cociclos de Hopf es equivalente a la clasificación de extensiones de Hopf-Galois del cuerpo base. El resultado principal de este trabajo de Maestría, es la clasificación de las extensiones de Hopf-Galois del cuerpo base para el álgebra de Hopf $(kG)^*$, donde G es un grupo finito y k es un cuerpo arbitrario, este tipo de extensiones de Hopf-Galois serán llamadas simplemente **G-álgebras de Galois sobre k**.

A continuación describimos brevemente el contenido del trabajo.

En los *Preliminares* presentamos algunas nociones, notaciones y resultados sobre cohomología de grupos, cohomología de Hochschild, álgebras simples y álgebras de grupo torcidas, fundamentales en el desarrollo de nuestro trabajo.

En el *Segundo Capítulo* presentamos la noción de álgebra de Galois y definimos el concepto de álgebra inducida. Como resultado principal de este capítulo, mostramos que toda G-álgebra de Galois se puede construir como la inducida de una S-álgebra de Galois simple, donde S es un subgrupo de G. Lo anterior reduce la clasificación a las álgebras de Galois simples.

En el *Tercer Capítulo* clasificamos las álgebras de Galois simples. Para ello definimos un dato asociado al grupo G y al cuerpo k, esto es, una colección (K, N, σ, γ) tal que

i) N es un subgrupo normal de G

ii) $K \supseteq k$ es una extensión de Galois con grupo de Galois G/N

iii) $\mathrm{char}(K) \nmid |N|$

iv) $\sigma : N \times N \to K^\times$ es un 2-cociclo no degenerado

v) $\gamma : G \to C^1(N, K^\times)$ es un 1-cociclo de Hochschild que representa la acción de G sobre $K_\sigma N$.

Mostramos que existe una correspondencia biyectiva entre G-álgebras de Galois sobre k (salvo isomorfismo) y datos asociados G y k (salvo cierta relación de equivalencia definida sobre el conjunto de datos).

En el *Cuarto Capítulo* presentamos la noción general de deformación y su relación con las extensiones de Hopf-Galois.

Por último en el *Quinto Capítulo* presentamos la noción de **grupo cuántico compacto** y mostramos que toda deformación de un grupo finito sobre el cuerpo de los números complejos posee estructura de grupo cuántico compacto.

Los siguiente resultados son aportes nuevos en la teoría:

- ◇ Presentación y demostración de una caracterización de álgebras de Galois alternativa a la dada en Davydov, Proposición 2.1.10.
- ◇ Secciones 2.2 y 2.3.
- ◇ Capítulo 3.
- ◇ Presentación y demostración de una caracterización de álgebras de Galois simples por medio de un dato, Teorema 3.2.19.

El presente trabajo pretende ser autocontenido, sin embargo algunas demostraciones de Teoremas clásicos serán omitidos. Las razones: lo extensas que estas pueden llegar a ser y la poca relevancia de los métodos de demostración para nuestros objetivos principales.

CAPÍTULO 1

Preliminares

El objetivo principal de este capítulo es establecer de manera sucinta, los conceptos y algunos resultados en álgebras, coálgebras, cohomología de grupos, cohomología de Hochschild, álgebras graduadas, G-álgebras, álgebras simples centrales y álgebras de grupo torcidas; que el lector debe tener presente para la lectura de este escrito. Asimismo fijaremos la notación que usaremos en el escrito.

A continuación presentamos por secciones, la conexión del contenido del capítulo y el resto del escrito.

- 1.1 Álgebra y coálgebra: Nociones fundamentales a lo largo del escrito.
- 1.2 Cohomología de grupos: Establecemos el concepto de 2-cociclo, noción fundamental en la construcción de productos cruzados (ver sección 3.1).
- 1.3 Cohomología de Hochschild: Noción que usaremos en la sección 3.2, como otra forma de escribir las condiciones de la función γ (ver Lema 3.2.7).
- 1.4 Álgebras graduadas: Noción que usaremos en el capítulo 3, para establecer que las álgebras de Galois simples son álgebras graduadas (ver Proposición 3.1.3).
- 1.4 G-álgebra: Noción fundamental a lo largo del escrito.
- 1.5 Álgebras simples centrales: Noción que usaremos en el capítulo 3. Estableceremos que las álgebras de Galois simples están determinadas por un dato (ver Teorema Principal 3.2.19).
- 1.6 Álgebras de grupo torcidas simples: Noción que usaremos en el capítulo 3. Estableceremos que las álgebras de Galois simples son álgebras de grupo torcidas (ver Proposición 3.1.5).

Como referencia para este capítulo están los libros [Lor08, GS06, Kas95, DNR01, Mon93, Wei94, DF04].

Denotamos por k un cuerpo arbitrario. A menos que indiquemos lo contrario, todos los espacios vectoriales, transformaciones lineales y productos tensoriales serán considerados sobre el cuerpo k.

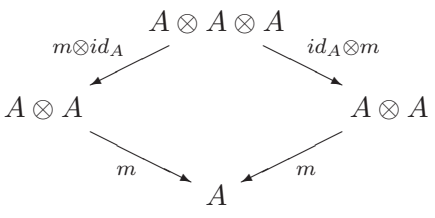
1.1. Álgebras y coálgebras

En esta sección introducimos de manera breve los conceptos de álgebras y coálgebras. Presentamos la notación de Sweedler para coálgebras y comódulos; convención que usaremos sistemáticamente en este trabajo, como una simplificación en la escritura.

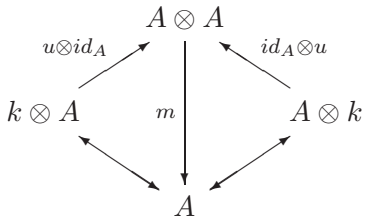
Como referencia para esta sección está el libro [Mon93].

1.1.1 Definición. Un **álgebra** sobre k es una tripla (A, m, u), donde A es un espacio vectorial, $m : A \otimes A \to A$ y $u : k \to A$ son transformaciones lineales tales que los siguientes diagramas son conmutativos:

a) Asociatividad:



b) Unidad:

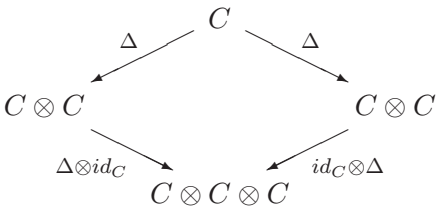


La transformación m es llamada la **multiplicación** en A. La transformación u determina un único elemento $1 = 1_A = u(1_k) \in A$ llamada la **unidad** del álgebra A.

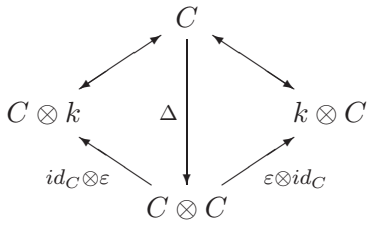
Ahora dualizamos la noción de álgebra.

1.1.2 Definición. Una **coálgebra** sobre k es una tripla (C, Δ, ε), donde C es un espacio vectorial, $\Delta : C \to C \otimes C$ y $\varepsilon : C \to k$ son transformaciones lineales tales que los siguientes diagramas son conmutativos:

a) Coasociatividad:



b) Counidad:



Las transformaciones Δ y ε son llamadas, respectivamente, la **comultiplicación** y la **counidad** de la coálgebra C.

La multiplicación en un álgebra transforma dos elementos en uno solo. Por otro lado, en una coálgebra la comultiplicación transforma un elemento en una "familia de pares de elementos". Por lo tanto los cálculos en una coálgebra resultan ser más engorrosos. Es por esto que para la comultiplicación tenemos la siguiente convención: llamada la **notación de Sweedler**.

1.1.3 Notación (Notación de Sweedler)**.** Sea (C, Δ, ε) una coálgebra. Para $c \in C$ el elemento $\Delta(c) = \sum_i c_{1i} \otimes c_{2i}$ será denotado por:

$$\Delta(c) = c_{(1)} \otimes c_{(2)}. \tag{1.1}$$

Usando (1.1) podemos expresar la coasociatividad de C de la forma

$$(c_{(1)})_{(1)} \otimes (c_{(1)})_{(2)} \otimes c_{(2)} = c_{(1)} \otimes (c_{(2)})_{(1)} \otimes (c_{(2)})_{(2)}. \tag{1.2}$$

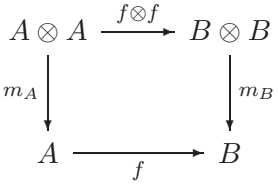
Por convención identificamos ambos lados de la igual (1.2) por

$$c_{(1)} \otimes c_{(2)} \otimes c_{(3)}.$$

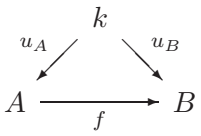
1.1.4 Definición. Consideremos las álgebras (A, m_A, u_A), (B, m_B, u_B) y las coálgebras $(C, \Delta_C, \varepsilon_C)$, $(D, \Delta_D, \varepsilon_D)$.

i) Una transformación lineal $f : A \to B$ es un **morfismo de álgebras** si los siguientes diagramas son conmutativos:

a)

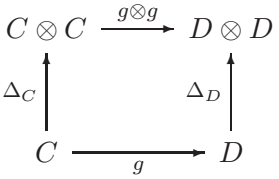


b)

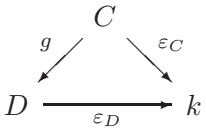


ii) Una transformación lineal $g : C \to D$ es un **morfismo de coálgebras** si los siguientes diagramas son conmutativos:

a)



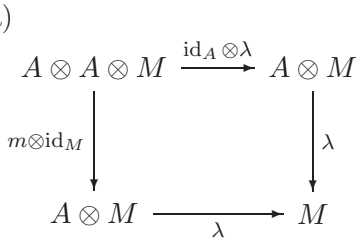
b)



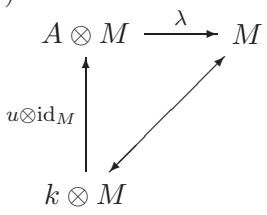
1.1.5 Definición. Sean (A, m, u) un álgebra y (C, Δ, ε) una coálgebra.

i) Un **A-módulo a izquierda** es un par (M, λ), donde M es un espacio vectorial y $\lambda : A \otimes M \to M$ es una transformación lineal tal que los siguientes diagramas son conmutativos:

a)



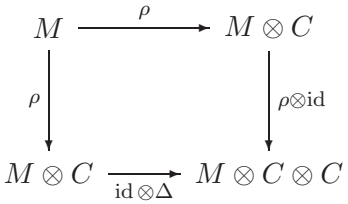
b)



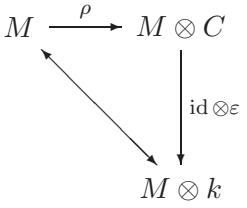
La transformación λ es llamada el **morfismo de estructura** del A-módulo M.

ii) Un **C-comódulo a derecha** es un par (M, ρ), donde M es un espacio vectorial y $\rho : M \to M \otimes C$ es una transformación lineal tal que los siguientes diagramas son conmutativos:

a)



b)



(1.3)

La transformación ρ es llamada el **morfismo de estructura** del C-comódulo M.

Usamos la notación de Sweedler para comódulos del siguiente modo: si M es un C-comódulo a derecha, entonces por convención escribimos

$$\rho(m) = m_{(0)} \otimes m_{(1)} \in M \otimes C \quad (m \in M) \tag{1.4}$$

Usando (1.4) podemos expresar la conmutatividad del diagrama a) en (1.3) por

$$(m_{(0)})_{(0)} \otimes (m_{(0)})_{(1)} \otimes m_{(1)} = m_{(0)} \otimes (m_{(1)})_{(1)} \otimes (m_{(1)})_{(2)}. \tag{1.5}$$

Por convención identificamos ambos lados de la igual (1.5) por

$$m_{(0)} \otimes m_{(1)} \otimes m_{(2)}.$$

1.2. Cohomología de Grupos

El objetivo principal de esta sección es presentar algunas ideas y conceptos básicos en cohomología de grupos, como son los G-módulos, n-cadenas, homomorfismos cofrontera, n-cociclos, n-cobordes y n-ésimos grupos de cohomología. En particular, trabajaremos de manera sistemática con los 2-cociclos de G (un grupo finito) a valores en un G-módulo A. Usaremos los 2-cociclos para construir álgebras de grupo torcida (ver Sección 1.4) y asociar un álgebra de Galois a un dato (ver Teorema Principal 3.2.19).

Como referencia para esta sección está el libro [DF04, Section 17.2].

1.2.1 Definición. Sean G un grupo con unidad e y A un grupo abeliano (escrito aditivamente) con unidad 0.

i) Una **acción a izquierda** de G sobre A, es un homomorfismo de G en el grupo de automorfismos de grupos de A. Equivalentemente, decimos que G **actúa a izquierda** sobre A si existe una función $G \times A \to A$ dada por $(g, a) \mapsto g \rightharpoonup a$, tal que cumple las siguientes condiciones:

- $e \rightharpoonup a = a; \quad a \in A.$
- $(gh) \rightharpoonup a = g \rightharpoonup (h \rightharpoonup a); \quad g, h \in G$ y $a \in A.$
- $g \rightharpoonup (a + b) = (g \rightharpoonup a) + (g \rightharpoonup b); \quad g \in G$ y $a, b \in A.$

ii) Una **acción a derecha** de G sobre A, es un homomorfismo de G^{op} ($G^{op} = G$ como conjuntos, y el producto esta dado por $x \cdot_{op} y = yx$, para $x, y \in G$) en el grupo de automorfismos de grupos de A. Equivalentemente, decimos que G **actúa a derecha** sobre A si existe una función $A \times G \to A$ dada por $(a, g) \mapsto a \leftharpoonup g$, tal que cumple las siguientes condiciones:

- $a \leftharpoonup e = a; \quad a \in A.$
- $a \leftharpoonup (gh) = (a \leftharpoonup g) \leftharpoonup h; \quad g, h \in G$ y $a \in A.$
- $(a + b) \leftharpoonup g = (a \leftharpoonup g) + (b \leftharpoonup g); \quad g \in G$ y $a, b \in A.$

1.2.2 Definición. Sea G un grupo. El grupo abeliano A es un **G-módulo a izquierda**, si G actúa a izquierda sobre A. Análogamente, el grupo abeliano A es un **G-módulo a derecha**, si G actúa a derecha sobre A. Decimos que A es un **G-bimódulo** si G actúa a derecha e izquierda de A y las acciones a derecha e izquierda son **compatibles**, esto es,

$$(x \rightharpoonup a) \leftharpoonup y = x \rightharpoonup (a \leftharpoonup y) \qquad (\forall x, y \in G \text{ y } a \in A).$$

1.2.3 Ejemplo.

i) G actúa **trivialmente** sobre A, si $g \rightharpoonup a = a$ para cada $a \in A$ y $g \in G$.

ii) La función

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{C} &\to \mathbb{C} \\ (0, a+ib) &\mapsto a+ib \\ (1, a+ib) &\mapsto a-ib, \end{aligned}$$

es una acción del grupo aditivo de los enteros módulo 2 al grupo aditivo de los números complejos.

1.2.4 Definición. Dada A un G-módulo a izquierda, el conjunto

$$A^G = \{a \in A | g \rightharpoonup a = a \ \ \forall g \in G\}$$

es el subgrupo de A de los elementos que quedan fijos bajos todos los elementos de G. Llamamos a este subgrupo el **grupo de invariantes de** A, si no hay lugar a confusión sobre el grupo G que actúa sobre A.

1.2.5 Ejemplo.

i) Si G actúa trivialmente sobre A, entonces $A^G = A$.

ii) Sea K una extensión de Galois de k con grupo de Galois $G = \mathrm{Gal}(K/k)$. Para $f \in G$ y $\alpha \in K$, la acción $f \cdot \alpha = f(\alpha)$ le da al grupo aditivo de K una estructura de G-módulo a izquierda, con $K^G = k$.

Dados dos G-módulos a izquierda $(A, \rightharpoonup)$ y $(A', \cdot)$. Un homomorfismo de grupos abelianos $\psi : A \to A'$ es un **homomorfismo de G-módulos** si

$$\psi(g \rightharpoonup a) = g \cdot \psi(a) \quad \forall g \in G, a \in A.$$

1.2.6 Definición. Para A un G-módulo a izquierda, sean $C^0(G, A) = A$ y, para $n \geq 1$, $C^n(G, A)$ la colección de todas las funciones de $G^n = G \times \cdots \times G$ (n veces) a A. Los elementos de $C^n(G, A)$ son llamados **n-cadenas (de G a valores en A)**.

Cada $C^n(G, A)$ es un grupo abeliano: para $C^0(G, A) = A$ dada por la estructura de grupo de A; para $n \geq 1$ dada por la suma puntual de funciones:

$$(f_1 + f_2)(g_1, g_2, \ldots, g_n) = f_1(g_1, g_2, \ldots, g_n) + f_2(g_1, g_2, \ldots, g_n).$$

1.2.7 Definición. Para $n \geq 0$, el n**-ésimo homomorfismo cofrontera** de $C^n(G,A)$ a $C^{n+1}(G,A)$ es la función determinada por la ecuación:

$$\begin{aligned} d_n(f)(x_1, x_2, \ldots, x_{n+1}) &= x_1 \rightharpoonup f(x_2, \ldots, x_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, x_{i+2}, \ldots, x_{n+1}) \\ &\quad + (-1)^{n+1} f(x_1, \ldots, x_n), \end{aligned}$$

donde el producto $x_i x_{i+1}$ ocupa la posición i en los valores que toma la función f.

Es inmediato de la definición que d_n es un homomorfismo de grupos y $d_n(d_{n-1}) = 0$ para todo $n \geq 1$.
Tenemos entonces una sucesión ascendente de grupos abelianos

$$0 \to C^0(G,A) \overset{d_0}{\to} \cdots \overset{d_{n-1}}{\to} C^n(G,A) \overset{d_n}{\to} C^{n+1}(G,A) \overset{d_{n+1}}{\to} \cdots$$

1.2.8 Definición. Para A un G-modulo a izquierda.

i) Sea $Z^n(G,A) = \ker d_n$ para $n \geq 0$. Los elementos de $Z^n(G,A)$ son llamados n**-cociclos**.

ii) Sea $B^n(G,A) = \text{Im } d_{n-1}$ para $n \geq 1$ y sea $B^0(G,A) = 0$. Los elementos de $B^n(G,A)$ son llamados n**-cobordes**.

1.2.9 Definición. Sea $f \in Z^n(G,A)$ un n-cociclo. Si $x_i = e$ para algún $1 \leq i \leq n$ implica que $f(x_1, \ldots, x_{i-1}, e, x_{i+1}, \ldots, x_n) = 0$, decimos que f es un n**-cociclo normalizado**.

Dado que $d_n(d_{n-1}) = 0$, para $n \geq 1$, entonces Im $d_{n-1} \subseteq \ker d_n$. Es decir, $B^n(G,A)$ es un subgrupo de $Z^n(G,A)$.

1.2.10 Definición. Dado un G-módulo a izquierda A, el grupo cociente $Z^n(G,A)/B^n(G,A)$ lo llamamos el n**-ésimo grupo de cohomología de** G **con coeficientes en** A y lo denotamos por $H^n(G,A)$, $n \geq 0$.

1.2.11 Ejemplo.

i) Sean G un grupo y A un G-módulo a izquierda. De acuerdo a la definición 1.2.7, para $f = a \in A = C^0(G,A)$ tenemos que

$$d_0(f)(x) = x \rightharpoonup a - a,$$

entonces $\ker d_0$ es el conjunto $\{a \in A | x \rightharpoonup a = a \ \ \forall x \in G\}$, es decir, $Z^0(G,A)$ coincide con el grupo de invariantes A^G. Por lo tanto

$$H^0(G,A) = Z^0(G,A)/B^0(G,A) = A^G/0 = A^G.$$

Para $f \in C^1(G,A)$ tenemos que

$$d_1(f)(x,y) = x \rightharpoonup f(y) - f(xy) + f(x),$$

entonces un 1-cociclo es una función $f : G \to A$ que satisface la **condición de 1-cociclo**:

$$f(xy) = x \rightharpoonup f(y) + f(x).$$

Para $f \in C^2(G, A)$ tenemos que

$$d_2(f)(x, y, z) = x \rightharpoonup f(y, z) - f(xy, z) + f(x, yz) - f(x, y),$$

entonces un 2-cociclo es una función $f : G \times G \to A$ que satisface la **condición de 2-cociclo**:

$$f(x, y) + f(xy, z) = x \rightharpoonup f(y, z) + f(x, yz).$$

ii) Supongamos que $G = \{e\}$ es el grupo trivial. El grupo $G^n = \{(e, \dots, e)\}$ es también el grupo trivial, entonces $f \in C^n(G, A)$ está completamente determinado por su valor en $(e, \dots, e)$, digamos $f(e, \dots, e) = a \in A$. Identificamos a f con a y obtenemos que $C^n(G, A) = A$ para todo $n \geq 0$. Entonces, si $f = a \in A$,

$$d_n(f)(e, \dots, e) = a + \sum_{i=1}^{n} (-1)^i a + (-1)^{n+1} a = \begin{cases} 0 & \text{si } n \text{ es par,} \\ a & \text{si } n \text{ es impar.} \end{cases}$$

Entonces $d_n = 0$ si n es par y $d_n = 1$ es la identidad si n es impar. Por lo tanto

$$H^0(1, A) = A^G = A,$$
$$H^n(1, A) = 0 \ \text{ para todo } n \geq 1.$$

La siguiente proposición la usaremos en la sección 3.2 para simplificar los cálculos. La demostración de la misma será omitida, pues son necesarios algunos conceptos y resultados de cohomología algebraica. Resultados que escapan a los objetivos de estos preliminares.

1.2.12 Proposición. *Sea A un G-módulo a izquierda tal que G actúa trivialmente sobre A. Entonces todo 2-cociclo es cohomólogo a un 2-cociclo $f \in Z^2(G, A)$ tal que*

$$f(x, y) = -f(y^{-1}, x^{-1}) \quad \forall x, y \in G. \tag{1.6}$$

Demostración. Ver [Yam02, Remark, pag 88]. □

1.2.13 Nota. En particular, si $A = k^\times$ son los elementos no nulos del cuerpo k y G actúa de trivialmente sobre A, entonces todo 2-cociclo es cohomólogo a un 2-cociclo $\sigma \in Z^2(G, k^\times)$ tal que

$$\sigma(x, x^{-1}) = \pm 1 \quad (\forall x \in G). \tag{1.7}$$

En el caso de la observación anterior, consideremos la función

$$\begin{aligned} \epsilon_\sigma : G &\to \{1, -1\} \\ x &\mapsto \sigma(x, x^{-1}). \end{aligned}$$

1.2.14 Lema. *Sean G un grupo que actúa trivialmente sobre $k^\times$ y $\sigma \in Z^2(G, k^\times)$ un 2-cociclo que satisface la condición* (1.7)*. Entonces la función ϵ_σ es un homomorfismo de grupos. Llamamos al homomorfismo ϵ_σ el **signo** del 2-cociclo σ.*

Demostración. Es evidente que $\epsilon_\sigma(x) = \epsilon_\sigma(x^{-1}) = \epsilon_\sigma(x)^{-1}$, para todo $x \in G$. Para $x, y \in G$, la ecuación

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

muestra que

$$\begin{aligned}\epsilon_\sigma(xy)\epsilon_\sigma(x) &= \sigma(y^{-1}, x^{-1})\sigma(y, y^{-1}x^{-1}) \\ &= \sigma(y, y^{-1})\sigma(e, x^{-1}) \\ &= \epsilon_\sigma(y).\end{aligned}$$

Entonces ϵ_σ es un homomorfismo como se quería demostrar. □

1.3. Cohomología de Hochschild

El objetivo principal de esta sección es presentar ideas y conceptos básicos en cohomología de Hochschild, como son los, homomorfismos cofrontera de Hochschild, n-cociclos de Hochschild, n-cobordes de Hochschild y n-ésimos grupos de cohomología de Hochschild. Usaremos esta noción en la sección 3.2, como otra forma de escribir las condiciones de la función γ (ver Lema 3.2.7) y asociar G-álgebras de Galois simples a datos (K, N, σ, γ), donde K es un cuerpo, N es un subgrupo de G, σ es un 2-cociclo no degenerado y $\gamma : G \to C^1(N, K^\times)$ es un 1-cociclo de Hochschild.

Como referencia para esta sección está el libro [Wei94].

Sean G un grupo y A un G-bimódulo. Como en la sección anterior consideremos el grupo abeliano de la n-cadenas de G a valores en A, $C^n(G, A)$.

1.3.1 Definición. Para $n \geq 0$, el **n-ésimo homomorfismo cofrontera de Hochschild de $C^n(G, A)$ a $C^{n+1}(G, A)$** es la función determinada por la ecuación:

$$\begin{aligned}\hat{d}_n(f)(x_1, x_2, \ldots, x_{n+1}) &= x_1 \rightharpoonup f(x_2, \ldots, x_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_{i-1}, x_i x_{i+1}, x_{i+2}, \ldots, x_{n+1}) \\ &\quad + (-1)^{n+1} f(x_1, \ldots, x_n) \leftharpoonup x_{n+1},\end{aligned}$$

donde el producto $x_i x_{i+1}$ ocupa la posición i en los valores que toma la función f.

De la definición tenemos que $\hat{d}_n$ es un homomorfismo de grupos y $\hat{d}_n(\hat{d}_{n-1}) = 0$ para todo $n \geq 1$.
Tenemos entonces una sucesión ascendente de grupos abelianos

$$0 \to C^0(G, A) \overset{\hat{d}_0}{\to} \cdots \overset{\hat{d}_{n-1}}{\to} C^n(G, A) \overset{\hat{d}_n}{\to} C^{n+1}(G, A) \overset{\hat{d}_{n+1}}{\to} \cdots$$

1.3.2 Definición.

i) Sea $Z^n_H(G, A) = \ker \hat{d}_n$ para $n \geq 0$. Los elementos de $Z^n_H(G, A)$ son llamados **n-cociclos de Hochschild**.

ii) Sea $B^n_H(G, A) = \operatorname{Im} \hat{d}_{n-1}$ para $n \geq 1$ y sea $B^0_H(G, A) = 0$. Los elementos de $B^n_H(G, A)$ son llamados **n-cobordes de Hochschild**.

1.3.3 Definición. Sea $f \in Z_H^n(G,A)$ un n-cociclo de Hochschild. Si $x_i = e$ para algún $1 \leq i \leq n$ implica que $f(x_1,\ldots,x_{i-1},e,x_{i+1},\ldots,x_n) = 0$, decimos que f es un **n-cociclo normalizado de Hochschild**.

Dado que $\hat{d}_n(\hat{d}_{n-1}) = 0$ para $n \geq 1$, entonces Im $\hat{d}_{n-1} \subseteq \ker \hat{d}_n$. Es decir, $B_H^n(G,A)$ es un subgrupo de $Z_H^n(G,A)$.

1.3.4 Definición. Sea A un G-bimódulo. El grupo cociente $Z_H^n(G,A)/B_H^n(G,A)$ lo llamamos el **n-ésimo grupo de la cohomología de Hochschild de G con coeficientes en** A y lo denotamos por $H_H^n(G,A)$, $n \geq 0$.

1.3.5 Ejemplo.

i) Sean G un grupo y A un G-bimódulo. Para $f = a \in A = C^0(G,A)$ tenemos que

$$\hat{d}_0(f)(x) = x \rightharpoonup a - a \leftharpoonup x,$$

entonces $\ker \hat{d}_0$ es el conjunto $A^G = \{a \in A | x \rightharpoonup a = a \leftharpoonup x \ \ \forall x \in G\}$, es decir, $Z_H^0(G,A) = A^G$ y por lo tanto

$$H_H^0(G,A) = A^G.$$

Para $f \in C^1(G,A)$ tenemos que

$$\hat{d}_1(f)(x,y) = x \rightharpoonup f(y) - f(xy) + f(x) \leftharpoonup y,$$

entonces un 1-cociclo de Hochschild es una función $f : G \to A$ que satisface la **condición de 1-cociclo de Hochschild**:

$$f(xy) = x \rightharpoonup f(y) + f(x) \leftharpoonup y.$$

Para $f \in C^2(G,A)$ tenemos que

$$\hat{d}_2(f)(x,y,z) = x \rightharpoonup f(y,z) - f(xy,z) + f(x,yz) - f(x,y) \leftharpoonup z,$$

entonces un 2-cociclo de Hochschild es una función $f : G \times G \to A$ que satisface la **condición de 2-cociclo de Hochschild**:

$$f(x,y) \leftharpoonup z + f(xy,z) = x \rightharpoonup f(y,z) + f(x,yz).$$

ii) Supongamos que $G = \{e\}$ es el grupo trivial. Como en el Ejemplo 1.2.11 tenemos que $\hat{d}_n = 0$ si n es par y $\hat{d}_n = 1$ es la identidad si n es impar. Por lo tanto

$$H_H^0(1,A) = A^G = A,$$
$$H_H^n(1,A) = 0 \ \text{ para todo } n \geq 1.$$

1.4. Álgebras graduadas y G-álgebras

En esta sección presentamos algunas ideas y conceptos básicos en álgebras graduadas y productos cruzados, esto es, álgebras de graduadas en la que cada componente homogénea contiene un elemento invertible. Mostramos que los productos cruzados están en correspondencia biunívoca con los sistemas (A, G, π, σ), donde A es un álgebra, G es un grupo, π es una acción débil y σ es un 2-cociclo. Usaremos este resultado para mostrar que las álgebras de Galois son álgebras de grupo torcidas (ver Sección 3.1).

Como referencia de la sección están, entre otros, el libro [NO04] y las notas [Mas97].

Denotamos por G un grupo con unidad e y por A un álgebra sobre k.

1.4.1 Definición. Decimos que

i) A es un **álgebra graduada** de tipo G o A está **graduada** por G, si existe una descomposición $A = \bigoplus_{g\in G} A_g$ como espacio vectorial, tal que $A_g A_h \subseteq A_{gh}$ para cualesquiera $g, h \in G$.

ii) Un álgebra graduada de tipo G es **fuertemente graduada** si $A_g A_h = A_{gh}$ para cualesquiera $g, h \in G$.

iii) Para A y B álgebras graduadas del tipo G. Un morfismo de álgebras $f : A \to B$, es un **morfismo de álgebras graduadas** si $f(A_g) \subseteq B_g$ para todo $g \in G$.

Usamos la simplificación **álgebra graduada** para un álgebra graduada por G, cuando no haya lugar a confusión sobre el grupo G en el cual llevamos la graduación. El subespacio A_g de la definición es llamada la **g-ésima componente homogénea** del álgebra graduada A.

1.4.2 Nota. Un álgebra graduada está fuertemente graduada si y sólo si para cualquier g en G, tenemos que $A_g A_{g^{-1}} = A_e$. En efecto, si $A_g A_{g^{-1}} = A_e$, entonces para cualesquiera $g, h \in G$

$$A_{gh} \subseteq A_{gh}A_e = A_{gh}A_{h^{-1}}A_h \subseteq A_g A_h,$$

luego $A_{gh} = A_g A_h$.

Un ejemplo importante de álgebras graduadas son los productos cruzados.

1.4.3 Definición. Sea A un álgebra graduada por G. A es un **G-producto cruzado**, si para cada g en G la g-ésima componente homogénea de A contiene un elemento invertible u_g.

Usamos la simplificación **producto cruzado** para un G-producto cruzado, cuando no haya lugar a confusión sobre el grupo G.

1.4.4 Nota. Si A es un producto cruzado, entonces A está fuertemente graduada. En efecto, si u_g es un elemento invertible en la g-ésima componente homogénea de A, entonces $A_e = (A_e u_g^{-1})u_g \subseteq A_{g^{-1}} A_g$.

1.4.5 Definición. Una **acción** a izquierda del grupo G sobre el álgebra A, es un homomorfismo del grupo G al grupo $\mathrm{Aut}(A)$ de automorfismos de álgebras de A. Equivalentemente, decimos que la función

$$\begin{aligned} G \times A &\to A \\ (g, a) &\mapsto g \rightharpoonup a \end{aligned}$$

es una **acción** a izquierda de G sobre A si para cualesquiera $a, b \in A$ y $g, h \in G$ tenemos que:

i) La función

$$\begin{aligned} A &\to A \\ a &\mapsto g \rightharpoonup a, \end{aligned}$$

es una transformación lineal para cada $g \in G$.

ii) $e \rightharpoonup a = a$,

iii) $(gh) \rightharpoonup a = g \rightharpoonup (h \rightharpoonup a)$,

iv) $g \rightharpoonup (ab) = (g \rightharpoonup a)(g \rightharpoonup b)$,

v) $g \rightharpoonup 1 = 1$.

Un álgebra A sobre la cual G actúa es llamada una **G-álgebra**. Un morfismo de álgebras $f : A \to B$, entre las G-álgebras A y B, es un **morfismo de G-álgebras** si

$$f(g \rightharpoonup a) = g \rightharpoonup f(a) \quad \text{para todo } g \in G \text{ y } a \in A.$$

A continuación presentamos una caracterización de los productos cruzados por medio de una "acción débil" y un "2-cociclo".

1.4.6 Definición. Llamamos a (A, G, π, σ) un **sistema cruzado** si A es un álgebra, G es un grupo, $\pi : G \to \mathrm{Aut}(A)$ y $\sigma : G \times G \to A^\times$ son, respectivamente, una función de G al grupo de los automorfismos del álgebra A y una función de $G \times G$ al grupo $A^\times$ de las unidades de A, tales que para cualesquiera $x, y, z \in G$ y $a \in A$ satisfacen las siguientes condiciones:

i) $(a^y)^x = \sigma(x, y) a^{xy} \sigma(x, y)^{-1}$,

ii) $\sigma(y, z)^x \sigma(x, yz) = \sigma(x, y)\sigma(xy, z)$,

iii) $\sigma(x, e) = \sigma(e, x) = 1$,

donde hemos denotado a $\pi(x)(a) = a^x$. La función π es llamada una **acción débil** de G sobre A y la función σ es llamado un 2-**cociclo**[1].

[1] Si el grupo $A^\times$ es abeliano, entonces las dos nociones de 2-cociclo (Definiciones 1.2.8 y 1.4.6) coinciden.

1.4.7 Nota. Si σ es trivial, entonces por la condición $i)$ para $x = y = e$ la ecuación

$$(a^e)^e = a^e, \qquad (a \in A)$$

implica que $\pi(e) \circ \pi(e) = \pi(e)$, entonces $\pi(e) = \mathrm{id}_A$, es decir, π es un homomorfismos de grupos o π es una acción de G sobre A, y denotamos a a^g por $g \rightharpoonup a$. Las condiciones $iii)$ y $iv)$ en la definición anterior son llamadas la **ecuación de cociclo** y la **condición de normalidad**, respectivamente. Denotamos como es usual por $Z^2(G, A^\times)$ al conjunto de los 2-cociclos de G en $A^\times$.

Ahora cada sistema cruzado determina un álgebra como se muestra a continuación.

Sea (A, G, π, σ) un sistema cruzado. Consideremos el espacio vectorial $\bigoplus_{g\in G} Au_g$ de las k-combinaciones lineales au_g, que satisfacen las relaciones

$$(a + b)u_g = au_g + bu_g,$$
$$\alpha(au_g) = (\alpha a)u_g,$$

para cualesquiera $a, b \in A$, $g \in G$ y $\alpha \in k$. La ecuación

$$(au_g)(bu_h) = ab^g\sigma(g, h)u_{gh} \tag{1.8}$$

provee a este espacio de un producto con unidad u_e. Denotamos por $A\#_\sigma G$ a este espacio vectorial con producto dado en (1.8).

1.4.8 Proposición. *$A\#_\sigma G$ es un álgebra.*

Demostración. Sean $a, b, c \in A$ y $x, y, z \in G$, la sucesión de igualdades

$$\begin{aligned}
&(au_x)[(bu_y)(cu_z)]\\
&= (au_x)[bc^y\sigma(y, z)u_{yz}]\\
&= a(bc^y\sigma(y, z))^x\sigma(x, yz)u_{xyz}\\
&= ab^x(c^y)^x\sigma(y, z)^x\sigma(x, yz)u_{xyz}\\
&= ab^x(c^y)^x\sigma(x, y)\sigma(xy, z)u_{xyz} && \text{(ecuación de cociclo)}\\
&= ab^x\sigma(x, y)c^{yx}\sigma(xy, z)u_{xyz} && \text{(por } ii \text{ en 1.4.6)}\\
&= (ab^x\sigma(x, y)u_{xy})cu_z\\
&= [(au_x)(bu_y)]cu_z
\end{aligned}$$

demuestran la asociatividad del producto dado en (1.8). □

1.4.9 Proposición. *A es un G-producto cruzado si y sólo si existe un sistema cruzado $(\hat{A}, G, \pi, \sigma)$ tal que*

$$A \simeq \hat{A}\#_\sigma G,$$

como álgebras.

Demostración. Sea $(\hat{A}, G, \pi, \sigma)$ un sistema cruzado. Veamos que $\hat{A}\#_\sigma G$ es un G-producto cruzado. Es evidente que para cada g en G, las g-ésimas componentes homogéneas $A_g =$

Au_g de $A\#_\sigma G$ cumplen la propiedad $A_gA_h = A_{gh}$, y cada componente Au_g contiene un elemento invertible u_g, con inverso

$$(u_g)^{-1} = (\sigma(g^{-1}, g))^{-1}u_{g^{-1}}.$$

En efecto, por la condición de cociclo tenemos que

$$\sigma(g^{-1}, g)^g\sigma(g, e) = \sigma(g, g^{-1})\sigma(e, g),$$

esto es,

$$\sigma(g^{-1}, g)^g = \sigma(g, g^{-1}).$$

Entonces

$$\begin{aligned} u_g(\sigma(g^{-1}, g))^{-1}u_{g^{-1}} &= (\sigma(g^{-1}, g)^g)^{-1}\sigma(g, g^{-1})u_e \\ &= (\sigma(g^{-1}, g)^g)^{-1}\sigma(g, g^{-1})u_e \\ &= u_e. \end{aligned}$$

Análogamente obtenemos $(\sigma(g^{-1}, g))^{-1}u_{g^{-1}}u_g = u_e$.

Recíprocamente, sea $A = \bigoplus_{g\in G} A_g$ un álgebra graduada que posee un elemento invertible u_g en cada componente A_g. La componente A_e es naturalmente un álgebra. Consideremos las funciones $\pi : G \to \mathrm{Aut}(A_e)$ y $\sigma : G \times G \to A_e^\times$, definidas, respectivamente, por

$$\begin{aligned} \pi(x)(\hat{a}) &= \hat{a}^x = u_x\hat{a}u_x^{-1}, \\ \sigma(x, y) &= u_xu_yu_{xy}^{-1}. \end{aligned}$$

Veamos que (A_e, G, π, σ) es un sistema cruzado: sean $x, y, z \in G$ y $\hat{a} \in A_e$, entonces la sucesión de igualdades

$$\begin{aligned} (\hat{a}^y)^x &= u_x(u_y\hat{a}u_y^{-1})u_x^{-1} \\ &= \sigma(x, y)u_{xy}\hat{a}u_{xy}^{-1}\sigma(x, y)^{-1} \\ &= \sigma(x, y)\hat{a}^{xy}\sigma(x, y)^{-1} \end{aligned}$$

muestran que π es una acción débil de G sobre A_e. Del mismo modo la sucesión de igualdades

$$\begin{aligned} \sigma(y, z)^x\sigma(x, yz) &= u_xu_yu_zu_{xyz}^{-1} \\ &= u_xu_yu_{xy}^{-1}u_{xy}u_zu_{xyz}^{-1} \\ &= \sigma(x, y)\sigma(xy, z) \end{aligned}$$

muestran que σ es un 2-cociclo. Ahora

$$A_g = (A_gu_g^{-1})u_g \subseteq A_eu_g \subseteq A_g,$$

entonces $A_g = A_eu_g$ y así $A = \bigoplus_{g\in G} A_eu_g$. Por último para $\hat{a}, \hat{b} \in A_e$ y $x, y \in G$ tenemos que

$$(\hat{a}u_x)(\hat{b}u_y) = \hat{a}(u_x\hat{b}u_x^{-1})(u_xu_yu_{xy}^{-1})u_{xy} = \hat{a}\hat{b}^x\sigma(x, y)u_{xy},$$

por lo tanto A es isomorfa al álgebra $A_e\#_\sigma G$. □

1.4.10 Nota. Si A es un álgebra conmutativa, la acción débil $\pi : G \to \mathrm{Aut}(A)$ es en realidad una acción de G sobre A.

Nos interesa ahora saber cuando dos sistemas cruzados (A, G, π, σ) y (A, G, π, σ') generan en esencia un mismo producto cruzado. Para esto tenemos la siguiente definición tomada de [Mas97].

1.4.11 Definición. Sean G un grupo y A una G-álgebra conmutativa. Decimos que los G-productos cruzados $A\#_\sigma G$ y $A\#_{\sigma'}G$ son **equivalentes** si existe un isomorfismo $f : A\#_\sigma G \to A\#_{\sigma'}G$ de G-álgebras graduadas que preserva cada elemento en A, esto es, si el siguiente diagrama

$$\begin{array}{ccc} A & \longleftrightarrow & A \\ \downarrow & & \downarrow \\ A\#_\sigma G & \xrightarrow[f]{} & A\#_{\sigma'}G \end{array} \tag{1.9}$$

conmuta. Denotamos por $\mathcal{E}(A, G, \pi)$ al conjunto de las clases de equivalencia de G-productos cruzados sobre A con acción π.

La siguiente proposición es un ejercicio propuesto en [Mas97, Proposition 1.9].

1.4.12 Proposición. *Sean G un grupo y A una G-álgebra conmutativa. La función $\sigma \mapsto A\#_\sigma G$ induce una biyección entre*

$$H^2(G, A^\times) \simeq \mathcal{E}(A, G, \pi),$$

donde $H^2(G, A^\times)$ es el segundo grupo de cohomología normalizada de G a valores en $A^\times$.

Demostración. Supongamos que σ y σ' están en la misma clase de cohomología, entonces existe una función $\nu : G \to A^\times$, con $\nu(e) = 1$, tal que

$$\sigma(x, y) = [x \rightharpoonup \nu(y)\nu(xy)^{-1}\nu(x)]\sigma'(x, y).$$

Consideremos la transformación lineal

$$\begin{aligned} \kappa : A\#_\sigma G &\to A\#_{\sigma'}G \\ au_x &\mapsto a\nu(x)u'_x, \end{aligned}$$

donde u'_x es un elemento invertible en la x-ésima componente homogénea de $A\#_{\sigma'}G$. Dejamos al lector la verificación que κ es un isomorfismo lineal. Veamos que κ es un isomorfismo de álgebras: sean $a, b \in A$ y $x, y \in G$,

$$\begin{aligned} \kappa(au_x)(bu_y) &= \kappa(a(x \rightharpoonup b)\sigma(x, y)u_{xy}) \\ &= a(x \rightharpoonup b)\sigma(x, y)\nu(xy)u'_{xy} \\ &= a(x \rightharpoonup b\nu(y))\nu(x)\sigma'(x, y)u'_{xy} \\ &= (a\nu(x)u'_x)(b\nu(y)u'_y) \\ &= \kappa(au_x)\kappa(bu_y). \end{aligned}$$

Entonces, evidentemente, κ es un isomorfismo de G-álgebras graduadas que deja fijo los elementos de A_e. Por lo tanto la función $\sigma \mapsto A\#_\sigma G$ está bien definida.

Recíprocamente, supongamos que existe un isomorfismo $f : A\#_\sigma G \to A\#_{\sigma'} G$ tal que el diagrama (1.9) conmuta. Consideremos la función $\nu : G \to A^\times$, definida por $\nu(x) = f(u_x)u'^{-1}_x$, donde u'_x es un elemento invertible en la x-ésima componente homogénea de $A\#_{\sigma'}G$. Ahora, para $x, y \in G$,

$$\begin{aligned} d_0(\nu)(x,y) &= [x \rightharpoonup f(u_y)(u'_x)^{-1}]f(u_{xy})^{-1}(u'_{xy})f(u_x)(u'_x)^{-1} \\ &= [x \rightharpoonup f(u_y)][x \rightharpoonup (u'_x)^{-1}]f(u_{xy})^{-1}(u'_{xy})f(u_x)(u'_x)^{-1} \\ &= [u'_x f(u_y)(u'_x)^{-1}][u'_x(u'_x)^{-1}(u'_x)^{-1}]f(u_{xy})^{-1}(u'_{xy})f(u_x)(u'_x)^{-1} \\ &= f(u_y u_{xy}^{-1} u_x)(u'_x(u'_{xy})^{-1}u'_y)^{-1} \\ &= f(\sigma(x,y))(\sigma'(x,y))^{-1} \\ &= \sigma(x,y)(\sigma'(x,y))^{-1}. \end{aligned}$$

Entonces $\sigma = d_0(\nu)\sigma'$, es decir, σ y σ' son 2-cociclos cohomólogos. □

1.4.13 Notación. Sea (A, G, π, σ) un sistema cruzado. Entonces

i) El álgebra $A\#_\sigma G$ es llamada el **producto cruzado** de G sobre A determinada por π y σ.

ii) Si σ es trivial, llamamos al álgebra $A\#_\sigma G$ el **producto semidirecto** de G sobre A y lo denotamos por $A \rtimes G$.

iii) Si π es trivial, llamamos al álgebra $A\#_\sigma G$ el **álgebra de grupo torcida** de G sobre A y lo denotamos por $A_\sigma G$.

iv) Si π y σ son ambas triviales, llamamos al álgebra $A\#_\sigma G$ el **álgebra de grupo** de G sobre A y lo denotamos por AG.

v) Usamos la notación au_g para los elementos en el producto cruzado, el producto semidirecto, el álgebra de grupo torcida y el álgebra de grupo, siempre que no haya lugar a confusión. En caso de confusión escribimos $a\#g$.

1.4.14 Nota. Quisimos establecer una coherencia en las notaciones de los capítulos 2 y 3 con las notaciones de los capítulos 4 y 5, donde el producto cruzado está definido con respecto a un álgebra de Hopf (ver Definición 4.2.6). Es por esta razón que adoptamos la notación $A\#_\sigma G$ tomada de [DNR01, Definition 6.1.9], para referirnos a un producto cruzado del grupo G sobre un álgebra A. En el caso que el 2-cociclo σ sea trivial, seguimos la notación clásica $A \rtimes G$ de [Mas97, Remark 1.4]. Las notaciones $A_\sigma G$ y AG, son las usuales en la literatura para referirse a el álgebra de grupo torcida y a el álgebra de grupo (ver [NO04, Section 4.1]).

1.5. Álgebras simples centrales

El objetivo principal de esta sección es presentar de manera sucinta algunas ideas y conceptos básicos de la teoría de álgebras simples. Los teoremas clásicos que presentamos son:

el Teorema de Wedderburn, el Lema de densidad de Jacobson y el Lema de Schur. Estos resultados son fundamentales como veremos en los capítulos 2 y 3.

Como referencia para esta sección están los libros [GS06, Lor08].

Asumimos que las álgebras a considerar son de dimensión finita sobre el cuerpo k. Recordemos que un álgebra A es **simple** si no posee ideales bilaterales más que 0 y A. Un álgebra sobre k simple es **central** si su centro coincide con k. En este caso decimos que A es un **álgebra simple central sobre k.**

Algunos ejemplos básicos de álgebras simples centrales:

1.5.1 Ejemplo.

i) Un álgebra de división D, es evidentemente un álgebra simple. Su centro $Z(D)$ es un cuerpo, por lo tanto D es un álgebra simple y central sobre su centro.

ii) Si D es un álgebra de división sobre k, el álgebra $M_n(D)$ de matrices de tamaño $n \times n$ sobre D es simple para todo $n \geq 1$. En efecto, sean M una matriz no nula en $M_n(D)$ y $\langle M \rangle$ el ideal bilateral generado por M. Consideremos las matrices E_{ij} que tiene un 1 en la j-ésima componente de la i-ésima fila y cero en el resto. Ahora cada elemento de $M_n(D)$ es una combinación D-lineal de las matrices E_{ij}, entonces para mostrar que $\langle M \rangle = M_n(D)$ es suficiente con mostrar que E_{ij} está en $\langle M \rangle$ para todo i, j. Pero la relación $E_{ki}E_{ij}E_{jl} = E_{kl}$ nos muestra que si E_{ij} está en $M_n(D)$ para algunos i, j, entonces E_{ij} está en $M_n(D)$ para todos los i, j en $\{1, ..., n\}$. Escojamos un elemento $m \in D$ no nulo de la j-ésima componente de la i-ésima fila de la matriz no nula M. Entonces $m^{-1}E_{ii}ME_{jj} = E_{ij}$, y obtenemos el resultado deseado.
Ahora evidentemente el centro de $M_n(D)$ contiene solamente múltiplos escalares de la matriz identidad, esto es, $Z(M_n(D)) = Z(D)I_n$. Por lo tanto $M_n(D)$ es un álgebra simple y central sobre $Z(D)$.

1.5.2 Lema (Lema de Schur)**.** *Sea A un álgebra y sean M y N A-módulos.*

i) *Si M es simple, toda transformación f no nula en* $\mathrm{Hom}_A(M, N)$ *es inyectiva. Si N es simple, toda transformación f no nula en* $\mathrm{Hom}_A(M, N)$ *es sobreyectiva.*

ii) *Si M y N son simples, $M \simeq N$ ó* $\mathrm{Hom}_A(M, N) = 0$

iii) *Si M es simple,* $\mathrm{End}_A(M)$ *es un álgebra de división.*

Demostración.

i) Sea f un homomorfismo no nulo en $\mathrm{Hom}_A(M, N)$. El núcleo y la imagen de f son submódulos de M y N, respectivamente. Entonces el núcleo de f es distinto de M y la imagen de f es distinto del módulo nulo. Si M es simple, el núcleo de f es igual al submódulo nulo y si N es simple, la imagen de f coincide con N.

ii) Se sigue de (i) que cualquier homomorfismo f no nulo en $\mathrm{Hom}_A(M, N)$ es un isomorfismo.

iii) Si M es simple, todo $f \in \mathrm{End}_A(M)$ no nulo es un isomorfismo y por tanto tiene un inverso a derecha e izquierda en $\mathrm{End}_A(M)$.

□

1.5.3 Nota. Sean A un álgebra, M un A-módulo y $C = \mathrm{End}_A(M)$ su álgebra de endomorfismos. Para $h \in C$ y $x \in M$, M tiene naturalmente estructura de C-módulo con acción $h \cdot x = h(x)$. Consideremos el homomorfismo natural $A \to \mathrm{End}_C M$ que envía un elemento a de A en el endomorfismo $x \mapsto a \cdot x$. Sean $h \in C$, $a \in A$ y $x \in M$, la ecuación

$$h \cdot (a \cdot x) = h(a \cdot x) = a \cdot h(x) = a \cdot (h \cdot x),$$

demuestra que el homomorfismo natural es en efecto un C-homomorfismo.

A continuación presentamos el Teorema de densidad de Jacobson, el cual lo podemos considerar como una generalización del Teorema de Wedderburn 1.5.5.

1.5.4 Lema (Teorema de Densidad de Jacobson)**.** *Sean A un álgebra, M un A-módulo semisimple y $C = \mathrm{End}_A(M)$ su álgebra de endomorfismos. Consideremos el homomorfismo natural de la Nota 1.5.3*

$$A \to \mathrm{End}_C(M). \tag{1.10}$$

La imagen de A bajo (1.10) *es densa en el siguiente sentido: dado $f \in \mathrm{End}_C(M)$ y una cantidad finita de elementos $x_1, x_2, \ldots, x_n$ en M, existe necesariamente un elemento a en A tal que*

$$f(x_i) = ax_i \quad \text{para todo } 1 \leq i \leq n.$$

Si M es finitamente generado como un C-módulo, entonces (1.10) *es, de hecho, sobreyectivo.*

Demostración. Consideremos el A-módulo $M^n = M \times \cdots \times M$ (n veces) y $x = (x_1, \ldots, x_n)$ un elemento en M^n. El A-módulo M^n es semisimple dado que M lo es, luego Ax es un sumando directo de M^n. Sea $p : M^n \to M^n$ una proyección sobre Ax. Entonces p está en $C' = \mathrm{End}_A(M^n)$. Veamos a f como un endomorfismo de M^n, esto es,

$$f(y) = (f(y_1), \ldots, f(y_n)) \text{ para } y = (y_1, \ldots, y_n) \in M^n.$$

Por [Lor08, F4, pag 131] f es un C'-homomorfismo de M^n, entonces $fp = pf$. Así, $fx = fpx = pfx \in Ax$, entonces existe un elemento a en A tal que

$$fx = ax,$$

como queríamos demostrar. □

A continuación enunciamos el bello Teorema de Wedderburn para álgebras simples, resultado muy importante en nuestro trabajo. En la Observación 1.5.6 destacamos algunos puntos de la demostración, la cual no realizamos por lo extensa que puede llegar a ser.

1.5.5 Teorema (Wedderburn)**.** *Sea A un álgebra simple y central de dimensión finita sobre k. Entonces existen un entero $n \geq 1$ y un álgebra de división $D \supseteq k$ tal que A es isomorfo al álgebra de matrices $M_n(D)$. Además, el álgebra de división D está unívocamente determinado salvo isomorfismos.*

Demostración. Ver [GS06, Theorem 2.1.3]. □

1.5.6 Nota. Destacamos unos puntos importantes en la construcción del álgebra de división D y el entero n en la demostración del Teorema de Wedderburn:

Sea L un ideal a izquierda simple del álgebra simple A.

- Por el Lema (1.5.2) de Schur, $D = \mathrm{End}_A(L)$ es un álgebra de división.
- $n = \dim_D(L)$.
- $A \simeq \mathrm{End}_D(L) \simeq M_n(D)$.

1.5.7 Corolario. *Sea k un cuerpo algebraicamente cerrado. Entonces toda álgebra simple y central de dimensión finita sobre k es isomorfa al álgebra de matrices $M_n(k)$ para algún $n \geq 1$.*

Demostración. Por el Teorema de Wedderburn es suficiente mostrar que no existe otra álgebra de dimensión finita $D \supseteq k$ más que el propio cuerpo k. Para esto, sea d un elemento de D que no está en k. Como D es de dimensión finita sobre k, las potencias $\{1, d, d^2, \ldots\}$ son linealmente dependientes, entonces existe un polinomio $f \in k[x]$ tal que $f(d) = 0$. Como el álgebra D es de división podemos asumir que el polinomio f es irreducible. Consideremos el homomorfismo evaluación $\phi_d : k[x]/\langle f\rangle \to D$, definido por $\phi_d(p) = p(d)$. Entonces el cuerpo $k(d) = k[x]/\langle f\rangle$ es una k-subálgebra de D. Pero k es algebraicamente cerrado, entonces $k(d) \simeq k$, lo cual es contradictorio a la suposición $d \in D \setminus k$. □

El **radical de Jacobson** del álgebra A, denotado $\mathrm{J}(A)$, es definido como la intersección de todos los ideales a izquierda maximales de A o, equivalentemente, $\mathrm{J}(A)$ es la intersección de todos los ideales a derecha maximales de A. A continuación consideramos una caracterización del radical de Jacobson cuya demostración escapa a los objetivos de estos preliminares.

1.5.8 Lema. *Sea A un álgebra con unidad 1, entonces*

$$\mathrm{J}(A) = \{x \in A |\ \textit{para cada } a \in A \textit{ existe } u \in A \textit{ tal que } (1 - xa)u = 1\}.$$

Demostración. Ver [AM92, Theorem 15.3, pág 166] . □

1.5.9 Definición. Sea A un álgebra de dimensión finita. Decimos que A es un álgebra **semisimple** si $\mathrm{J}(A) = 0$.

Ahora presentamos una versión para álgebras semisimples del Teorema de Wedderburn (1.5.5). La demostración es omitida por las mismas razones por las cuales omitimos la demostración del Teorema de Wedderburn para álgebras simples.

1.5.10 Teorema. *Un álgebra A es semisimple si y sólo si*

$$A \simeq M_{r_1}(D_1) \times M_{r_2}(D_2) \times \cdots \times M_{r_n}(D_n),$$

donde los D_i son álgebras de división. El entero $n \geq 1$ del número de factores, la clase de isomorfismos de los D_i, así como los enteros r_i, están unívocamente determinados.

Demostración. Ver [Lor08, Theorem 4] página 157. □

1.5.11 Nota. En la situación del Teorema 1.5.10, tenemos que el centro de A está dado por

$$Z(A) \simeq Z(M_{r_1}(D_1)) \times \cdots \times Z(M_{r_n}(D_n)) \simeq Z(D_1) \times \cdots \times Z(D_n).$$

Como lo podemos ver en [Lor08, **F5**, pág 154].

1.6. Álgebras de grupo torcidas simples

El objetivo principal de esta sección es presentar algunos resultados que involucran álgebras de grupo torcidas simples. Un resultado clásico que presentamos es el Teorema de Maschke para álgebras de grupo torcidas, también mostramos que si la característica de k no divide al orden de G y σ es un 2-cociclo no degenerado, entonces el álgebra $k_\sigma G$ es un álgebra simple y central sobre k (Proposición 1.6.5). Usaremos este último resultado para la construcción de un álgebra simple central a partir de un dato (Proposición 3.2.10).

Como referencia de la sección está el libro [Kar85] y el artículo [Dav01].

Consideramos a (k, G, π, σ) un sistema cruzado, donde G es un grupo finito y π es una acción débil trivial. Además consideramos a $k_\sigma G$ el álgebra de grupo torcida definido en 1.4.13.

A continuación presentamos una versión para álgebras de grupo torcida del Teorema de Maschke. La demostración será omitida por lo extensa de la misma.

1.6.1 Teorema (Maschke)**.** *Si la característica de k no divide al orden de G, entonces el álgebra de grupo torcida $k_\sigma G$ es semisimple.*

Demostración. Ver [Kar85, 2.10 Theorem]. □

Para $x \in G$, consideremos el homomorfismo

$$\begin{aligned} \sigma_x : C_G(x) &\longrightarrow k^\times \\ t &\longmapsto \frac{\sigma(x,t)}{\sigma(t,x)}, \end{aligned} \tag{1.11}$$

donde $C_G(x)$ es el subgrupo **centralizador** del elemento x en G.

1.6.2 Definición. Un 2-cociclo $\sigma \in Z^2(G, k^\times)$ es **no degenerado** si para cualquier $x \in G$, el homomorfismo σ_x es no trivial.

El siguiente lema toma ideas de [Dav01, Lemma 3.4].

1.6.3 Lema. *La dimensión del centro del álgebra $k_\sigma G$ es igual al número de clases de conjugación del grupo G para el cual el homomorfismo* (1.11) *es trivial.*

Demostración. Sea $z = \sum_{g\in G} z(g)u_g$, donde $z(g) \in k$, un elemento en el álgebra de grupo torcida. El elemento z está en el centro de $k_\sigma G$ si y sólo si

$$zu_t = u_t z \qquad \forall t \in G.$$

Consideremos

$$\begin{aligned} zu_t &= \sum_{g\in G} (z(g)u_g)u_t \\ &= \sum_{g\in G} z(g)\sigma(g,t)u_{gt} \end{aligned} \tag{1.12}$$

$$\begin{aligned} u_t z &= \sum_{g\in G} u_t(z(g)u_g) \\ &= \sum_{g\in G} z(g)\sigma(t,g)u_{tg} \end{aligned} \tag{1.13}$$

Comparando los coeficientes de u_{gt} en las expresiones (1.12) y (1.13) obtenemos las ecuaciones

$$z(t^{-1}gt)\sigma(t,t^{-1}gt) = z(g)\sigma(g,t), \qquad \forall t,g \in G, \tag{1.14}$$

que equivalen a condiciones suficientes y necesarias para que z pertenezca al centro del álgebra de grupo torcida. Sea g un elemento en G para el cual el homomorfismo σ_g dado en (1.11) es trivial. El elemento

$$z_g = \sum_{t\in G/C_G(g)} \frac{\sigma(t,g)}{\sigma(t^{-1}gt,t)} u_{tgt^{-1}}$$

pertenece al centro de $k_\sigma G$ y no depende (salvo la multiplicación de una constante no nula) de la elección de g en su clase de conjugación. Entonces, la condición (1.14) implica que $z(g) = 0$ para cualquier g para el cual el homomorfismo σ_g es no trivial. Por lo tanto, cualquier elemento del centro de $k_\sigma G$ es una combinación lineal de los elementos z_g, para los g representantes de las clases de conjugación tales que el homomorfismo σ_g es trivial. □

Inmediatamente obtenemos que:

1.6.4 Corolario. *Un 2-cociclo σ es no degenerado si y sólo si la dimensión sobre k del centro de $k_\sigma G$ es igual a 1.*

□

1.6.5 Proposición. *Sean G un grupo finito y $\sigma \in Z^2(G,k^\times)$ un 2-cociclo. Si la característica de k no divide al orden de G y σ es un 2-cociclo no degenerado, entonces el álgebra $k_\sigma G$ es un álgebra simple y central sobre k.*

Demostración. Supongamos que $\mathrm{char}(k) \nmid |G|$, entonces por el Teorema de Maschke 1.6.1, $k_\sigma G$ es un álgebra semisimple. Además si σ es no degenerado por el Corolario 1.6.4, el centro del álgebra torcida es de dimensión 1, es decir, coincide con el cuerpo k. Por lo tanto $k_\sigma G$ es simple y central sobre k. □

1.6.1. Ejemplos de álgebras de grupo torcidas simples

En esta subsección nos referimos a los trabajos hechos por Aljadeff, Haile y Natapov en [AHN05, Nat07b], para presentar algunos ejemplos de álgebras de grupo torcidas $k_\sigma G$ simples. Suponemos que $k_\sigma G$ es un álgebra de división. En este caso el papel del grupo finito G es fundamental.

Consideremos la siguiente lista de p-grupos:

1. G es abeliano de tipo simétrico, esto es $G \simeq \prod_i (\mathbb{Z}_{p^{n_i}} \times \mathbb{Z}_{p^{n_i}})$,
2. $G \simeq G_1 \times G_2$, donde $G_1 = \mathbb{Z}_{p^n} \rtimes \mathbb{Z}_{p^n} = \text{gen}\{a, b | a^{p^n} = b^{p^n} = 1 \text{ y } aba^{-1} = b^{p^s+1}, 1 \leq s < n \text{ y } 1 \neq s \text{ si } p = 2\}$, y G_2 es un grupo abeliano de tipo simétrico de exponente menor o igual a p^s,
3. $G \simeq G_1 \times G_2$, donde $G_1 = \mathbb{Z}_{2^{n+1}} \rtimes (\mathbb{Z}_{2^n} \times \mathbb{Z}_2)$ y G_2 es un grupo abeliano de tipo simétrico de exponente menor o igual a 2.

Decimos que G está en la lista Λ si G es de la forma 1, 2 o 3.

El siguiente teorema es el resultado principal del artículo [Nat07b] y caracteriza las álgebras de grupo torcidas que son a su vez álgebras de división.

1.6.6 Teorema. *Sea G un grupo finito. Entonces existe un cuerpo k y una clase de cohomología $\sigma \in H^2(G, k^\times)$ tal que el álgebra de grupo torcida $k_\sigma G$ es un álgebra de división central sobre k si y sólo si G es nilpotente y todos los p-subgrupos de Sylow de G están en la lista Λ.*

Demostración. Ver [Nat07b, Theorem 3] □

1.6.7 Nota. Sean σ un 2-cociclo y G un grupo nilpotente tal que todos sus p-subgrupos de Sylow están en la lista Λ. Por el Teorema 1.6.6, existe un cuerpo k tal que el álgebra de grupo torcida $k_\sigma N$ es un álgebra de división central sobre k. Entonces por el corolario 1.6.4 σ es un 2-cociclo no degenerado.

CAPÍTULO 2

Álgebras de Galois

El objetivo principal de este capítulo es demostrar que toda G-álgebra de Galois es isomorfa como G-álgebra, al álgebra inducida de una S-álgebra simple, donde S es un subgrupo de G (ver Teorema 2.3.4). Este resultado nos permite reducir el problema de clasificar las álgebras de Galois a clasificar las álgebras de Galois simples (ver Capítulo 3).

A continuación presentamos por secciones, el contenido del capítulo y las conexiones que el mismo tiene con el resto del escrito.

- 2.1 Álgebras de Galois: Presentamos la noción de álgebra de Galois y demostramos una primera caracterización mediante ideales G-invariantes y el álgebra de invariantes (ver Proposición 2.1.10). Usaremos este resultado de manera técnica en algunas demostraciones expuestas en el escrito (ver, por ejemplo, Corolario 2.3.2).
- 2.2 Álgebras imprimitivas y álgebras inducidas: Presentamos la noción de álgebra imprimitiva y de la noción de álgebra inducida. Usaremos estas nociones como herramienta principal en la clasificación de las álgebras de Galois.
- 2.3 Álgebras de Galois asociada a un álgebra inducida: En esta sección se establece el objetivo principal de este capítulo. Usaremos estos resultados para clasificar las álgebras de Galois.

En este capítulo la mayoría de los resultados son ideas originales del autor y su orientador. Es por ello que no se cita un artículo o libro en especifico, salvo para algunas partes de la sección 2.1, donde podemos citar el artículo de Davydov [Dav01].

2.1. Álgebras de Galois

En esta sección presentamos el concepto de G-álgebra de Galois sobre k, el cual generaliza la noción clásica de extensión de Galois en teoría de cuerpos (ver Ejemplo 2.1.7).

Como referencia para esta sección está el artículo [Dav01].

Suponemos a lo largo de la sección y del capítulo que (A, G, π, σ) es un **sistema cruzado**, donde G es un **grupo finito** con unidad e, σ **es un 2-cociclo trivial** y A *es una G-álgebra no nula de dimensión finita sobre k*. La acción $\pi(g)(a)$ la denotamos por $g \rightharpoonup a$.

2.1.1 Definición.

i) Un ideal J de A es **G-invariante** si

$$g \rightharpoonup x \in J \quad \text{para todo} \quad x \in J, g \in G.$$

ii) El conjunto $A^G = \{a \in A | g \rightharpoonup a = a, \forall g \in G\}$ es una subálgebra de A, la cual llamamos el **álgebra de invariantes** de A por la acción de G.

El producto semidirecto $A \rtimes G$ de G sobre A, definido en 1.4.13, es el álgebra $A = \bigoplus_{g \in G} Au_g$, con multiplicación

$$(au_g)(bu_h) = a(g \rightharpoonup b)u_{gh} \quad (a, b \in A, g, h \in G)$$

y unidad u_e. Consideremos la transformación

$$\begin{aligned} \theta : A \rtimes G &\to \mathrm{End}(A) \\ au_g &\mapsto \theta_{au_g} = [b \mapsto a(g \rightharpoonup b)], \end{aligned} \tag{2.1}$$

del producto semidirecto al álgebra de endomorfismos lineales de A.

2.1.2 Lema. *La transformación θ es un homomorfismo de anillos. Entonces A tiene estructura de $A \rtimes G$-módulo a través de θ.*

Demostración. Sea $a \in A$, la ecuación $\theta_{u_e}(a) = 1(e \rightharpoonup a) = a$ muestra que $\theta_{u_e} = \mathrm{Id}_A$. Ahora sean $a, b, c \in A$ y $g, h \in G$, la sucesión de igualdades

$$\begin{aligned} \theta_{(au_g)(bu_h)}(c) &= \theta_{a(g \rightharpoonup b)u_{gh}}(c) \\ &= a(g \rightharpoonup b)(gh \rightharpoonup c) \\ &= a(g \rightharpoonup b)(g \rightharpoonup (h \rightharpoonup c)) \\ &= a(g \rightharpoonup b(h \rightharpoonup c)) \\ &= \theta_{(au_g)} b(h \rightharpoonup c) \\ &= \theta_{(au_g)} \circ \theta_{(bu_h)}(c) \end{aligned}$$

muestran que $\theta_{(au_g)(bu_h)} = \theta_{(au_g)} \circ \theta_{(bu_h)}$. Entonces θ es un homomorfismo de anillos, como se quería demostrar. □

2.1.3 Lema. *Con las hipótesis del lema anterior, tenemos que*

$$\theta(A \rtimes G) \subseteq \mathrm{End}_{A^G}(A),$$

donde A es un A^G-módulo a derecha con la multiplicación de A.

Demostración. La ecuación

$$\theta_{xu_g}(y \cdot b) = x(g \rightharpoonup yb) = x(g \rightharpoonup y)b = \theta_{xu_g}(y) \cdot b,$$

implica que $\theta_{xu_g} \in \mathrm{End}_B(A)$ para cualquier $x, y \in A$, $b \in A^G$ y $g \in G$. □

Entonces A tiene estructura de $A \rtimes G$-módulo a izquierda, con acción $au_g \cdot b = a(g \rightharpoonup b)$ y sea $D = \mathrm{End}_{A \rtimes G}(A)$ su álgebra de endomorfismos. Por la Nota 1.5.3, A tiene estructura de D-módulo. Veamos que

2.1.4 Lema. *Las álgebras* $\mathrm{End}_D(A)$ *y* $\mathrm{End}_{A^G}(A)$ *coinciden.*

Demostración. En efecto, sean $\tau \in \mathrm{End}_D(A)$, $a \in A$ y $b \in A^G$. La transformación $f_b : A \to A$ definida por $f_b(a) = ab$, es un $A \rtimes G$-morfismo de módulos, es decir, $f_b \in D$ para $b \in A^G$. Entonces la sucesión de ecuaciones

$$\tau(a \cdot b) = \tau(f_b \cdot a) = f_b \cdot \tau(a) = \tau(a) \cdot b$$

muestran que τ es un A^G-morfismo de módulos, es decir, $\tau \in \mathrm{End}_{A^G}(A)$.

Recíprocamente, sean $\tau \in \mathrm{End}_{A^G}(A)$, $f \in D$ y $a \in A$. Evidentemente, $f(1) = f(g \rightharpoonup 1) = g \rightharpoonup f(1)$ está en A^G. Entonces la sucesión de ecuaciones

$$\tau(f \cdot a) = \tau(f(a)) = \tau(a \cdot f(1)) = \tau(a) \cdot f(1) = f \cdot \tau(a)$$

muestran que τ es un D-morfismo de módulos, es decir, $\tau \in \mathrm{End}_D(A)$. □

2.1.5 Definición. Sea A una G-álgebra con $B = A^G$, decimos que la extensión $B \subseteq A$ es de **Galois** si el homomorfismo

$$\theta : A \rtimes G \to \mathrm{End}_B(A)$$

es un isomorfismo.

2.1.6 Definición (Álgebra de Galois)**.** Sea A una **G-álgebra sobre** k, decimos que A es una G-álgebra de Galois sobre k si $A^G = k$ y A es una extensión de Galois.

Un ejemplo de álgebras de Galois son las extensiones Galois para cuerpos. Para su demostración tomamos ideas de Montgomery en [Mon93].

2.1.7 Ejemplo. Sean K un cuerpo, $G \subseteq \mathrm{Aut}(K)$ un grupo finito y $k = K^G$ el cuerpo fijo de K sobre G. Entonces $K \supseteq k$ es una extensión de Galois con grupo de Galois $G = \mathrm{Gal}(K/k)$ si y sólo si K es una G-álgebra de Galois sobre k.

Demostración. Supongamos que $K \supseteq k$ es una extensión de Galois. Evidentemente K es una G-álgebra con acción natural

$$\begin{aligned} G \times K &\to K \\ (g, \alpha) &\to g(\alpha). \end{aligned}$$

Consideremos el homomorfismo de anillos

$$\theta : K \rtimes G \to \mathrm{End}_k(K); \quad \theta(\alpha u_g)(\beta) = \alpha g(\beta).$$

Por [Mon80, Theorem 2.3, pag 20] el producto semidirecto $K \rtimes G$ es un álgebra simple. Entonces por el Lema de Schur 1.5.2, θ es inyectiva. Además,

$$\dim_k(K \rtimes G) = [K : k]|G| = [K : k]^2 = \dim_k(\mathrm{End}_k(K)), \tag{2.2}$$

por ser $K \supseteq k$ una extensión de Galois. Por lo tanto θ es un isomorfismo de álgebras, como se quería demostrar.

Recíprocamente, supongamos que K es una G-álgebra de Galois sobre k. Entonces por la Ecuación (2.2) $[K : k] = |G|$ y esto a su vez implica que K es una extensión de Galois de k con grupo de Galois G (ver [DNR01, Example 6.4.3, pag 255]). □

2.1.8 Definición. Sean A y B dos G-álgebras sobre k, decimos que la transformación lineal $f : A \to B$ es un **homomorfismo de G-álgebras de Galois** si f es un homomorfismo de G álgebras.

2.1.9 Lema. *Sea $f : A \to B$ un isomorfismo de G-álgebras. Entonces A es una G-álgebra de Galois sobre k si y sólo si B es una G-álgebra de Galois.*

□

A continuación presentamos una caracterización de las G-álgebras de Galois sobre k un cuerpo arbitrario; usando ideales G-invariantes y una condición fundamental sobre el álgebra A^G de invariantes.

2.1.10 Proposición. *Sea A una G-álgebra sobre k. Entonces, A es de Galois si y sólo si A satisface las siguientes condiciones:*

i) La dimensión de A sobre k coincide con el orden de G.

ii) A no posee ideales a izquierda G-invariantes no triviales.

iii) $A^G = k$.

Demostración. Supongamos que A una G-álgebra de Galois sobre k.

i) La ecuación

$$\dim_k(A)|G| = \dim_k(A \rtimes G) = \dim_k(\mathrm{End}_k(A)) = (\dim_k(A))^2,$$

muestra que la dimensión de A es igual al orden de G.

ii) Sea J un ideal a izquierda G-invariante de A. La condición sobre J implica que $\theta(A \rtimes G)(J) \subseteq J$ y dado que $\theta(A \rtimes G) = \mathrm{End}(A)$, por ser θ un isomorfismo, obtenemos que J es invariante bajo todos los endomorfismos lineales de A. Supongamos que J es no nulo y consideremos $x \in J$, $x \neq 0$. Entonces, existe $\tau \in \mathrm{End}(A)$ tal que $\tau(x) = 1 \in J$. Por lo tanto $J = A$, esto es, J es un ideal trivial de A.

Recíprocamente, supongamos que A cumple las tres condiciones del teorema. Consideremos el álgebra A como un $A \rtimes G$-módulo a izquierda con morfismo estructura θ. La condición (i) implica que A es un $A \rtimes G$-módulo simple (y artiniano, es decir, semisimple). Si $D = \mathrm{End}_{A \rtimes G}(A)$ y $\mathrm{End}_D(A) = \mathrm{End}_{A^G}(A)$ (ver Lema 2.1.4), entonces aplicando el Teorema de densidad de Jacobson (1.5.4) para A y $\mathrm{End}_D(A)$ tenemos que el homomorfismo natural

$$\theta : A \rtimes G \to \mathrm{End}_D(A) = \mathrm{End}_{A^G}(A) = \mathrm{End}_k(A)$$

es sobreyectivo. Ahora la ecuación

$$\dim_k(\ker\theta) = \dim_k(A \rtimes G) - \dim_k(\mathrm{End}_k(A)) = |G|^2 - |G|^2 = 0,$$

implica que el homomorfismo θ es un inyectivo. Por lo tanto θ es un isomorfismo, es decir, A es una G-álgebra de Galois sobre el cuerpo k. □

La condición impuesta sobre el álgebra de invariantes no es necesaria si k es un cuerpo algebraicamente cerrado, ya que cualquier álgebra de división $D \supseteq k$ coincide con k (ver [GS06, Corollary 2.1.7]). Es por ello que Davydov en [Dav01, Proposition 3.1, pag 280] no lo tiene en cuenta. Pero en nuestro caso es absolutamente necesario como se muestra a continuación.

2.1.11 Nota. Mostremos que la condición $A^G = k$ en la Proposición (2.1.10) es necesaria. Sean k un cuerpo que no sea algebraicamente cerrado, K una extensión finita de k; de dimensión $[K : k] = n > 1$, y $G = \mathbb{Z}_n$ el grupo de los enteros módulo n que actúa trivialmente sobre K, es decir, $K^G = K \neq k$. Entonces, si K es una G-álgebra de Galois sobre k, el homomorfismo de anillos

$$\begin{aligned} \theta : K \rtimes G &\to \mathrm{End}_k(K) \\ \alpha u_g &\mapsto \theta_{\alpha u_g} = [\beta \mapsto \alpha\beta] \end{aligned}$$

es un isomorfismo y esto implica que el homomorfismo de anillos

$$\begin{aligned} \tau : K &\to \mathrm{End}_k(K) \\ \alpha &\mapsto \tau_\alpha = [\beta \mapsto \alpha\beta], \end{aligned}$$

es un isomorfismo lo cual es una contradicción porque

$$[K : k] = n \neq n^2 = \dim_k(\mathrm{End}_k(K)).$$

Veamos que toda álgebra de Galois es un álgebra semisimple.

2.1.12 Lema. *El radical de Jacobson de A es un ideal G-invariante.*

Demostración. Usamos la equivalencia para el radical de Jacobson dada en el Lema 1.5.8. Entonces para cada $x \in \mathrm{J}(A)$ y cada $a \in A$ existe un $u \in A$ tal que

$$(1 - xa)u = 1.$$

Aplicando a la ecuación anterior la acción $\rightharpoonup$ para un $g \in G$ obtenemos que

$$g \rightharpoonup (1 - xa)u = g \rightharpoonup 1 \Rightarrow [1 - (g \rightharpoonup x)(g \rightharpoonup a)]g \rightharpoonup u = 1.$$

Entonces $g \rightharpoonup x$ está en $\mathrm{J}(A)$ para cualesquiera $g \in G$ y $x \in \mathrm{J}(A)$, como queríamos demostrar. □

2.1.13 Corolario. *Toda G-álgebra de Galois es semisimple.*

Demostración. Sea A una G-álgebra de Galois. El Lema 2.1.12 afirma que $\mathrm{J}(A)$ es un ideal G-invariante. Entonces debemos tener que $\mathrm{J}(A) = 0$ ó $\mathrm{J}(A) = A$. Pero $\mathrm{J}(A) \neq A$ por la definición del radical de Jacobson. Por lo tanto $\mathrm{J}(A) = 0$, es decir, A es semisimple. □

2.2. Álgebras imprimitivas y álgebras inducidas

En esta sección definimos la noción de álgebra imprimitiva y álgebra inducida. La noción de álgebra imprimitiva esta inspirada en algunas ideas de la teoría de Clifford (ver [CR90, Section 6]). Establecemos y demostramos una construcción alternativa a la presentada en Davydov [Dav01, Section 3].

Como es usual en nuestro trabajo, G denota un grupo y A un álgebra.

Supongamos que A se descompone en una suma directa de ideales bilaterales $\{A_i\}$, esto es,

$$A = A_1 \oplus \cdots \oplus A_n. \tag{2.3}$$

Entonces por cada $1 \leq i \leq n$ existen $\{e_i\}$ elementos en A_i tales que

$$1 = e_1 + \cdots + e_n. \tag{2.4}$$

Así, para cada $x \in A$, tenemos que

$$x = xe_1 + \cdots + xe_n = e_1x + \cdots e_nx, \text{ y } \ xe_i, \ e_ix \in A_i.$$

Esto nos muestra que si $x \in A_i$, entonces $x = xe_i = e_ix$ y $xe_j = e_jx = 0$ para $i \neq j$. Por lo tanto tenemos que

$$A_i = Ae_i = e_iA, \ e_i^2 = e_i \neq 0, \ e_ie_j = 0 \ \forall i \neq j, \ e_ia = ae_i \ \forall a \in A. \tag{2.5}$$

Decimos que $\{e_1, \ldots, e_n\}$ es un conjunto de **idempotentes centrales ortogonales** si este satisface las condiciones en (2.4) y (2.5). Recíprocamente, si tenemos un conjunto de idempotentes centrales ortogonales $\{e_1, \ldots, e_n\}$ en A, entonces A se descompone en una suma directa $A = \oplus Ae_i$ de ideales bilaterales Ae_i. Un idempotente $e \in A$ lo llamamos **primitivo** si no es expresable como la suma de dos idempotentes centrales ortogonales. Entonces por el Teorema de Wedderburn un álgebra A es semisimple si y sólo si contiene un conjunto de idempotentes centrales ortogonales primitivos tal que A se descompone como en (2.3) y cada A_i es simple, en este caso, decimos que A posee una **descomposición de Wedderburn** y el hecho que cada e_i sea primitivo implica que el conjunto $\{e_1, \ldots, e_n\}$ es el único conjunto de idempotentes centrales ortogonales primitivos de A, en este caso, decimos que $\{e_1, \ldots, e_n\}$ es el **sistema de Wedderburn** para A determinado por la descomposición (2.3).

2.2.1 Definición. Sea A una G-álgebra. Un conjunto $\{e_1, \ldots, e_n\}$ de idempotentes centrales ortogonales de A es un **sistema de idempotentes centrales ortogonales compatible con la acción de** G, o simplemente un **sistema imprimitivo**, si la acción de G sobre A induce una acción de G sobre el conjunto $\{e_1, \ldots, e_n\}$. En este caso decimos que A es una **G-álgebra imprimitiva.**

Consideremos a continuación dos G-álgebras determinadas por S un subgrupo de G y B una S-álgebra, con acción denotada $\rightharpoonup$.

1) El espacio vectorial

$$kG \otimes_{kS} B$$

con G-acción y multiplicación dadas, respectivamente, por

$$g \cdot (h \otimes x) = gh \otimes x$$
$$(g \otimes x)(h \otimes y) = \begin{cases} h \otimes (h^{-1}g \rightharpoonup x)y & \text{si } h^{-1}g \in S \\ 0 & \text{si } h^{-1}g \notin S, \end{cases}$$

para $g, h \in G$ y $x, y \in B$.

2) El espacio de funciones

$$A_S(G, B) = \{r : G \to B | r(sg) = s \rightharpoonup r(g) \qquad \forall s \in S, g \in G\},$$

con la multiplicación puntual entre funciones y G-acción definida por $(g \cdot r)(x) = r(xg)$.

Entonces,

2.2.2 Proposición. *$A_S(G, B) \simeq kG \otimes_{kS} B$ como G-álgebras.*

Demostración. Ver [GN07, Proposition 3.3]. □

2.2.3 Definición. Llamamos a la G-álgebra $A_S(G, B) \simeq kG \otimes_{kS} B$ el **álgebra inducida** por la S-álgebra B y la denotamos por $\mathrm{Ind}_S^G(B)$.

La siguiente proposición nos da una caracterización de las álgebras imprimitivas por medio de álgebras inducidas. Las ideas son originales de Galindo y Natale (ver [GN07]).

2.2.4 Proposición. *Sea A una G-álgebra imprimitiva tal que G actúa transitivamente sobre el sistema imprimitivo $\{e_1, \ldots, e_n\}$, y sea S el estabilizador de e_1 bajo la acción de G. Entonces*

i) e_1A es una S-álgebra,

ii) existe un isomorfismo de G-álgebras entre A y $\mathrm{Ind}_S^G(e_1A)$.

Demostración. El número $[G : S]$ de coclases a izquierda de S en G es igual al número de elementos de la órbita de e_1 y dado que G actúa transitivamente sobre el sistema de elementos imprimitivos $\{e_1, \ldots, e_n\}$, entonces $[G : S] = n$. Por lo tanto podemos elegir un conjunto $\{g_1, \ldots, g_n\}$ de representantes de las coclases a izquierda de S en G tales que $g_i \rightharpoonup e_1 = e_i$. Así, evidentemente, tenemos que

$$\mathrm{Ind}_S^G(e_1A) = kG \otimes_{kS} e_1A = \bigoplus_{i=1}^{n} g_i \otimes e_1A.$$

Consideremos la transformación lineal

$$\psi : kG \otimes_{kS} e_1A \to A$$
$$\sum_{i=1}^{n} g_i \otimes e_1x_i \mapsto \sum_{i=1}^{n} e_i(g_i \rightharpoonup x_i).$$

Primero veamos que la transformación está bien definida. Supongamos a $\tilde{g}_i$ otros representantes de las coclases g_iS, es decir, $\tilde{g}_i = g_is_i$ para algunos $s_i \in S$ y $\tilde{g}_i \rightharpoonup e_1 = e_i$. Sean $x = \sum_{i=1}^n g_i \otimes e_1x_i$ y $\tilde{x} = \sum_{i=1}^n \tilde{g}_i \otimes e_1\tilde{x}_i$ elementos en $\bigoplus_{i=1}^n g_i \otimes e_1A$, la sucesión de ecuaciones

$$\begin{aligned}
&\sum_{i=1}^n g_i \otimes e_1x_i = \sum_{i=1}^n \tilde{g}_i \otimes e_1\tilde{x}_i \\
\leftrightarrow &\sum_{i=1}^n g_i \otimes e_1x_i = \sum_{i=1}^n g_i \otimes s_i \rightharpoonup (e_1\tilde{x}_i) \\
\leftrightarrow &\sum_{i=1}^n g_i \otimes e_1x_i = \sum_{i=1}^n g_i \otimes e_1(s_i \rightharpoonup \tilde{x}_i) \\
\leftrightarrow &\qquad\qquad x_i = s_i \rightharpoonup \tilde{x}_i,
\end{aligned}$$

muestran que $x = \tilde{x}$ si y sólo si $x_i = s_i \rightharpoonup \tilde{x}_i$ para cada $1 \leq i \leq n$. Por lo tanto si $x = \tilde{x}$ tenemos que

$$\psi(x) = \sum_{i=1}^n e_i(\tilde{g}_i \rightharpoonup \tilde{x}_i) = \sum_{i=1}^n e_i(g_i \rightharpoonup x_i) = \psi(\tilde{x}).$$

Veamos que ψ es un isomorfismo. Sea $\sum_{i=1}^n g_i \otimes e_1x_i \in \ker\psi$, esto es,

$$\sum_{i=1}^n e_i(g_i \rightharpoonup x_i) = 0.$$

Multiplicando consecutivamente la ecuación anterior por e_i tenemos que cada $g_i \rightharpoonup x_i = 0$, lo que implica que $x_i = 0$, entonces $\sum_{i=1}^n g_i \otimes e_1x_i = 0$. Ahora evidentemente ψ es sobreyectiva, ya que G actúa por automorfismos de A y $A = \bigoplus_{i=1}^n e_iA$. Veamos que ψ es un morfismo de anillos. Sean $\sum_{i=1}^n g_i \otimes e_1x_i$ y $\sum_{j=1}^n g_j \otimes e_1\tilde{x}_j$, elementos en $kG \otimes_{kS} e_1A$, su producto es igual a

$$\sum_{i,j=1}^n (g_i \otimes e_1x_i)(g_j \otimes e_1\tilde{x}_j) = \sum_{i,j=1}^n g_j \otimes (g_j^{-1}g_i \rightharpoonup (e_1x_i))e_1\tilde{x}_j \tag{2.6}$$

aplicando ψ a la Ecuación (2.6), obtenemos

$$\begin{aligned}
&\sum_{i,j=1}^n e_j(g_j \rightharpoonup [(g_j^{-1}g_i \rightharpoonup e_1x_i)(e_1\tilde{x}_j)]) \\
&= \sum_{i,j=1}^n e_j(e_i(g_i \rightharpoonup x_i)e_j(g_j \rightharpoonup \tilde{x}_j)) \\
&= \sum_{i=1}^n e_i(g_i \rightharpoonup x_i)(g_i \rightharpoonup \tilde{x}_i) \\
&= \psi(\sum_{i=1}^n g_i \otimes e_1x_i)\psi(\sum_{j=1}^n g_j \otimes e_1\tilde{x}_j).
\end{aligned}$$

Por último es claro que ψ es un morfismo de G-álgebras. Por lo tanto ψ es un isomorfismo de G-álgebras como queríamos demostrar. □

2.2.5 Lema. *Sean S un subgrupo de G y B una S-álgebra. Entonces el álgebra inducida $Ind_S^G(B)$ por B es isomorfa, como álgebra, al producto*

$$\prod_{[G:S]-veces} B.$$

Además, la subálgebra de G-invariantes de $Ind_S^G(B)$ es isomorfa a la subálgebra de S-invariantes de B.

Demostración. Sean $g_1 = e$, $m = [G : S]$ y $\{g_1, \ldots, g_m\}$ un conjunto de representantes de las coclases a derecha de S en G. Consideremos las funciones e_i en $\mathrm{Ind}_S^G(B)$ definidas por

$$e_i(x) = \begin{cases} 1_B, & \text{si } x \in Sg_i, \\ 0, & \text{si } x \notin Sg_i. \end{cases}$$

Para $x \in G$ y $r \in \mathrm{Ind}_S^G(B)$, los numerales $i)$, $ii)$, $iii)$ y $iv)$ muestran que el conjunto $\{e_1 \ldots, e_m\}$ es un sistema imprimitivo para $\mathrm{Ind}_S^G(B)$.

$i)$
$$e_i(x)r(x) = r(x)e_i(x) = \begin{cases} r(x), & \text{si } x \in Sg_i, \\ 0, & \text{si } x \notin Sg_i. \end{cases}$$

$ii)$
$$e_i \cdot e_j(x) = e_j \cdot e_i(x) = \begin{cases} 1_B, & \text{si } i = j, x \in Sg_i, \\ 0, & \text{si } i \neq j. \end{cases}$$

$iii)$ $\sum_{i=1}^m e_i(x) = 1_B$

$iv)$ Si $g_i g^{-1} \in Sg_j$, entonces

$$(g \cdot e_i)(x) = e_i(xg) = e_j(x) = \begin{cases} 1_B, & \text{si } xg \in Sg_i, \\ 0, & \text{si } xg \notin Sg_i. \end{cases}$$

Entonces

$$\mathrm{Ind}_S^G(B) \simeq e_1\mathrm{Ind}_S^G(B) \times \cdots \times e_m\mathrm{Ind}_S^G(B).$$

Ahora consideremos los isomorfismo lineales

$$e_i\mathrm{Ind}_S^G(B) \to e_1\mathrm{Ind}_S^G(B); \text{ definido por } e_i r \mapsto e_1 r_i \tag{2.7}$$
$$e_1\mathrm{Ind}_S^G(B) \to B; \text{ definido por } e_1 r \mapsto r(e) \tag{2.8}$$

donde $r_i : G \to B$ está definida por $r_i(x) = r(xg_i)$. Por lo tanto tenemos que para $1 \leq i \leq m$

$$e_i\mathrm{Ind}_S^G(B) \simeq e_1\mathrm{Ind}_S^G(B) \quad \text{y} \quad e_1\mathrm{Ind}_S^G(B) \simeq B.$$

Para demostrar nuestra segunda afirmación, consideremos la transformación lineal

$$\begin{aligned} B^S &\to (\mathrm{Ind}_S^G(B))^G \\ b &\mapsto r_b = [x \mapsto b], \end{aligned} \tag{2.9}$$

la cual es evidentemente un isomorfismo de álgebras. □

2.3. Álgebra de Galois asociada a un álgebra inducida

En esta sección mostramos el resultado principal de este capítulo. Demostramos que dada A una G-álgebra de Galois existe una S-álgebra de Galois simple B tal que el álgebra inducida por B es isomorfa como G-álgebras, a A.

Recordemos que si A es un álgebra semisimple, por el Teorema de Wedderburn 1.5.10 para álgebras semisimples, A posee una descomposición de Wedderburn

$$A \simeq M_{r_1}(D_1) \times M_{r_2}(D_2) \times \cdots \times M_{r_n}(D_n), \tag{2.10}$$

donde D_i son álgebras de división y r_i, n son enteros mayores o iguales a 1, que están unívocamente determinados. Usamos la notación

$$a = (a_1, a_2, \ldots, a_n),$$

para una matriz a en A construida en bloques, donde cada a_i está en $M_{r_i}(D_i)$. Con operaciones obvias extendidas

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Consideremos las matrices

$$E_i = (0, \ldots, 0, e_i, 0, \ldots, 0) \tag{2.11}$$

de A, donde e_i es la matriz identidad de $M_{n_i}(D_i)$, para $1 \leq i \leq n$. Es evidente que cada matriz E_i es un elemento central del álgebra A, $E_i E_j = E_i(\delta_{i,j})$, $1_A = \sum_{i=1}^{n} E_i = (e_1, e_2, \ldots, e_n)$ y cada E_i es un idempotente primitivo. Entonces el conjunto $\{E_1, \ldots, E_n\}$ es el sistema de Wedderburn determinado por el isomorfismo dado en (2.10).

2.3.1 Lema. *Sean A un álgebra semisimple y G un grupo finito que actúa sobre A tal que $A^G = k$. Entonces el conjunto $\{E_i\}$ de las matrices en A, definidas en* (2.11)*, es un sistema imprimitivo para A el cual es transitivo bajo la acción de G.*

Demostración. Dado que G actúa sobre A por automorfismos tenemos que G actúa sobre $\{E_i\}$ por permutaciones de los E_i, es decir, la acción de G sobre A, induce una acción de G sobre el conjunto $\{E_i\}$. Veamos que G actúa transitivamente sobre $\{E_i\}$. Supongamos lo contrario. Consideremos, reordenando los índices si es necesario, para $(1 \leq t < n)$ y $(t < r \leq n)$, la órbita $\{E_1, \ldots, E_t\}$ de E_1 y la órbita $\{E_{t+1}, \ldots, E_r\}$ de E_{t+1}. Entonces, evidentemente, las matrices

$$x_1 = E_1 + \cdots + E_t \quad \text{y} \quad x_2 = E_{t+1} + \cdots + E_r$$

de A, son invariantes bajo G, es decir, $x_1, x_2 \in A^G$. Además, x_1 y x_2 son linealmente independientes sobre k. Pero esto es contradictorio al hecho que $\dim_k A^G = 1$. □

2.3.2 Corolario. *Si A es un álgebra semisimple y G un grupo finito que actúa sobre A tal que $A^G = k$, entonces existen S un subgrupo de G y B una S-álgebra tal que*

$$A \simeq Ind_S^G(B), \text{ como } G\text{-álgebras.}$$

Además, tenemos que B es simple y $B^S = k$.

Demostración. Sean S el estabilizador de E_1 en G y

$$B = E_1 A \simeq M_{r_1}(D_1).$$

Por la Proposición 2.2.4 y el Lema 2.3.1 tenemos que $A \simeq \mathrm{Ind}_S^G(B)$. Además, por el Lema 2.2.5

$$k = A^G \simeq (\mathrm{Ind}_S^G(B))^G \simeq B^S.$$

□

2.3.3 Proposición. *Sean G un grupo finito, S un subgrupo de G y B una S-álgebra. Entonces B es una S-álgebra de Galois sobre k si y sólo si el álgebra inducida $Ind_S^G(B)$ es una G-álgebra de Galois sobre k.*

Demostración. Sea B una S-álgebra simple y de Galois sobre k. La ecuación

$$\dim(\mathrm{Ind}_S^G(B)) = \dim(kG \otimes_{kS} B) = \dim(B)[G:S] = |S|[G:S] = |G|,$$

nos muestra que la dimensión del álgebra inducida por B coincide con el orden de G.

Por el Lema 2.2.5 tenemos que

$$\mathrm{Ind}_S^G(B) \simeq \prod_{i=1}^{[G:S]} B \qquad \text{y} \quad (\mathrm{Ind}_S^G(B))^G = k. \tag{2.12}$$

Dado que el álgebra B es simple, entonces $\mathrm{Ind}_S^G(B)$ es un álgebra semisimple y sean

$$\mathrm{Ind}_S^G(B) \simeq e_1\mathrm{Ind}_S^G(B) \oplus \cdots \oplus e_m\mathrm{Ind}_S^G(B). \tag{2.13}$$

una descomposición de Wedderburn para $\mathrm{Ind}_S^G(B)$ y $\{e_1, \ldots, e_m\}$ su respectivo sistema de Wedderburn, el cual es transitivo bajo la acción de G. Consideremos a

$$J = J_1 \oplus \cdots \oplus J_m \subseteq \mathrm{Ind}_S^G(B),$$

un ideal a izquierda G-invariante y $\{g_1 = e, \ldots, g_m\}$ un conjunto de representantes de las coclases a izquierda de S en G tal que $g_i \cdot e_1 = e_i$. Tenemos que $r \in J_i$ si y sólo si $r \in J$ y

$$r(x) = \begin{cases} s \rightharpoonup r(g_i), & \text{si } x = sg_i \in Sg_i \\ 0, & \text{si } x \notin Sg_i. \end{cases}$$

En particular, $r \in J_1$ si y sólo si $r \in J$ y

$$r(x) = \begin{cases} x \rightharpoonup r(e), & \text{si } x \in S \\ 0, & \text{si } x \notin S. \end{cases}$$

Es evidente que J_1 es un ideal S-invariante de $e_1\mathrm{Ind}_S^G(B) \simeq B$ y

$$J_i = g_i J_1 = \{g_i \cdot r | r \in J_1\}.$$

Entonces J es un ideal nulo o coincide con $\mathrm{Ind}_S^G(B)$.

Recíprocamente, supongamos que $\mathrm{Ind}_S^G(B)$ es una G-álgebra de Galois sobre k. La ecuación

$$|G| = \dim(\mathrm{Ind}_S^G(B)) = \dim(B)[G:S] = \dim(B)\frac{|G|}{|S|},$$

nos muestra que la dimensión del álgebra B coincide con el orden de S. Además,

$$k = \mathrm{Ind}_S^G(B) \simeq B^S.$$

El álgebra $\mathrm{Ind}_S^G(B)$ es semisimple y sea $\{e_1, \ldots, e_m\}$ el sistema de Wedderburn determinado por (2.13). Entonces por el Lema 2.3.1 $\{e_1, \ldots, e_m\}$ es transitivo bajo G y análogamente como en la implicación anterior, consideremos a J un ideal S-invariante y a $\{g_1 = e, \ldots, g_m\}$ un conjunto de representantes de las coclases a izquierda de S en G tal que $g_i \cdot e_1 = e_i$. Afirmamos sin demostrarlo que

$$\tilde{J} = g_1 J \oplus \cdots \oplus g_m J \subseteq \mathrm{Ind}_S^G(B)$$

es un ideal G-invariante. Entonces es nulo o coincide con $\mathrm{Ind}_S^G(B)$. Por lo tanto J es un ideal nulo o coincide con B. □

Resumimos, en el siguiente teorema, los resultados obtenidos hasta ahora.

2.3.4 Teorema. *Sea A una G-álgebra sobre k. Entonces A es de Galois si y sólo si existen S un subgrupo de G que estabiliza un elemento idempotente central en A bajo la acción de G y B una S-álgebra de Galois simple tal que*

$$A \simeq Ind_S^G(B).$$

□

CAPÍTULO 3

Álgebras de Galois simples

El objetivo principal de este capítulo es establecer el teorema principal de este trabajo, esto es, demostrar que toda G-álgebra de Galois simple está determinada de manera biunívoca por un dato asociado (ver Teorema Principal 3.2.19).

A continuación presentamos por secciones, el contenido del capítulo y sus conexiones con el resto del escrito.

- 3.1 Álgebras de Galois simples como álgebras de grupo torcidas: Demostramos que las álgebras de Galois simples son isomorfas a un álgebra de grupo torcida.
- 3.2 G-Álgebras de Galois simples como álgebras de grupo torcidas: Demostramos que las álgebras de Galois simples son isomorfas a un álgebra de grupo torcida, como G-álgebras. Usaremos este resultado para clasificar las álgebras de Galois simples mediante un dato (ver Teorema principal 3.2.19).

En este capítulo así como en el anterior, la mayoría de los resultados son ideas originales del autor y su orientador. Aclaramos que algunos de los resultados en álgebras de Galois sobre anillos conmutativos son tomados de los artículos [Tak65, Kan65].

En este capítulo denotamos por A una G-álgebra de Galois simple con centro el cuerpo K.

3.1. Álgebras de Galois simples como álgebras de grupo torcidas

En esta sección mostramos que toda álgebra de Galois simple es isomorfa como álgebra, a cierta álgebra de grupo torcida.

A continuación presentamos una versión de la acción de Miyashita-Ulbrich para extensiones de Hopf-Galois, aplicada en álgebras de Galois (ver [Sch96]).

Para $g \in G$, consideremos el subespacio de A

$$A_g = \{a \in A | ax = (g \rightharpoonup x)a \text{ para todo } x \in A\}.$$

Algunas observaciones evidentes:

3.1.1 Nota.

i) $A_g A = A A_g$ es un ideal bilateral de A,

ii) A_g es un subespacio de A sobre K,

iii) $A_e = K$.

3.1.2 Lema. *Si $g, h \in G$, entonces*

i) $A_g A_h \subseteq A_{gh}$

ii) $g \rightharpoonup A_h = A_{ghg^{-1}}$

Demostración.

i) Sea $a \in A_g A_h$. Sin perdida de generalidad podemos considerar que existen $a_g \in A_g$ y $a_h \in A_h$ tal que $a = a_g a_h$. Las condiciones $a_g \in A_g$ y $a_h \in A_h$ implican que

$$a_g x = (g \rightharpoonup x)a_g \quad \text{y} \quad a_h x = (h \rightharpoonup x)a_h, \quad \text{para cualquier } x \in A.$$

En particular,

$$a_g a_h = (g \rightharpoonup a_h)a_g. \tag{3.1}$$

Entonces

$$\begin{aligned} ax &= (a_g a_h)x \\ &= (g \rightharpoonup a_h)a_g x \qquad \text{por ecuación (3.1)} \\ &= (g \rightharpoonup a_h)(g \rightharpoonup x)a_g \\ &= (g \rightharpoonup a_h x)a_g \\ &= (g \rightharpoonup (h \rightharpoonup x)a_h)a_g \\ &= (g \rightharpoonup (h \rightharpoonup x))(g \rightharpoonup a_h)a_g \\ &= (gh \rightharpoonup x)a_g a_h \\ &= (gh \rightharpoonup x)a. \end{aligned}$$

ii) Sean $a_h \in A_h$ y $x \in A$, la sucesión de ecuaciones

$$\begin{aligned} (ghg^{-1} \rightharpoonup x)(g \rightharpoonup a_h) &= g \rightharpoonup [(hg^{-1} \rightharpoonup x)a_h] \\ &= g \rightharpoonup [(h \rightharpoonup (g^{-1} \rightharpoonup x))a_h] \\ &= g \rightharpoonup [a_h (g^{-1} \rightharpoonup x)] \\ &= (g \rightharpoonup a_h)x, \end{aligned}$$

muestran que $g \rightharpoonup A_h \subseteq A_{ghg^{-1}}$. Recíprocamente, sean $a \in A_{ghg^{-1}}$ y $x \in A$, la sucesión de ecuaciones

$$\begin{aligned}(g^{-1} \rightharpoonup a)x &= g^{-1} \rightharpoonup (a(g \rightharpoonup x)) \\ &= g^{-1} \rightharpoonup (ghg^{-1} \rightharpoonup (g \rightharpoonup x)a) \\ &= (h \rightharpoonup x)(g^{-1} \rightharpoonup a),\end{aligned}$$

muestra que $g^{-1} \rightharpoonup a \in A_h$, entonces $a \in g \rightharpoonup A_h$.

□

Consideremos la transformación lineal

$$\begin{aligned}\mathrm{Hom}_A(A, A) &\to A^{op} \\ \tau &\mapsto \tau(1),\end{aligned} \tag{3.2}$$

donde A^{op} denota el espacio vectorial A con multiplicación opuesta. Es evidente que la transformación dada en (3.2) es un isomorfismo de álgebras.

En la siguiente proposición usamos ideas originales de Kanzaki en [Kan65, Proposition 1].

3.1.3 Proposición. *Si A es una G-álgebra de Galois sobre k, entonces*

$$A = \bigoplus_{g \in G} A_g.$$

Demostración. Por el isomorfismo $\theta : A \rtimes G \to \mathrm{End}(A)$, podemos identificar a $A \rtimes G$ con $\bigoplus_{g \in G} Ag$, donde $ag : A \to A$ es la transformación lineal $ag(b) = a(g \rightharpoonup b)$. Entonces un elemento ag está en $\mathrm{Hom}_A(A, A)$ si y sólo si

$$\begin{aligned}&ag(xby) = x(ag(b))y \quad (\forall x \in A, b \in A, y \in A^G = k) \\ \leftrightarrow &a(g \rightharpoonup xby) = xa(g \rightharpoonup b)y \quad (\forall x \in A, b \in A, y \in A^G = k) \\ \leftrightarrow &a(g \rightharpoonup x) = xa \quad (\forall x \in A) \\ \leftrightarrow &a \in A_{g-1}.\end{aligned} \tag{3.3}$$

Entonces por la Ecuación (3.3) y el isomorfismo θ tenemos el isomorfismo de álgebras

$$\begin{aligned}\mathrm{Hom}_A(A, A) &\to \bigoplus_{g \in G} A_{g^{-1}} u_g \\ ag &\mapsto au_g.\end{aligned}$$

De otro lado consideremos la transformación lineal

$$\begin{aligned}\bigoplus_{g \in G} A_{g^{-1}} u_g &\to (\bigoplus_{g \in G} A_{g^{-1}})^{op} \\ au_g &\mapsto a,\end{aligned}$$

la cual es un isomorfismo de álgebras. En efecto, sean $a \in A_{g^{-1}}$ y $b \in A_{h^{-1}}$, entonces

$$(au_g)(bu_h) = a(g \rightharpoonup b)u_{gh} \mapsto a(g \rightharpoonup b) = ba = a \cdot_{op} b.$$

Por lo tanto usando el isomorfismo dado en (3.2) tenemos el isomorfismo de álgebras entre A^{op} y $(\bigoplus_{g \in G} A_{g^{-1}})^{op}$, el cual implica la igualdad deseada. □

Consideremos el subgrupo

$$N = \{h \in G | h \rightharpoonup \alpha = \alpha \ \ \forall \alpha \in K\}, \tag{3.4}$$

el cual es normal sobre G. En efecto, sean $g \in G$, $h \in N$ y $\alpha \in K$. Por el Lema 3.1.2 tenemos que $g^{-1} \rightharpoonup \alpha \in A_e = K$, entonces

$$ghg^{-1} \rightharpoonup \alpha = g \rightharpoonup (h \rightharpoonup (g^{-1} \rightharpoonup \alpha)) = \alpha.$$

Llamamos a N el subgrupo **estabilizador del centro de A**.

3.1.4 Lema. *Sea A una G-álgebra de Galois sobre k. Las siguientes proposiciones son equivalentes.*

i) $h \in N$, *el estabilizador del centro de* A.

ii) $A_h \neq 0$.

iii) $A_h A_{h^{-1}} = A_{h^{-1}} A_h = K$.

iv) Existe un elemento invertible en la h*-ésima componente homogénea* A_h.

v) $A_g A_h = A_{gh}$ *para todo* $g \in G$.

Demostración.

i) $\Rightarrow$ *ii)* Sea $h \in N$. Consideremos la transformación lineal

$$\begin{aligned} A \otimes_K A_h &\to A \\ a \otimes x &\mapsto ax, \end{aligned}$$

el cual es un isomorfismo (ver [AG60, Theorem 3.1]), por lo tanto $A_h \neq 0$.

ii) $\Rightarrow$ *iii)* El orden de contenencias $0 \subsetneq A_h \subseteq A_h A$, junto al hecho que $A_h A = A A_h$ es un ideal bilateral en el álgebra simple A implica que $A_h A = A A_h = A$. La ecuación

$$\bigoplus_{g \in G} A_g = A = A_h A = \bigoplus_{g \in G} A_h A_g,$$

nos muestra que $A_h A_{h^{-1}} = A_e = K$. De manera análoga usando que $A A_h = A$ obtenemos que $A_{h^{-1}} A_h = A_e = K$.

iii) $\Rightarrow$ *iv)* Si $A_h A_{h^{-1}} = K$, entonces podemos suponer sin perdida de generalidad que existen $x \in A_h$ y $y \in A_{h^{-1}}$ tal que

$$xy = 1. \tag{3.5}$$

Ahora $A_{h^{-1}} x \subseteq K$ y por la Ecuación (3.5) tenemos que existen $\hat{y} \in A_{h^{-1}}$ y $u \in K$ tal que $\hat{y}x = u \neq 0$. Entonces tomando recíprocos tenemos que $(u^{-1}\hat{y})x = 1$. Por lo tanto x tiene un inverso a derecha e izquierda los cuales deben coincidir, es decir, $xy = yx = 1$ como queríamos demostrar.

iv) $\Rightarrow$ *v)* Ver Notas 1.4.4 y 1.4.2.

$v) \Rightarrow i)$ Supongamos a $x \neq 0$ en A_h y α un elemento cualquiera en K, tenemos que

$$[(h \rightharpoonup \alpha) - \alpha]x = 0.$$

Entonces

$$[(h \rightharpoonup \alpha) - \alpha]K = ([(h \rightharpoonup \alpha) - \alpha]A_h)A_{h^{-1}} = 0.$$

Por lo tanto $(h \rightharpoonup \alpha) - \alpha = 0$ para cualquier $\alpha \in K$, es decir, $h \in N$.

□

Ahora por la Proposición 3.1.3 y el lema anterior tenemos que

$$A = \bigoplus_{h \in N} A_h = \bigoplus_{h \in N} K u_h,$$

donde u_h es un elemento invertible de A_h. Entonces A es un N-producto cruzado y por la Proposición 1.4.9 tenemos que

$$A \simeq K \#_\sigma N,$$

como álgebras, donde el 2-cociclo no degenerado $\sigma : N \times N \to K^\times$ y la acción débil $\pi : G \to \mathrm{Aut}(K)$ vienen dadas por

$$\sigma(x, y) = u_x u_y u_{xy}^{-1} \quad \text{y} \quad \pi(x)(\alpha) = u_x \alpha u_x^{-1} = \alpha,$$

para $x, y \in N$, $\alpha \in K$ y u_x, u_y elementos invertibles en las componentes A_x y A_y respectivamente. Entonces, como π es trivial tenemos que

$$A \simeq K \#_\sigma N = K_\sigma N. \tag{3.6}$$

En resumen,

3.1.5 Proposición. *Toda G-álgebra A de Galois sobre k simple y central sobre K es isomorfa, como álgebra, al álgebra de grupo torcida $K_\sigma N$, donde N es el subgrupo de G que estabiliza a K y $\sigma : N \times N \to K^\times$ es un 2-cociclo no degenerado.*

□

3.2. G-Álgebras de Galois simples como álgebras de grupo torcidas

En la sección anterior mostramos que un álgebra de Galois simple es isomorfa, como álgebra, a un álgebra de grupo torcida $K_\sigma N$, donde σ es un 2-cociclo no degenerado. En esta sección mostramos que el álgebra de grupo torcida $K_\sigma N$ tiene estructura de G-álgebra, representada por un 1-cociclo de Hochschild γ de G a valores en $C^1(N, K^\times)$ (Proposición 3.2.4). Finalmente, demostramos que toda álgebra de Galois simple está en correspondencia biyectiva con G-álgebras de grupo torcida $K_\sigma N$ con G-acción determinada por γ.

Recordemos que A denota un G-álgebra de Galois simple con centro el cuerpo K y N es el subgrupo de G que estabiliza a K. Usando la Proposición 3.1.5, identificamos al álgebra de Galois A con $K_\sigma N$ (Teorema 3.2.19).

3.2.1 Nota. Para $h \in N$, $x \in K_\sigma N$ y $\alpha \in K$, tenemos que

$$h \rightharpoonup \alpha x = \alpha(h \rightharpoonup x).$$

3.2.2 Lema. *Si $h \in N$, entonces*

$$h \rightharpoonup x = u_h x u_h^{-1}$$

para cualquier $x \in K_\sigma N$

Demostración. Para $h \in N$, tenemos que

$$y \in A_h = K u_h \;\leftrightarrow\; yx = (h \rightharpoonup x)y \;\; \forall x \in K_\sigma N$$

Entonces por la Observación 3.2.1 podemos suponer que $y = u_h$ y obtenemos que $h \rightharpoonup x = u_h x u_h^{-1}$, como queríamos demostrar. □

3.2.3 Proposición. *Si A es una G-álgebra de Galois sobre k, entonces K es una extensión de Galois sobre k con grupo de Galois $Gal(K/k) \simeq G/N$.*

Demostración. Ver [Kan65, Proposition 3]. □

Supongamos que $K_\sigma N$ es una G-álgebra de Galois simple y central sobre K. Por la Proposición 3.2.3, K es una extensión de Galois con grupo de Galois $Gal(K/k) \simeq G/N$. Sean $\pi : G \to G/N$ el homomorfismo natural y $\psi : G/N \to Gal(K/k)$, un isomorfismo entre G/N y $Gal(K/k)$ la composición $G \xrightarrow{\pi} G/N \xrightarrow{\psi} Gal(K/k)$ determina la G-acción restringida de A sobre K, esto es,

$$\begin{aligned} G \times K &\to K \\ (g, \alpha) &\mapsto \bar{g}(\alpha), \end{aligned} \tag{3.7}$$

donde $\bar{g}$ es el automorfismo $\psi \circ \pi(g)$.

Conocemos como actúan los elementos de N sobre el álgebra de grupo torcida, nuestro propósito ahora es conocer como actúan los elementos de G sobre el álgebra de grupo torcida. Para $g \in G$ y $\alpha u_x \in A_x$, el ítem *ii*) del Lema 3.1.2 nos muestra que $g \rightharpoonup \alpha u_x \in A_{gxg^{-1}} = K u_{gxg^{-1}}$.
Entonces la acción $\rightharpoonup$ determina una función $\gamma : G \times N \to K^\times$, definida unívocamente (aunque depende de $\bar{g}$) por la siguiente relación:

$$g \rightharpoonup \alpha u_x = (g \rightharpoonup \alpha)(g \rightharpoonup u_x) = \bar{g}(\alpha)\gamma(g, x) u_{{}^g x}, \tag{3.8}$$

para $g \in G$, $x \in N$ y $\alpha \in K$, donde ${}^g x = gxg^{-1}$.

De ahora en adelante en este capítulo, por la Proposición 1.2.12, podemos suponer que el 2-cociclo $\sigma \in Z^2(N, K^\times)$ satisface la condición

$$\sigma(x, y) = \sigma(y^{-1}, x^{-1})^{-1} \quad (\forall x, y \in G),$$

y consideremos la función ϵ_σ, el **signo** del 2-cociclo σ (ver Definición 1.2.14). La siguiente proposición establece condiciones suficientes y necesarias para que la función γ **represente** una acción de G sobre $K_\sigma N$.

3.2.4 Proposición. *La función definida en la Ecuación* (3.8) *es una acción de G sobre $K_\sigma N$ si y sólo si $\gamma : G \times N \to K^\times$ cumple las siguientes condiciones:*

i) Para $g, h \in N$,

$$\gamma(g,h) = \epsilon_\sigma(g)\sigma(g,h)\sigma(gh, g^{-1}). \tag{C1}$$

ii) Para $g \in G$ y $x, y \in N$,

$$\bar{g}(\sigma(x,y))\gamma(g,xy) = \sigma({}^g x, {}^g y)\gamma(g,x)\gamma(g,y). \tag{C2}$$

iii) Para $x, y \in G$ y $h \in N$,

$$\gamma(xy,h) = \bar{x}(\gamma(y,h))\gamma(x, {}^y h). \tag{C3}$$

Demostración. Para $g, h \in N$ y $\alpha \in K$, la condición (C1) es equivalente a la condición

$$g \rightharpoonup \alpha u_h = u_g(\alpha u_h)u_g^{-1}.$$

Para $g \in G$, $x, y \in N$ y $\alpha, \beta \in K$, la condición (C2) es equivalente a la condición

$$g \rightharpoonup (\alpha u_x)(\beta u_y) = (g \rightharpoonup \alpha u_x)(g \rightharpoonup \beta u_y).$$

Para $x, y \in G$, $h \in N$ y $\alpha, \beta \in K$, la condición (C3) es equivalente a la condición

$$x \rightharpoonup (y \rightharpoonup \alpha u_h) = xy \rightharpoonup (\alpha u_h).$$

□

3.2.5 Nota.

i) Si $g = e$ en (C1) tenemos que

$$\gamma(e,h) = \epsilon_\sigma(e)\sigma(e,h)\sigma(h,e) = 1.$$

ii) Si $x = y = e$ en (C2) tenemos que

$$\gamma(g,e) = \gamma(g,e)\gamma(g,e) \Rightarrow \gamma(g,e) = 1.$$

Escribamos de una manera diferente las condiciones dadas para γ. Consideremos el grupo abeliano de las 1-cadenas **normalizadas**, es decir, funciones $f : N \to K^\times$ de N con valores en $K^\times$ tal que $f(e) = 1$. Denotamos a este grupo abeliano por $C^1(N, K^\times)$, esto es,

$$C^1(N, K^\times) = \{f : N \to K^\times | f(e) = 1\}.$$

$C^1(N, K^\times)$ es un G-bimódulo con acción a izquierda definida por

$$(g \rightharpoonup f)(x) = \bar{g}(f(x)) \tag{3.9}$$

y acción a derecha definida por

$$(f \leftharpoonup g)(x) = f({}^g x) \tag{3.10}$$

para $g \in G, x \in N$ y $f \in C^1(N, K^\times)$.

3.2.6 Nota. Existe una correspondencia biyectiva entre funciones $\gamma : G \times N \to K^\times$ tal que

$$\gamma(e,h) = \gamma(g,e) = 1 \ \ \forall g \in G, h \in H$$

y funciones $\tilde{\gamma} : G \to C^1(N, K^\times)$ tal que $\tilde{\gamma}(e) = 1$.

3.2.7 Lema. *Usando la correspondencia de la Observación 3.2.6, una función $\gamma : G \to C^1(N, K^\times)$ con $\gamma(e) = 1$ satisface las condiciones* (C1), (C2) *y* (C3) *si y sólo si $\gamma : G \to C^1(N, K^\times)$ es un 1-cociclo de Hochschild normalizado que satisface las condiciones* (C1) *y* (C2).

Demostración. Para $x, y \in G, h \in N$, la ecuación

$$\begin{aligned}\gamma(xy)(h) &= [(x \rightharpoonup \gamma(y))(h)][(\gamma(x) \leftharpoonup y)(h)] \\ &= \bar{x}(\gamma(y)(h))\gamma(x)({}^y h) \\ &= \bar{x}(\gamma(y,h))\gamma(x, {}^y h),\end{aligned}$$

muestra que la condición de 1-cociclo de Hochschild es equivalente a la condición (C3). □

3.2.8 Definición. Sea $\gamma : G \to C^1(N, K^\times)$ un 1-cociclo de Hochschild, decimos que γ **representa la acción de G sobre $K_\sigma N$** si γ satisface las condiciones (C1) y (C2).

3.2.9 Definición. Sean G un grupo finito y k un cuerpo. Un **dato de G-álgebra de Galois simple sobre k**, o simplemente un **dato asociado a G y k**, es una colección (K, N, σ, γ) tal que

i) N es un subgrupo normal de G.

ii) $K \supseteq k$ es una extensión de Galois con grupo de Galois G/N.

iii) $\mathrm{char}(K) \nmid |N|$.

iv) $\sigma : N \times N \to K^\times$ es un 2-cociclo no degenerado.

v) $\gamma : G \to C^1(N, K^\times)$ es un 1-cociclo de Hochschild que representa la acción de G sobre $K_\sigma N$.

Sea (K, N, σ, γ) un dato asociado a G y k. Denotemos por $A(K_\sigma N, \gamma)$ a el álgebra de grupo torcida $K_\sigma N$ junto a la acción de G sobre $K_\sigma N$ definida en la Ecuación (3.8).

3.2.10 Proposición. *Sea (K, N, σ, γ) un dato asociado a G y k. La G-álgebra $A(K_\sigma N, \gamma)$ es:*
i) Un álgebra simple y central sobre K.
ii) Una G-álgebra de Galois sobre k.

Antes de demostrar la proposición dos resultados previos.

3.2.11 Proposición. *Sea A un álgebra simple y central sobre K. Entonces A es una G-álgebra de Galois sobre k si y sólo si A es una N-álgebra de Galois sobre K y K es una extensión de Galois sobre k con grupo de Galois G/N.*

Demostración. Ver [Tak65, Theorem 2]. □

3.2.12 Lema. *Si A es un álgebra simple y central sobre K, entonces la transformación lineal*

$$\begin{aligned} A \otimes_K A^{op} &\to \mathrm{End}_K(A) \\ a \otimes b &\mapsto [x \mapsto axb] \end{aligned}$$

es un isomorfismo.

Demostración. Ver [GS06, pag. 32]. □

Demostración Proposición 3.2.10. Denotemos por A a la G-álgebra $A(K_\sigma N, \gamma)$ y demostremos que A es una N-álgebra de Galois sobre K. Con este fin veamos que el homomorfismo $\theta_N : A \rtimes N \to \mathrm{End}_K(A)$, definido por $\theta_N(a\#h)(b) = a(h \rightharpoonup b)$ tiene la forma del isomorfismo en el Lema 3.2.12. En efecto, para $g, h \in N$ y $x \in A$ la sucesión de igualdades

$$\begin{aligned} \theta(u_g u_h \# h^{-1})(x) &= u_g u_h (h^{-1} \rightharpoonup x) \\ &= u_g u_h (u_{h^{-1}} x (u_{h^{-1}})^{-1}) \\ &= u_g \epsilon_\sigma(h) x \epsilon_\sigma(h^{-1}) u_h \\ &= u_g \epsilon_\sigma(h)^2 x u_h \\ &= u_g x u_h, \end{aligned}$$

así lo demuestran. Por lo tanto el homomorfismo θ es sobreyectivo. Además

$$\dim_K(A \rtimes N) = |N|^2 = \dim_K(\mathrm{End}_K(A)),$$

entonces el homomorfismo θ es un isomorfismo. El resultado de la proposición se sigue aplicando la Proposición 3.2.11. □

3.2.13 Definición. Decimos que dos datos (K, N, σ, γ) y $(K', N', \sigma', \gamma')$ asociados a G y k son **equivalentes** si existe un isomorfismo de G-álgebras entre $A(K_\sigma N, \gamma)$ y $A(K'_{\sigma'} N', \gamma')$.

Si $f : A \to A'$ es un isomorfismo de G-álgebras entre $A = A(K_\sigma N, \gamma)$ y $A' = A(K'_{\sigma'} N', \gamma')$, definido por $f(\alpha u_x) = \alpha' v_{x'}$, donde $\alpha' \in K'$ y $v_{x'}$ es un elemento invertible en la componente x'-homogéneo para $x' \in N'$. Es evidente que los elementos del centro de A están en correspondencia biunívoca con los elementos del centro de A', esto es, $K \simeq K'$. Además el isomorfismo f produce un isomorfismo de grupos

$$\begin{aligned} \hat{f} : N &\to N' \\ x &\mapsto x', \end{aligned}$$

entre N y N'. En resumen,

3.2.14 Lema. *Si (K, N, σ, γ) y $(K', N', \sigma', \gamma')$ son equivalentes, entonces $K \simeq K'$ y $N \simeq N'$. Es decir, el centro del álgebra y el subgrupo estabilizador del centro se mantienen bajo isomorfismos.*

□

Por lo tanto,

3.2.15 Proposición. *Si $K \simeq K'$ y $N \simeq N'$. Entonces los 2-cociclos σ y σ' están en la misma clase de cohomología si y sólo si existe un isomorfismo f de N-álgebras graduadas tal que el diagrama*

$$\begin{array}{ccc} K & \longleftrightarrow & K' \\ \downarrow & & \downarrow \\ K\#_\sigma N & \xrightarrow[f]{} & K'\#_{\sigma'} N' \end{array} \tag{3.11}$$

conmuta.

Demostración. Su demostración es análoga a la de la Proposición 1.4.12. □

La siguiente definición nos da una condición para saber cuando dos 1-cociclos de Hochschild $\gamma : G \to C^1(N, K^\times)$ y $\gamma' : G \to C^1(N, K^\times)$ representan la misma acción de G sobre $K_\sigma N$:

3.2.16 Definición. Sean $\gamma : G \to C^1(N, K^\times)$ y $\gamma' : G \to C^1(N, K^\times)$. Decimos que γ es **equivalente** a γ' si existen un automorfismo $\omega : K \to K$ que pertenezca al centro del grupo de Galois $Gal(K/k)$ y una función $\eta : N \to K^\times$ tal que para cualesquiera $x, y \in N$ y $g \in G$ tenemos que

$$\begin{aligned} \omega(\sigma(x,y))\eta(xy) &= \eta(x)\eta(y)\sigma(x,y), \\ \omega(\gamma(g,x))\eta({}^g x) &= \bar{g}(\eta(x))\gamma'(g,x). \end{aligned} \tag{3.12}$$

3.2.17 Proposición. *Sean (K, N, σ, γ) y $(K', N', \sigma', \gamma')$ dos datos asociados a G y k. Entonces los datos (K, N, σ, γ) y $(K', N', \sigma', \gamma')$ son equivalentes si y solo $K \simeq K'$, $N \simeq N'$, γ es equivalente a γ' y los 2-cociclos σ y σ' están en la misma clase de cohomología de grupos.*

Demostración. Por el Lema 3.2.14 y la Proposición 3.2.15 podemos suponer que $K = K'$, $N = N'$ y $\sigma = \sigma'$. Demostremos que γ y γ' son equivalentes si y sólo si la G-álgebra $K_\sigma N$ con acción

$$g \rightharpoonup \alpha u_x = \bar{g}(\alpha)\gamma(g,x)u_{gx} \quad (g \in G, x \in N, \alpha \in K),$$

denotada A, es isomorfa a la G-álgebra $K_\sigma N$ con acción

$$g \rightharpoonup \alpha u_x = \bar{g}(\alpha)\gamma'(g,x)u_{gx} \quad (g \in G, x \in N, \alpha \in K),$$

denotada A'. Supongamos que γ y γ' son equivalentes, y consideremos el isomorfismo lineal $f : A \to A'$, definido por $f(\alpha u_x) = \omega(\alpha)\eta(x)u_x$. Dejamos al lector la verificación que f es un isomorfismo de álgebras. Veamos que f es un isomorfismo de G-álgebras:

$$\begin{aligned} f(g \rightharpoonup \alpha u_x) &= f(\bar{g}(\alpha)\gamma(g,x)u_{gx}) \\ &= \omega(\bar{g}(\alpha)\gamma(g,x))\eta({}^g x)u_{gx} \\ &= \bar{g}(\omega(\alpha))\omega(\gamma(g,x))\eta({}^g x)u_{gx} \\ &= \bar{g}(\omega(\alpha))\bar{g}(\eta(x))\gamma'(g,x)u_{gx} \\ &= g \rightharpoonup(\omega(\alpha)\eta(x)u_x) \\ &= g \rightharpoonup f(\alpha u_x). \end{aligned}$$

Recíprocamente, supongamos que f es un isomorfismo de G-álgebras entre A y A'. Consideremos a $\omega = f|_K$ y $\eta : N \to K^\times$ determinada por la función f, esto es, tal que $f(u_x) = \eta(x)u_x$, para todo $x \in N$. Entonces realizando un procedimiento análogo como en la implicación anterior, demostramos que γ y γ' satisfacen las ecuaciones en (3.12). □

Antes de enunciar y demostrar nuestro teorema principal, veamos un resultado previo.

3.2.18 Lema. *Si $K_\sigma N$ es una G-álgebra de Galois sobre k, entonces $char(K) \nmid |N|$. En particular, $char(k) \nmid |N|$.*

Demostración. Por la Proposición 3.2.11 $K_\sigma N$ es una N-álgebra de Galois sobre K y consideremos el isomorfismo

$$\theta_N : K_\sigma N \rtimes G \to \mathrm{End}(K_\sigma N),$$

definido por $\theta_N(\alpha u_x \# y)(\beta u_z) = \alpha u_x(y \rightharpoonup \beta u_z)$. Sea $\sum_{y\in N} u_e \# y$ un elemento no nulo en $K_\sigma N \rtimes G$. Veamos que $\theta_N(\sum_{y\in N} u_e \# y)(u_h) = \sum_{y\in N} u_y u_h u_y^{-1}$ está en el centro del álgebra de grupo torcida. En efecto, sea u_x un elemento invertible en A_h, el cual, sin perdida de generalidad (extendiendo el cuerpo, si es necesario, a una clausura algebraica), podemos considerar con **signo positivo**, es decir, $\epsilon_\sigma(x) = 1$, entonces

$$\begin{aligned}
&u_x(\sum_{y\in N} u_y u_h u_y^{-1}) \\
&\quad = \sum_{y\in N} u_x u_y u_h u_y^{-1} \\
&\quad = \sum_{y\in N} \epsilon_\sigma(y)\sigma(x,y) u_{xy} u_h u_{y^{-1}} \\
&\quad = \sum_{t\in N} \epsilon_\sigma(x^{-1}t)\sigma(x,x^{-1}t) u_t u_h u_{t^{-1}x} && (t = xy) \\
&\quad = \sum_{t\in N} \epsilon_\sigma(xt^{-1})\sigma(x,x^{-1}t)\sigma(x^{-1},t) u_t u_h u_{t^{-1}} u_x && \text{(Proposición 1.2.12)} \\
&\quad = (\sum_{t\in N} \epsilon_\sigma(x)\epsilon_\sigma(t) u_t u_h u_{t^{-1}}) u_x \\
&\quad = \epsilon_\sigma(x)(\sum_{t\in N} u_t u_h u_t^{-1}) u_x \\
&\quad = (\sum_{t\in N} u_t u_h u_t^{-1}) u_x
\end{aligned}$$

Como la dimensión del centro es igual a 1, $Z(K_\sigma N) = K u_e$, entonces $\theta_N(\sum_{y\in N} u_e \# y)(u_h) = 0$ si $h \neq e$ y $\theta_N(\sum_{y\in N} u_e \# y)(u_e) = |N| u_e$ elemento no nulo del álgebra de grupo torcida, por lo tanto $|N| \neq 0$. □

3.2.19 Teorema (Principal)**.** *Sean G un grupo, k un cuerpo y A una k-álgebra simple. Entonces A es una G-álgebra de Galois sobre k si y sólo si existe un dato (K, N, σ, γ) asociado a G y k tal que*

$$A \simeq A(K_\sigma N, \gamma).$$

Demostración. Supongamos que A es una G-álgebra de Galois sobre k. Como A es simple, sean $K = Z(A)$ y $N = \{g \in G | g \rightharpoonup \alpha = \alpha \quad \forall \alpha \in K\}$. Por la Proposición 3.1.5 A es un N-producto cruzado y es isomorfa, como álgebra, al álgebra de grupo torcida $K_\sigma N$, donde $\sigma : N \times N \to K^\times$ es un 2-cociclo en la cohomología de grupos abelianos, aquí N actúa sobre $K^\times$ de manera trivial. Por el Corolario 1.6.4 el 2-cociclo σ es no degenerado. Por el Lema 3.2.18 $\mathrm{char}(K) \nmid |N|$. Ahora definimos la función γ determinada por la acción $\rightharpoonup$ como en la Ecuación (3.8), esto es,

$$g \rightharpoonup \alpha u_x = \bar{g}(\alpha)\gamma(g, x)u_{gx},$$

donde $\bar{g}$ es la acción de G sobre el cuerpo K definida en la Ecuación (3.7). Por la Proposición 3.2.4 γ satisface las condiciones (C1), (C2) y (C3) y esto a su vez se tiene si y sólo si γ representa la acción de G sobre $K_\sigma N$, Lema 3.2.7. Entonces (K, N, σ, γ) es un dato asociado a G y k y tenemos que

$$A \simeq A(K_\sigma N, \gamma)$$

como G-álgebras, como se quería demostrar. □

El siguiente teorema es el resultado principal de nuestro trabajo.

3.2.20 Teorema. *Sean G un grupo finito y k un cuerpo. Entonces A es una G-álgebra de Galois sobre k si y sólo si existen S un subgrupo de G que estabiliza un elemento idempotente central en A y (K, N, σ, γ) un dato asociado a S y k tal que A es isomorfa a $Ind_S^G(B)$,*

$$A \simeq Ind_S^G(B),$$

donde B es la S-álgebra simple $A(K_\sigma N, \gamma)$.

Demostración. Supongamos que A es una G-álgebra de Galois sobre k. Entonces A es semisimple y sean $e_1, e_2, \ldots, e_n$ un sistema de elementos idempotentes centrales de A. Consideremos el subgrupo $S = \{s \in G | s \rightharpoonup e_1 = e_1\}$, entonces por el Teorema 2.3.4 tenemos que

$$A \simeq \mathrm{Ind}_S^G(B),$$

para B una S-álgebra de Galois simple sobre k. Usando la caracterización de las álgebras simples dado en el Teorema principal 3.2.19, tenemos que existe un dato (K, N, σ, γ) asociado S y k tal que $B \simeq A(K_\sigma N, \gamma)$.

Recíprocamente si $A \simeq \mathrm{Ind}_S^G(B)$ con $A = A(K_\sigma N, \gamma)$ tenemos que A es una G-álgebra de Galois. □

CAPÍTULO 4

Deformaciones de Grupos finitos

El objetivo principal de este capítulo es presentar una correspondencia entre álgebras de Galois y deformaciones de grupos finitos (ver Proposición 4.4.6). De acuerdo a esta correspondencia y usando los resultados del Capítulo 3, podemos obtener una correspondencia entre deformaciones y datos asociados (ver Proposición 4.4.7).

A continuación presentamos por secciones, el contenido del capítulo y sus conexiones con el resto del escrito.

- 4.1 Biálgebras y álgebras de Hopf: Presentamos de manera sucinta las nociones de biálgebra y álgebra de Hopf. Usaremos de manera sistemática en los capítulos 4 y 5, estas nociones y algunos resultados en álgebras de Hopf.
- 4.2 Acciones y coacciones de álgebras de Hopf sobre álgebras: Presentamos la noción de coacción de un álgebra de Hopf sobre un álgebra, concepto que generaliza la noción de acción de un grupo sobre un álgebra. Usaremos este concepto para definir extensiones de Hopf-Galois de la sección 4.3.
- 4.3 Extensiones de Hopf-Galois: Presentamos la noción de extensión de Hopf-Galois, concepto que generaliza las álgebras de Galois del capítulo 3. Usaremos los resultados de esta sección para establecer una correspondencia entre extensiones de Hopf-Galois y deformaciones de un álgebra de Hopf por un 2-cociclo de Hopf (ver Sección 4.4).
- 4.4 Deformaciones de grupos finitos: Presentamos la noción de deformación de un álgebra de Hopf por un 2-cociclo de Hopf. En particular, si $H = (kG)^* = \mathrm{Hom}(kG, k)$ obtenemos una deformación de grupo finito.

Como referencia para este capítulo están los artículos [Mov94, GN08] y los libros [DNR01, Mon93].

4.1. Biálgebras y álgebras de Hopf

Tomando como referencia los libros [DNR01] y [Mon93], en esta sección presentamos algunos conceptos y resultados básicos sobre álgebras de Hopf.

A lo largo de esta sección y del capítulo denotamos por H un espacio vectorial sobre k y por A, como es usual en el trabajo, un álgebra sobre k.

4.1.1 Proposición. *Supongamos que H esta provisto de una estructura de álgebra (H, m, u) y una estructura de coálgebra (H, Δ, ε). Las siguientes dos afirmaciones son equivalentes:*

i) Las funciones m y u son morfismos de coálgebras.

ii) Las funciones Δ y ε son morfismos de álgebras.

Demostración. Ver [DNR01, Proposition 4.1.1] □

4.1.2 Nota. En notación de Sweedler la condición *ii)* impuesta sobre Δ y ε es expresada como:

$$(cd)_{(1)} \otimes (cd)_{(2)} = c_{(1)}d_{(1)} \otimes c_{(2)}d_{(2)},$$
$$\varepsilon(cd) = \varepsilon(c)\varepsilon(d) \quad (c, d \in H),$$
$$\Delta(1) = 1 \otimes 1.$$

4.1.3 Definición. Una **biálgebra** sobre k es un espacio vectorial H, provisto de una estructura de álgebra (H, m, u) y de una estructura de coálgebra (H, Δ, ε) tales que las transformaciones lineales m y u son morfismos de coálgebras (o equivalentemente, por la Proposición (4.1.1), Δ y ε son morfismos de álgebras).

Sean H y L dos biálgebras. Una transformación lineal $f : H \to L$ es un **morfismo de biálgebras** si $f : H \to L$ es un morfismo de álgebras y coálgebras.

A continuación presentamos algunos ejemplos de biálgebras (ver [DNR01, Section 4.1]).

4.1.4 Ejemplo.

i) Sea G un grupo con unidad e. El álgebra de grupo

$$kG = \left\{ \sum_{g \in G} \alpha_g u_g | \alpha_g \in k, \alpha_g \neq 0 \text{ para finitos } g \in G \right\}$$

sobre el cuerpo k, es una biálgebra con operaciones:

$$m(u_g \otimes u_h) = u_{gh} \qquad u(1) = u_e$$
$$\Delta(u_g) = u_g \otimes u_g \qquad \varepsilon(u_g) = 1$$

para $g, h \in G$.

ii) Sea G un grupo finito con unidad e. El espacio $(kG)^* = \mathrm{Hom}(kG, k)$ de los homomorfismos lineales de kG en k con adición puntual y multiplicación puntual es un álgebra conmutativa. Usando el isomorfismo natural

$$(kG)^* \otimes (kG)^* \to (kG \times kG)^*$$
$$f \otimes h \mapsto f \otimes h = [(x, y) \mapsto f(x)h(y)],$$

obtenemos que $(kG)^*$ es una biálgebra con comultiplicación y counidad dadas por:

$$\Delta(\phi)(g, h) = \phi(gh) \quad \varepsilon(\phi) = \phi(e)$$

para $g, h \in G$ y $\phi \in (kG)^*$.

iii) Sea L un álgebra de Lie con corchete de Lie $[\ ,\ ]$. El álgebra envolvente universal de L es el álgebra cociente $U(L) = T(L)/I$, donde $T(L) = \bigoplus_n L^{\otimes n}$ ($L^0 = k$, $L^{\otimes n} = L^{\otimes n-1} \otimes L$) es el álgebra tensorial de L e I es el ideal bilateral de $T(L)$ generado por los elementos de la forma

$$[x, y] - x \otimes y + y \otimes x \qquad (x, y \in L).$$

El álgebra $U(L)$ es una biálgebra con comultiplicación y counidad determinados por:

$$\Delta(x) = x \otimes 1 + 1 \otimes x \qquad \varepsilon(x) = 0$$

para $x \in L$ (por la propiedad universal de $U(L)$ las operaciones se pueden extender a todo $U(L)$). Note que aquí $\varepsilon(\alpha) = \alpha$ para $\alpha \in k$.

Un ejemplo importante de biálgebras son las álgebras de Hopf, trascendentes en nuestro trabajo.

Sean (C, Δ, ε) una coálgebra y (A, m, u) un álgebra. El espacio vectorial $\mathrm{Hom}(C, A)$ de transformaciones lineales de C en A, posee una estructura de álgebra sobre k, con producto $f * g = m(f \otimes g)\Delta$, para $f, g \in \mathrm{Hom}(C, A)$, el cual llamamos **producto convolución**. En notación de Sweedler el producto convolución tiene la forma:

$$(f * g)(c) = f(c_{(1)})g(c_{(2)}) \qquad (c \in C).$$

4.1.5 Lema. *El producto convolución es asociativo con elemento unidad* $u\varepsilon \in \mathrm{Hom}(C, A)$. *Por lo tanto* $(\mathrm{Hom}(C, A), *)$ *es un álgebra sobre* k.

Demostración. En efecto, para $f, g, h \in \mathrm{Hom}(C, A)$ y $c \in C$ tenemos que

$$\begin{aligned}
&((f * g) * h)(c) \\
&= (f * g)(c_{(1)})h(c_{(2)}) \\
&= f((c_{(1)})_{(1)})g((c_{(1)})_{(2)})h(c_{(2)}) \qquad \text{(asociatividad de } m\text{)} \\
&= f(c_{(1)})g((c_{(2)})_{(1)})h((c_{(2)})_{(2)}) \qquad \text{(coasociatividad de } \Delta\text{)} \\
&= f(c_{(1)})(g * h)(c_{(2)}) \\
&= (f * (g * h))(c).
\end{aligned}$$

Además,

$$f * (u\varepsilon)(c) = f(c_{(1)})u\varepsilon(c_{(2)}) = f(c_{(1)})\varepsilon(c_{(2)})1 = f(c).$$

Similarmente, $(u\varepsilon) * f = f$. □

4.1.6 Definición (Álgebra de Hopf)**.** Sea H una biálgebra. Decimos que H es un **álgebra de Hopf** si existe $S \in \mathrm{Hom}(H, H)$ que es una inversa a derecha e izquierda del homomorfismo identidad id_H de H con respecto al producto convolución. En este caso decimos que S es una **antípoda** de H. En notación de Sweedler la condición impuesta para la antípoda es:

$$S(h_{(1)})h_{(2)} = \varepsilon(h)1_H = h_{(1)}S(h_{(2)}) \qquad (\forall h \in H).$$

Sean H y K álgebras de Hopf. Una transformación lineal $f : H \to K$ es un **morfismo de álgebras de Hopf** si f es un morfismo de biálgebras.

La siguiente observación pone de manifiesto que todo morfismo de álgebras de Hopf conserva las antípodas (ver [DNR01, Proposition 4.2.5]).

4.1.7 Nota. Si $f : H \to K$ es un morfismo de álgebras de Hopf, entonces f preserva la antípoda, es decir, $f(S_H(h)) = S_K(f(h))$ para todo $h \in H$.

4.1.1. Ejemplos de Álgebras de Hopf

A continuación presentamos algunos ejemplos de álgebras de Hopf (ver [DNR01, Section 4.3]).

4.1.8 Ejemplo.

i) Sea G un grupo con unidad e. El álgebra de grupo kG, es un álgebra de Hopf con antípoda definida por:

$$S(u_g) = u_{g^{-1}} \quad (g \in G).$$

ii) Sea G un grupo finito con unidad e. La biálgebra $(kG)^*$ de los homomorfismos lineales de kG en k, es un álgebra de Hopf con antípoda definida por:

$$S(\phi)(g) = \phi(g^{-1}) \quad (g \in G, \phi \in (kG)^*).$$

iii) Sea L un álgebra de Lie con producto de Lie $[\ ,]$. El álgebra $U(L)$ envolvente universal de L es un álgebra de Hopf con antípoda definida por:

$$S(x) = -x \quad (x \in L).$$

4.2. Acciones y coacciones de álgebras de Hopf sobre álgebras

En esta sección presentamos las nociones de acciones y coacciones, fundamentales para definir extensiones de Hopf-Galois. Como referencia están los libros de [DNR01, Mon93].

Suponemos de ahora en adelante que H denota un álgebra de Hopf sobre k y, como es usual, A denota un álgebra sobre k.

4.2.1 Definición. Decimos que H **actúa a izquierda** sobre A (o A es un H**-módulo álgebra**) si las siguientes condiciones se satisfacen:

$(MA1)$ A es un H-módulo a izquierda, con morfismo estructura

$$H \otimes A \to A, \quad h \otimes a \mapsto h \cdot a.$$

$(MA2)$ $h \cdot (ab) = (h_{(1)} \cdot a)(h_{(2)} \cdot b), \qquad \forall h \in H \text{ y } a, b \in A.$

$(MA3)$ $h \cdot (1_A) = \varepsilon(h)1_A$, para todo $h \in H$.

Si solo las condiciones $(MA2)$ y $(MA3)$ se satisfacen, decimos que H es una **medida** para A.

4.2.2 Proposición. *Sea A un H-módulo a izquierda. Entonces A es un H-módulo álgebra si y sólo si la multiplicación en A, $m_A(a \otimes b) = ab$, es un morfismo de H-módulos, donde $A \otimes A$ es un H-módulo a izquierda con $h \cdot (a \otimes b) = (h_{(1)} \cdot a) \otimes (h_{(2)} \cdot b)$.*

Demostración. Ver [DNR01, Proposition 6.1.4]. □

4.2.3 Definición. Sea A un H-módulo álgebra. El subespacio

$$A^H = \{a \in A | h \cdot a = \varepsilon(h)a \ \ \forall h \in H\}$$

es una subálgebra de A, llamada la **subálgebra de invariantes** de A.

4.2.4 Definición. Si A es un H-módulo álgebra, el **producto semidirecto** entre A y H, denotado $A\#H$ es, como espacio vectorial, $A\#H = A \otimes H$, junto a la operación (denotamos $a \otimes b$ por $a\#b$)

$$(a\#h)(b\#g) = a(h_{(1)} \cdot b)\#h_{(2)}g. \tag{4.1}$$

4.2.5 Proposición. *El producto semidirecto $A\#H$ con multiplicación definida por la Ecuación* (4.1) *es un álgebra sobre k.*

Demostración. Ver [DNR01, Proposition 6.1.7]. □

A continuación presentamos una generalización del producto semidirecto usando "2-cociclos de Hopf":

4.2.6 Definición. Supongamos que H es una medida para A y $\alpha : H \otimes H \to A$ es un homomorfismo lineal invertible con respecto al producto convolución. Denotamos por $A\#_\alpha H$ al espacio vectorial $A \otimes H$, junto a la operación $(A \otimes H) \otimes (A \otimes H) \to (A \otimes H)$, definida por

$$(a\#h)(b\#g) = a(h_{(1)} \cdot b)\alpha(h_{(2)}, g_{(1)})\#h_{(3)}g_{(2)}, \tag{4.2}$$

donde denotamos $a \otimes h$ por $a\#h$.

4.2.7 Proposición. *El espacio vectorial $A\#_\alpha H$ es un álgebra con unidad $1_A\#1_H$ si y sólo si las siguientes dos condiciones se satisfacen:*

*i) A es un H-**módulo torcido**; esto es, $1 \cdot a = a$, para todo $a \in A$ y*

$$h \cdot (l \cdot a) = \alpha(h_{(1)}, l_{(1)})(h_{(2)}l_{(2)} \cdot a)\alpha(h_{(3)}, l_{(3)}), \tag{4.3}$$

para $h, l \in H$ y $a \in A$.

*ii) α es un **2-cociclo de Hopf**; esto es, $\alpha(x, 1) = \alpha(1, x) = \varepsilon(x)1$, para $x \in H$, y*

$$[x_{(1)} \cdot \alpha(y_{(1)}, z_{(1)})]\alpha(x_{(2)}, y_{(2)}z_{(2)}) = \alpha(x_{(1)}, y_{(1)})\alpha(x_{(2)}y_{(2)}, z), \tag{4.4}$$

para $x, y, z \in H$.

*En este caso llamamos a $A\#_\alpha H$ el **producto cruzado entre A y H**.*

4.2.8 Nota. Si $\alpha : H \otimes H \to A$ es un 2-cociclo de Hopf trivial, esto es, $\alpha(x, y) = \varepsilon(x)\varepsilon(y)1_A$, entonces el producto cruzado $A\#_\alpha H$ entre A y H es el producto semidirecto $A\#H$ entre A y H.

A continuación damos algunos ejemplos de acciones de álgebras de Hopf sobre álgebras (ver [DNR01, Section 6.1]).

4.2.9 Ejemplo.

i) Si H es un álgebra de Hopf, entonces $H^* = \mathrm{Hom}(H, k)$ es un H-módulo álgebra con acción definida por $(h \rightharpoonup f)(g) = f(gh)$ para $h, g \in H$ y $f \in H^*$.

ii) Sean G un grupo finito y A una G-álgebra sobre k. El álgebra de grupo $H = kG$ (que es un álgebra de Hopf, ver 4.1.1) actúa, de manera natural, sobre A. Entonces A es un H-módulo álgebra como se puede verificar fácilmente. En este caso tenemos que $A\#H = A \rtimes G$ es el producto semidirecto entre A y G como se definió en (1.4.13) y tenemos que $A^H = A^G$ es el álgebra de elementos fijos por G.

Para H un álgebra de Hopf y A un álgebra dualizamos el concepto de módulo álgebra.

4.2.10 Definición. Decimos que H **coactúa a derecha** sobre A (o A es un H**-comódulo álgebra**) si las siguientes condiciones se satisfacen:

$(CA1)$ A es un H-comódulo a derecha, con morfismo estructura

$$\rho : A \to A \otimes H, \quad \rho(a) = a_{(0)} \otimes a_{(1)},$$

$(CA2)$ $(ab)_{(0)} \otimes (ab)_{(1)} = a_{(0)}b_{(0)} \otimes a_{(1)}b_{(1)}, \quad \forall a, b \in A,$

$(CA3)$ $\rho(1) = 1_A \otimes 1_H$.

4.2.11 Proposición. *Sea A un H-comódulo a derecha con morfismo estructura $\rho : A \to A \otimes H$. Las siguientes afirmaciones son equivalentes:*

i) *A es un H-comódulo álgebra.*

ii) *ρ es un morfismo de álgebras.*

iii) *La multiplicación y la unidad de A son morfismos de comódulos.*

Demostración. Ver [DNR01, Proposition 6.2.2]. □

4.2.12 Definición. Sea A un H-comódulo a derecha, con ρ morfismo de estructura. El subespacio

$$A^{coH} = \{a \in A | \rho(a) = a \otimes 1\} \subseteq A,$$

es una subálgebra de A, llamada la **subálgebra de coinvariantes** de A.

A continuación damos algunos ejemplos de coacciones de álgebras de Hopf sobre álgebras (ver [DNR01, Section 6.2])

4.2.13 Ejemplo.

i) Cualquier álgebra de Hopf H es un H-comódulo álgebra sobre si misma, con morfismo estructura Δ. Calculemos H^{coH}. Si $h \in H^{coH}$, tenemos que $\Delta(h) = h_{(1)} \otimes h_{(2)} = h \otimes 1$. Aplicando $\mathrm{id} \otimes \varepsilon$ en ambos lados de la igualdad, obtenemos que $h = \varepsilon(h)1$, por lo tanto $H^{coH} \subseteq k1$. Similarmente obtenemos la otra inclusión, entonces $H^{coH} = k1$.

ii) Sean G un grupo arbitrario con unidad e, y A una álgebra graduada de tipo G, $A = \bigoplus_{g\in G} A_g$. Entonces A es un kG-comódulo álgebra con morfismo estructura dado por:

$$\rho : A \to A \otimes kG, \quad \rho(a) = \sum_{g\in G} a_g \otimes g,$$

donde $a = \sum_{g\in G} a_g$, $a_g \in A_g$ y $a_g \neq 0$ para un numero finito de g en G. En este caso tenemos que $A^{co\ kG}$ coincide con A_e.

iii) Sean H un álgebra de Hopf, A un álgebra y $\alpha : H \otimes H \to A$ un 2-cociclo de Hopf. El producto cruzado $A\#_\alpha H$ entre A y H es un H-comódulo álgebra con morfismo estructura

$$\rho : A\#_\alpha H \to (A\#_\alpha H) \otimes H, \quad \rho(au_h) = au_{h_{(1)}} \otimes h_{(2)}.$$

En este caso $(A\#_\alpha H)^{coH} = A\#_\alpha 1 \simeq A$. En efecto, si $au_h \in (A\#_\alpha H)^{coH}$, entonces aplicando $\mathrm{id} \otimes \mathrm{id} \otimes \varepsilon$ a la igualdad $\rho(au_h) = au_h \otimes 1$ obtenemos que $au_h \in A\#_\alpha 1$, la otra inclusión es clara.

4.2.14 Proposición. *Sean H un álgebra de Hopf de dimensión finita y A un álgebra. Entonces A es un H-comódulo álgebra si y sólo si A es un H^*-módulo álgebra. En este caso tenemos que $A^{H^*} = A^{coH}$.*

Demostración. Ver [DNR01, Proposition 6.2.4]. □

4.3. Extensiones de Hopf-Galois

A continuación presentamos la definición de extensión de Hopf-Galois dada en términos de coacciones para un álgebra H de Hopf, ver [Mon93, Definition 8.1.1].

4.3.1 Definición. Sea A un H-comódulo álgebra con morfismo estructura $\rho : A \to A \otimes H$. Decimos que la extensión $A \supseteq A^{coH}$ es una **H-extensión de Hopf-Galois** si la transformación lineal

$$\beta : A \otimes_{A^{coH}} A \to A \otimes_k H, \text{ dada por } a \otimes b \mapsto (a \otimes 1)\rho(b),$$

es biyectiva. Si A es una H-extensión de Hopf-Galois con $A^{coH} = k$ decimos que $A \supseteq k$ es una **H-extensión de Galois**.

Suponemos de ahora en adelante que H denota un álgebra de Hopf de dimensión finita sobre el cuerpo k.

Para A un H-módulo álgebra, consideremos la transformación lineal $\pi : A\#H \to \mathrm{End}(A_{A^H})$, definida por

$$\pi(a\#h)(b) = a(h \cdot b), \tag{4.5}$$

para $a, b \in A$ y $h \in H$.

4.3.2 Lema. *La transformación π es un homomorfismo de anillos. Entonces A tiene estructura de $A\#H$-módulo a través de π.*

Demostración. Análoga a la demostración en el Lema 2.1.2. □

A continuación, usando la Proposición 4.2.14, presentamos una definición de extensión de Hopf-Galois en términos de acciones.

4.3.3 Proposición. *Sea A un H-módulo álgebra. Entonces $A \supseteq A^H$ es una H^*-extensión de Hopf-Galois si y sólo si el homomorfismo $\pi : A\#H \to \mathrm{End}(A_{A^H})$ es un isomorfismo de álgebras y A es un A^H-módulo a derecha proyectivo finitamente generado.*

Demostración. Ver [Mon93, 8.3.3 Theorem]. □

4.3.4 Corolario. *A es una H^*-extensión de Galois si y sólo si A es finito dimensional y el homomorfismo $\pi : A\#H \to \mathrm{End}(A)$ es un isomorfismo.*

□

En particular para G un grupo finito, A un álgebra de dimensión finita sobre k y $(kG)^* = \mathrm{Hom}(kG, k)$, obtenemos un enlace entre las nociones de extensión de Hopf-Galois y álgebras de Galois:

4.3.5 Corolario. *A es una G-álgebra de Galois sobre k si y sólo si A es una $(kG)^*$-extensión de Galois.*

□

4.4. Deformaciones de grupos finitos

Tomando como referencia los artículos de [Sch96, Doi93, GN08], en esta sección presentamos la noción y algunos resultados de deformaciones de un grupo finito G.

Recordemos que toda álgebra de Hopf H de dimensión finita actúa a izquierda y a derecha trivialmente sobre k, esto es, k es trivialmente un H-módulo álgebra y un H-comódulo álgebra. Entonces para $\alpha : H \otimes H \to k$ un 2-cociclo de Hopf, consideramos una nueva multiplicación en H:

$$x \cdot_\alpha y = \alpha(x_{(1)}, y_{(1)})\alpha(x_{(3)}, y_{(3)})^{-1}x_{(2)}y_{(2)} \qquad (x, y \in H). \tag{4.6}$$

4.4.1 Definición. El espacio vectorial H con multiplicación definida en la Ecuación (4.6) junto a la comultiplicación y antípoda de H, es de nuevo un álgebra de Hopf denotado por H^α. Llamamos a H^α una **deformación de H por el 2-cociclo** α o, simplemente, una **deformación de** H. En el caso que $H = (kG)^* = \mathrm{Hom}(kG, k)$, con G un grupo finito, decimos que $H^\alpha = ((kG)^*)^\alpha$ es una **deformación del grupo finito** G.

4.4.2 Nota. Existe una correspondencia entre deformaciones de un álgebra de Hopf H y 2-cociclos de Hopf $\alpha : H \otimes H \to k$ de H a valores en k.

4.4.3 Proposición. *Sea A un H-módulo álgebra tal que $A\#H$ es simple y artiniana. Entonces*

i) $A \supseteq A^H$ *es una* H^**-extensión de Hopf-Galois.*

ii) $A \supseteq A^H$ *tiene la* ***propiedad de la base normal****; esto es,* $A \simeq A^H \otimes H$ *como* A*-módulo a izquierda y* H*-comódulo a derecha.*

iii) A *es isomorfa* $A \simeq A^H \#_\alpha H^*$ *al producto cruzado entre* A^H *y* H^**.*

Demostración. Ver [Mon93, 8.3.5 Corollary and 8.3.6 Proposition]. □

4.4.4 Corolario. *Sea* A *un* H*-comódulo álgebra. Entonces* A *es una* H*-extensión de Galois si y sólo si existe un 2-cociclo de Hopf* $\alpha : H \otimes H \to k$ *tal que el producto cruzado* $k\#_\alpha H$ *es isomorfo a* A*,* $A \simeq k\#_\alpha H$*.*

Demostración. Ver [GN08, Proposition 2.4]. □

En el caso que $H = (kG)^*$ tenemos que:

4.4.5 Corolario. *A es una* G*-álgebra de Galois sobre* k *si y sólo si existe un 2-cociclo de Hopf* $\alpha : (kG)^* \otimes (kG)^* \to k$ *tal que*

$$A \simeq k\#_\alpha (kG)^*.$$

□

El corolario anterior establece una correspondencia entre G-álgebras de Galois y 2-cociclos de Hopf $\alpha : (kG)^* \otimes (kG)^* \to k$. Además por la Observación 4.4.2 encontrar deformaciones del grupo G es equivalente a encontrar 2-cociclos de Hopf. Por lo tanto:

4.4.6 Proposición. *Dado* G *un grupo finito, existe una correspondencia entre* G*-álgebras de Galois y deformaciones de* G*.*

□

4.4.7 Proposición. *Dada el álgebra de Hopf* $H = (kG)^*$ *las deformaciones de* H *están determinadas por un dato* (K, N, σ, γ) *asociado a* G *y* k*.*

□

CAPÍTULO 5

Grupos cuánticos compactos

El objetivo principal de este capítulo es presentar una familia de ejemplos no triviales de grupos cuánticos compactos finitos, esta es construida a partir de deformaciones de grupos finitos, las cuales fueron estudiadas en el capítulo anterior (ver Teorema 5.2.3). Mostramos que todas las deformaciones de grupos finitos sobre el cuerpo de los números complejos poseen una estructura de grupo cuántico compacto finito.

A continuación presentamos por secciones, el contenido del capítulo y sus conexiones con el resto del escrito.

- 5.1 $*$-Álgebras de Hopf: Presentamos de manera sucinta las nociones de $*$-álgebra de Hopf, corepresentación unitaria y grupo cuántico compacto finito.
- 5.2 Ejemplos de grupos cuánticos finitos: En esta sección establecemos el objetivo principal de este capítulo.

Como referencia para este capítulo están los artículos [DK94, Mov94] y el libro [Arv76].

En este capítulo todos los espacios vectoriales, transformaciones lineales y productos tensoriales serán considerados sobre el cuerpo de los números complejos $\mathbb{C}$. Denotamos por $H = (H, m, u, \Delta, \varepsilon, S)$ un álgebra de Hopf de dimensión finita sobre $\mathbb{C}$.

5.1. $*$-Álgebras de Hopf

En esta sección presentamos de manera sucinta las nociones de $*$-álgebra, $*$-álgebra de Hopf, corepresentación unitaria y corepresentación unitarizable. Asimismo definimos el concepto de grupo cuántico compacto y buscaremos un ejemplo en las deformaciones de grupos finitos sobre el cuerpo de los números complejos.

Como referencia para esta sección está el artículo [DK94] y el libro [Arv76].

5.1.1 Definición. Sea A un álgebra. Una **$*$-estructura** para A es una transformación antilineal $* : A \to A$ (escribimos x^* a la imagen de x por medio de $*$) tal que para todo $x, y \in A$ se cumple las siguientes condiciones:

i) $(xy)^* = y^*x^*$,

ii) $1^* = 1$,

iii) $(x^*)^* = x$.

Una **$*$-álgebra** es una álgebra con una $*$-estructura. Dadas dos $*$-álgebras, A y B, un homomorfismo de álgebras $f : A \to B$ es un **$*$-homomorfismo** si para todo $x \in A$

$$f(x^*) = f(x)^*.$$

5.1.2 Definición. Una **$*$-álgebra de Hopf** $(H, *)$ es un álgebra de Hopf H con una $*$-estructura tal que los homomorfismos de álgebras Δ y ε son $*$-homomorfismos. En notación de Sweedler las condiciones sobre ε y Δ son escritas, respectivamente, por:

$$\varepsilon(x^*) = \overline{\varepsilon(x)}, \quad \text{y} \quad x^*_{(1)} \otimes x^*_{(2)} = {x_{(1)}}^* \otimes {x_{(2)}}^*, \quad \text{para todo } x \in H.$$

Sean H una álgebra de Hopf y V un H-comódulo a derecha, con morfismo estructura π (ver Definición 4.2.10). En este caso $\pi : V \to V \otimes H$ también se denomina una **corepresentación** de H en el espacio V. Si el espacio V es de dimensión finita y los elementos $\{v_i\}$ forman una base de V, entonces escribimos $\pi(v_j) = \sum_i v_i \otimes \pi_{ij}$, donde los π_{ij} son elementos de H. Entonces $\pi = (\pi_{ij})$ es una matriz (llamada la **matriz de corepresentación**) con coeficientes en H y

$$\Delta(\pi_{ij}) = \sum_k \pi_{ik} \otimes \pi_{kj}, \quad \varepsilon(\pi_{ij}) = \delta_{ij}.$$

Supongamos que H es una $*$-álgebra de Hopf y V es un espacio vectorial con producto interno $\langle , \rangle$. Una corepresentación π de H en V es **unitaria** si

$$\langle v_{(1)}, w\rangle S(v_{(2)}) = \langle v, w_{(1)}\rangle w^*_{(2)} \quad \forall v, w \in V.$$

Aquí usamos la notación de Sweddler para comódulos, esto es,

$$\pi(v) = v_{(1)} \otimes v_{(2)}, \quad (\pi \otimes \mathrm{id}) \circ \pi(v) = (\mathrm{id} \otimes \pi) \circ \pi(v) = v_{(1)} \otimes v_{(2)} \otimes v_{(3)},$$

donde $v_{(1)}$ está en V y $v_{(2)}$, $v_{(3)}$ están en H.

Si V es de dimensión finita y $\pi = (\pi_{ij})$ es la matriz de corepresentación con respecto a una base ortogonal $\{v_i\}$ de V. Entonces π es unitaria si y sólo si la siguientes condiciones se satisfacen:

$$S(\pi_{ij}) = \pi^*_{ji} \iff \sum_k \pi^*_{ki}\pi_{kj} = \delta_{ij}\, 1 \iff \sum_k \pi_{ik}\pi^*_{jk} = \delta_{ij}\, 1.$$

Una corepresentación π en un espacio vectorial V es **unitarizable** si existe un producto interno sobre V tal que π es unitaria con respecto a ese producto interno.

5.1.3 Definición. Una $*$-álgebra de Hopf H de dimensión finita es un **grupo cuántico compacto finito** si la corepresentación regular Δ de H es unitarizable.

5.2. Ejemplos de grupos cuánticos finitos

En esta sección establecemos nuestro objetivo principal del capítulo, esto es, mostrar que las deformaciones de grupos finitos sobre el cuerpo de los números complejos poseen una estructura de grupo cuántico compacto.

En esta sección los resultados son ideas originales del autor y su orientador.

5.2.1 Definición. Sean H una $*$-álgebra de Hopf y $\alpha : H \otimes H \to \mathbb{C}^*$ un 2-cociclo de Hopf. Decimos que el 2-cociclo α es de $*$**-Hopf** si:

- $\alpha^{-1} = \bar{\alpha}$.
- $\alpha(x, y) = \overline{\alpha(y^*, x^*)}$,

donde α^{-1} es el inverso con respecto al producto convolución.

5.2.2 Nota. Es evidente que si α es un 2-cociclo de $*$-Hopf para una $*$-álgebra de Hopf H, entonces la deformación H^α es una $*$-álgebra de Hopf con la misma $*$-estructura. Más aun, si H es un grupo cuántico compacto finito, entonces H^α también lo es.

Veamos ahora que toda G-álgebra de Galois compleja es isomorfa a una G-álgebra con $*$-estructura compatible con la G-acción. Sea $\mathbb{T} = \{z \in \mathbb{C} || z| = 1\}$, entonces para cualquier grupo finito, la inclusión $\mathbb{T} \subseteq \mathbb{C}^*$, induce un homomorfismo de grupos $H^n(G, \mathbb{T}) \to H^n(G, \mathbb{C}^*)$, el cual es un isomorfismo por el Teorema de Coeficientes Universales [Wei94]. Así, usando la Ecuación 1.7, podemos considerar que los 2-cociclos satisfacen las siguientes dos propiedades:

- $\sigma(g, h) \in \mathbb{T}$,
- $\sigma(g, h) = \overline{\sigma(h^{-1}, g^{-1})}$,

para todo $g, h \in G$. Estos 2-cociclos los llamamos **unitarios**.

Sea G un grupo finito, $S \subset G$ un subgrupo y $\sigma \in Z^2(S, \mathbb{T})$ un 2-cociclo no degenerado y unitario. Entonces el álgebra de grupo torcida $\mathbb{C}_\sigma S$ es una $*$-álgebra con $u_g^* = \epsilon_\sigma(g) u_{g^{-1}}$ para todo $g \in H$. Por lo tanto la G-álgebra de Galois $A = \mathrm{Ind}_S^G(\mathbb{C}_\sigma S)$, es una $*$-álgebra de G-Galois con $f^*(g) = f(g)^*$ para $g \in G$ y $f : G \to \mathbb{C}_\sigma S$. Por el Teorema Principal 3.2.19 denotemos por α al 2-cociclo de Hopf asociado a A.

5.2.3 Teorema. *La deformación $(\mathbb{C}G)^{*\alpha}$ asociada a la G-álgebra de Galois A, es un grupo cuántico compacto finito.*

Demostración. Dado que el álgebra de G-Galois A es una $*$-álgebra de Hopf y G actúa en forma unitaria, se sigue del argumento [Mov94, Proposition 5], que el 2-cociclo de Hopf asociado a α tiene las siguientes propiedades:

i) $\alpha^{-1} = \bar{\alpha}$.

ii) $\alpha(x, y) = \overline{\alpha(y^*, x^*)}$,

para todo $x, y \in (\mathbb{C}G)^*$, es decir, es un 2-cociclo de $*$-Hopf para $(\mathbb{C}G)^*$ y por tanto la deformación es un grupo cuántico compacto finito. $\square$

Conclusiones

⋆ Sean G un grupo finito, k un cuerpo y A una G-álgebra de Galois A sobre k. Entonces

- A es isomorfa a el álgebra inducida $\mathrm{Ind}_S^G(B)$, donde S es un subgrupo de G que estabiliza un elemento idempotente central primitivo del álgebra A y B es una S-álgebra de Galois simple.
- El álgebra de Galois simple B es isomorfa a el álgebra $A(K_\sigma N, \gamma)$, donde (K, N, σ, γ) es un dato de S-álgebra de Galois simple sobre k.

En resumen, *Dados G un grupo finito y k un cuerpo. Entonces A es una G-álgebra de Galois sobre k si y sólo si existen S un subgrupo de G que estabiliza un elemento idempotente central primitivo en A y (K, N, σ, γ) es un dato asociado a S y k tal que A es isomorfa a $Ind_S^G(B)$,*

$$A \simeq Ind_S^G(B),$$

donde B es la S-álgebra simple $A(K_\sigma N, \gamma)$.

⋆ A toda álgebra de Galois le corresponde un 2-cociclo de Hopf (y viceversa). Cada 2-cociclo de Hopf determina una deformación. Por lo tanto existe una correspondencia entre álgebras de Galois y deformaciones de grupos finitos.

⋆ Toda deformación de un grupo finito sobre el cuerpo de los números complejos posee estructura de grupo cuántico compacto.

Trabajo futuro

⋆ Establecer una teoría de obstrucción a la función γ.

⋆ Extender los resultados para anillos con acciones ergódicas, esto es, acciones tal que el álgebras de invariantes A^G coincida con su cuerpo base k, donde A es un anillo, G un grupo finito y k un cuerpo arbitrario.

⋆ Clasificar las estructuras cotriangulares de las deformaciones de $(kG)^*$.

⋆ Describir las subálgebras de Hopf normales usando técnicas de [GN08].

Bibliografía

[AG60] M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc (1960), no. 97, 367–409.

[AHN05] E. Aljadeff, D. Haile, and M. Natapov, *Projective bases of division algebras and groups of central type*, Israel J. Math. (2005), no. 146, 317–335.

[AM92] Frank Anderson and Kent Muller, *Rings and categories of modules*, second ed., Springer-Verlag, 1992.

[Arv76] William Arveson, *An invitation to C^*-algebras*, Springer Verlag, 1976.

[AS06] Nicolas Andruskiewitsch and H.-J. Schneider, *On the clasification of finite-dimensional pointed Hopf algebras*, To appear in Annals of Mathematics. Available in Arxiv:QA/0502157 (2006).

[BKJ01] B. Bakalov and A. Kirillov Jr., *Lectures on tensor categories and modular functors*, Amer. Math. Soc., Providence, 2001.

[CP95] V. Chari and A. Pressley, *A guide to quantum groups*, Cambridge University Press, 1995.

[CR90] Charles Curtis and Irving Reiner, *Methods of representation theory, I*, Wiley Interscience Publications, New York, 1990.

[Dav01] A. A. Davydov, *Galois algebras and monoidal functors between categories of representations of finite groups*, Journal of Algebra **244** (2001), 273–301.

[DF04] David Dummit and Richard Foote, *Abstract algebra*, III ed., John Wiley and Sons, Inc., 2004.

[DK94] Mathijs Dijkhuizen and Tom H. Koornwinder, *CQG algebras: a direct algebraic approach to compact quantum groups*, Available in arXiv:hep-th/9406042v1 (1994).

[DNR01] Sorin Dăscălescu, Constantin Năstăsescu, and Şerban Raianu, *Hopf algebras: and introduction*, Pure and applied mathematics. Marcel Decker, Inc, New York, 2001.

[Doi93] Yukio Doi, *Braided bialgebras and quadratic bialgebras*, Communications in Algebra (1993), no. 21, 1731–1749.

[GN07] César Galindo and Sonia Natale, *Simple Hopf algebras and deformations of finite groups*, Math. Res. Lett. (2007), no. 14, 943–954.

[GN08] ———, *Normal Hopf subalgebras in cocycle deformations of finite groups*, Manuscripta Math. 125 (2008), 501–504.

[GS06] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambrigde University Press, 2006.

[Kan65] Teuro Kanzaki, *On Galois algebra over a commutative ring*, Osaka Journal of Mathematics (1965), no. 2, 309–317.

[Kar85] Gregory Karpilovsky, *Projective representation of finite groups*, vol. 94, Pure and Applied Mathematics, Marcel Dekker, New York-Basel, 1985.

[Kas95] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics 155, Springer- Verlag, New York, 1995.

[Lor08] Falko Lorenz, *Algebra: Fields with structure, algebras and advanced topics*, vol. II, Springer, 2008.

[Maj95] S. Majid, *Foundations of quantum group theory*, Cambridge University Press, 1995.

[Mas97] Akira Masuoka, *Extensions of Hopf algebras*, Notas FaMAF (1997).

[Mon80] Susan Montgomery, *Fixed rings of finite automorphism groups of associative ring*, Lecture Notes in Mathematics, 818. Berlin - Heidelberg - New York: Springer-Verlag., 1980.

[Mon93] ———, *Hopf algebras and their action on rings*, vol. 82, Am. Math. Soc., Providence, Rhode Island, 1993.

[Mov94] M. Movshev, *Twisting in group algebras of finite groups*, Func. Anal Appl. (1994), no. 27, 240–244.

[Nat07a] Sonia Natale, *Semisolvability of semisimple Hopf algebras of low dimension*, Memoirs Amer. Math. Soc. (2007), no. 186.

[Nat07b] M. Natapov, *Projective bases of division algebras and groups of central type II*, ArXiv:0710.5468v1 (2007).

[NO04] Constantin Năstăsescu and Freddy Van Oystaeyen, *Methods of graded rings*, Springer Verlag, 2004.

[Sch96] Peter Schauenburg, *Hopf bigalois extensions*, Communications in Algebra **24** (1996), 3797 – 3825.

[Tak65] Yasuji Takeuchi, *On Galois extensions over commutative ring*, Osaka Journal of Mathematics (1965), no. 2, 137–145.

[Tur94] V.G. Turaev, *Quantum invariants of knots and 3-manifolds*, Walter de Gruyter, 1994.

[Wei94] Charles Weibel, *An introduction to homological algebra*, Cambridge University Press, 1994.

[Yam02] Shigeru Yamagami, *Polygonal presentations of semisimple tensor categories*, Journal of Mathematics Society Japan **54** (2002), no. 1, 61–88.