Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Matemáticas

TEORÍA DE HOPF-GALOIS

Autor/a: Mencía González Martín

Tutor: Jose Ramón Brox López

Resumen: El teorema fundamental de la teoría de Galois es crucial en el estudio de las extensiones de cuerpos. Este teorema establece que hay una correspondencia biyectiva entre los subcuerpos de una extensión de Galois y los subgrupos del grupo de Galois asociado a esa extensión. En otras palabras, cada subcuerpo de la extensión se puede asociar de manera única a un subgrupo del grupo de Galois, y viceversa.

La teoría de Hopf Galois amplía esta idea al considerar las álgebras de Hopf en el lugar del grupo de Galois. En el contexto de la teoría de Hopf Galois, se reemplazan los subgrupos del grupo de Galois por subálgebras de Hopf.

La base de esta teoría es la observación de que el grupo de Galois actúa sobre su extensión de cuerpos. Esta acción se puede extender a una acción del álgebra de grupo correspondiente, que es un tipo especial de álgebra de Hopf. Las subálgebras de Hopf de esta álgebra de grupo corresponden a los subgrupos del grupo de Galois.

La teoría de Hopf Galois permite estudiar extensiones de cuerpos que no necesariamente son de Galois, pero que aún pueden ser analizadas utilizando álgebras de Hopf. Esto abre nuevas posibilidades para entender y clasificar extensiones de cuerpos, proporcionando una herramienta más general y flexible que la teoría de Galois clásica

Palabras clave: Extensión de cuerpos, estructura de Galois, extensión normal, extensión separable, estructura de Hopf-Galois, álgebra, coálgebra, biálgebra, módulo, comódulo, coproducto, counidad, álgebra de Hopf, álgebra de comódulo, producto tensorial, teorema de Greither-Pareigis, estructura casi Galois clásica, traducción de Byott.

Abstract: The fundamental theorem of Galois theory is crucial in the study of field extensions. This theorem establishes a one-to-one correspondence between the subfields of a Galois extension and the subgroups of the associated Galois group. In other words, each subfield of the extension can be uniquely associated with a subgroup of the Galois group, and vice versa.

The Hopf Galois theory extends this idea by considering Hopf algebras in place of the Galois group. In the context of Hopf Galois theory, the subgroups of the Galois group are replaced by Hopf subalgebras.

The basis of this theory is the observation that the Galois group acts on its field extension. This action can be extended to an action of the corresponding group algebra, which is a special type of Hopf algebra. The Hopf subalgebras of this group algebra correspond to the subgroups of the Galois group.

Hopf Galois theory allows the study of field extensions that are not necessarily Galois but can still be analyzed using Hopf algebras. This opens up new possibilities for understanding and classifying field extensions, providing a more general and flexible tool than classical Galois theory.

Keywords: Field extension, Galois structure, normal extension, separable extension, Hopf-Galois structure, algebra, coalgebra, biálgebra, module, comodule, coproduct, counit, Hopf algebra, comodule algebra, tensor product, Greither-Pareigis theorem, almost classically Galois structure, Byott translation.

Índice general

Introducción

La teoría clásica de Galois estudia las propiedades de las extensiones de cuerpos L/K y su estructura de Galois, es decir, si L/K es una extensión finita de cuerpos y existe un subgrupo $G < Aut(L)$ tal que $L^G = K$, lo que significa que si K es el cuerpo fijo bajo un cierto subgrupo del grupo de automorfismos de L. Esto fue introducido por el matemático francés Évariste Galois en 1831, que encontró una condición necesaria y suficiente para la resolución de ecuaciones algebraicas por radicales. A este descubrimiento se le acuña el nombre de Gran Teorema de Galois.

La teoría clásica de Galois establece que si tenemos una extensión de cuerpos L/K finita, normal y separable, entonces existe una correspondencia biyectiva entre los subcuerpos intermedios y los subgrupos del grupo de Galois. Esto permite estudiar extensiones de cuerpos a través de grupos, de esta manera, podemos clasificar y entender las extensiones mediante la estructura de los grupos correspondientes. Sin embargo, esta teoría presenta limitaciones, ya que solo se centra en extensiones finitas, normales y separables, por lo que para subsanar esto se han buscado distintas generalizaciones, siendo una de ellas la teoría de Hopf-Galois.

La teoría de Hopf-Galois nace como un intento de expandir la teoría clásica de Galois a otro tipo de estructuras. En 1969, Stephen Chase y Moss Sweedler [3] introducen el concepto de extensión de Hopf-Galois que amplía la noción de extensión de Galois. Sus objetivos principales eran generalizar a extensiones no separables, y más en general, extender la teoría clásica de Galois a extensiones de anillos conmutativos. Para ello, en vez de estudiar extensiones normales y separables mediante grupos de automorfismos, recurrieron a las álgebras de Hopf, las cuales actúan sobre la extensión y permiten formular de manera más general la teoría de Galois en un contexto

más amplio.

El propósito de nuestro trabajo es el estudio detallado de las estructuras de Hopf-Galois en las extensiones de cuerpos, tanto en la construcción teórica como en ejemplos que ilustren su aplicación.

En el capítulo 1 recordaremos aquellos resultados más importantes de la teoría de Galois que son importantes para entender la teoría de Hopf-Galois.

En el capítulo 2 empezaremos definiendo el producto tensorial, ya que será la herramienta principal que nos permitirá describir todos los objetos implicados en esta teoría. Seguiremos introduciendo las definiciones categóricas de álgebra, coálgebra y biálgebra hasta llegar a precisar el concepto de álgebra de Hopf. Además, estudiaremos el concepto de álgebra de comódulo de una biálgebra, esencial para extender la teoría de Galois mediante álgebras de Hopf, y describiremos otras estructuras relacionadas.

Por último, en el capítulo 3 comenzaremos reformulando la definición de extensión de Galois en términos del álgebra de grupo. Esta reformulación permite generalizar la definición a cualquier álgebra de Hopf coconmutativa, dando lugar al concepto de estructuras de Hopf-Galois de una extensión. Veremos un ejemplo de extensión que no es de Galois pero posee una estructura de Hopf-Galois, mostrando que la teoría de Hopf-Galois es más general que la teoría clásica. Observaremos también que, aunque la estructura clásica de Galois de una extensión de Galois es única, en general una extensión de Hopf-Galois posee más de una estructura de Hopf-Galois; esto puede ocurrir incluso cuando la extensión es de Galois. A continuación, veremos que, al contrario que en la teoría de Galois, no podemos asegurar que la correspondencia entre las extensiones de cuerpos y las álgebras de Hopf sea biyectiva, únicamente inyectiva. En este sentido estudiaremos las estructuras casi Galois clásicas, que recuperan la biyectividad de la correspondencia. Seguidamente, presentaremos la teoría para extensiones separables. Aquí veremos el gran resultado de Greither-Pareigis [10], que establece una manera de encontrar todas las estructuras de Hopf-Galois que tiene una extensión, usando la teoría de grupos. Por último, veremos la traducción de Byott [2], que alivia el problema principal que presenta el teorema de Greither-Pareigis; gracias a él podremos determinar todas dichas estructuras reduciendo el número de cálculos.

Cerraremos la memoria mostrando importantes corolarios de estos resultados: mostraremos cuándo tienen estructura de Hopf-Galois las extensiones

de grado pequeño, daremos una fórmula general para el número de estructuras para cualquier extensión, y determinaremos cuándo la estructura de Galois de una extensión de Galois es la única estructura de Hopf-Galois que posee la extensión (teorema de unicidad de Byott).

Capítulo 1

Teoría de Galois

Aunque ya hemos estudiado la teoría de Galois en el grado, para entender la teoría de Hopf-Galois es necesario primero repasar algunos resultado importantes. Por eso, haremos una revisión poco profunda de la misma. En primer lugar, partiremos de los conceptos más básicos sobre extensiones de cuerpos, fundamentando cuándo tienen estructura de Galois. Una vez visto esto, introduciremos el concepto de grupo de Galois, y daremos un ejemplo completo del uso del teorema fundamental de la teoría de Galois.

1.1. Extensiones de cuerpos. Extensiones algebraicas y trascendentes

En esta primera parte vamos a entender qué es una extensión de cuerpos, dando su definición y poniendo algún ejemplo. Además, clasificaremos las extensiones en algebraicas o trascendentes. Empezamos con su definición:

Definición 1.1. Una extensión de cuerpos es un par de cuerpos, L,K, tales que K es un subcuerpo de L. Lo denotamos como L/K o $K \subset L$. El cuerpo K es el cuerpo base y el cuerpo L es el cuerpo de extensión.

Nota. En toda extensión L/K el cuerpo L es un espacio vectorial sobre el cuerpo K de forma natural, donde la acción de K está dada por el producto en L.

En definitiva, obtenemos una extensión de cuerpos cuando al cuerpo base

K le añadimos elementos nuevos, de forma que el conjunto resultante sigue siendo un cuerpo que contiene a K y respeta sus operaciones.

Definición 1.2. Llamamos grado de la extensión L/K y lo denotamos por $[L : K]$ a la dimensión de L como espacio vectorial sobre K. Si el grado es finito, se dice que la extensión es finita. En otro caso, se dice que la extensión es infinita.

Teorema 1.3 (del grado)**.** *(Proposición 7.1.2[5]) Sea $K \subset F \subset L$ una torre de cuerpos. Entonces*

$$[L : K] = [L : F][F : K]$$

Además, la extensión L/K es finita si, y solo si, las extensiones L/F y F/K son ambas finitas.

Ahora que ya hemos recordado qué es una extensión de cuerpos, podemos preguntarnos cuántos y qué tipo de elementos podemos añadir al cuerpo base. Estos elementos se clasifican dependiendo de si añadimos un número finito o infinito de ellos y de si cada uno es raíz de un polinomio con coeficientes en el cuerpo base. Veamos cómo se distinguen según estas propiedades:

Definición 1.4. Sea L/K una extensión de cuerpos. Un elemento $\alpha \in L$ se dice que es **algebraico** sobre K si existe un polinomio no nulo $f \in K[X]$ tal que $f(\alpha) = 0$. Si un elemento de L no es algebraico sobre K, se dice que es trascendente sobre K.

En caso de que todo elemento de L sea algebraico sobre K, se dice que L/K es una extensión algebraica. Si existe algún elemento de L que es trascendente sobre K, se dice que la extensión es **trascendente**. Vemos un ejemplo:

Ejemplo 1.5.

1. $\sqrt{3}$ es algebraico sobre $\mathbb{Q}$ ya que es raíz del polinomio $f(X) = x^2 - 3$.
2. i es algebraico sobre $\mathbb{R}$ ya que es raíz del polinomio $f(X) = x^2 + 1$.
3. e es trascendente sobre $\mathbb{Q}$ por un resultado de Hermite.

Definición 1.6. Sea L/K una extensión de cuerpos y $\alpha \in L$ algebraico sobre K. El polinomio mónico p irreducible sobre K tal que $p(\alpha) = 0$ se llama **polinomio mínimo** de α sobre K, y lo denotaremos por $Irr(\alpha, K)$.

Proposición 1.7. *(Proposición 1.1 [13]) Si L/K es una extensión finita de cuerpos, entonces L/K es algebraica.*

Definición 1.8. Sea L/K una extensión, y S un subconjunto de L. Diremos que S es un conjunto de generadores para L sobre K si $L = K(S)$.
Se dice que la extensión es finitamente generada si el conjunto S es finito.

Definición 1.9. Una extensión L/K se dice simple si existe un elemento $\alpha \in L$ tal que $L = K(\alpha)$. En tal caso, se dice que este elemento es un **elemento primitivo** para la extensión.

Proposición 1.10. *(Proposiciones 1.5,1.6 [13]) Sea L/K una extensión de cuerpos. Entonces:*

1. *Si L/K es una extensión finita, entonces es finitamente generada.*
2. *Si L/K es finitamente generada $L = K(\alpha_1, \ldots, \alpha_n)$, y los elementos $\alpha_i, i = 1 \ldots n$ son algebraicos sobre K, entonces la extensión L/K es finita.*
3. *Si $L = K(S)$ con $S \subseteq L$ arbitario, se tiene que F/K es algebraica si, y solo si, todo $\alpha \in S$ es algebraico sobre K.*

1.2. Cuerpos de descomposición. Extensiones normales finitas

El origen del estudio de las extensiones de cuerpos es la necesidad de construir cuerpos que contengan al cuerpo base K en los que existan raíces de polinomios dados de $K[X]$. Al querer resolver ecuaciones algebraicas que no tienen solución en K se intenta extender el cuerpo con los elementos necesarios para que el problema se pueda resolver dentro de un nuevo contexto más amplio.

En esta nueva sección vamos a ver cómo trabajamos con aplicaciones entre extensiones y además vamos a caracterizar las extensiones normales, un concepto fundamental en la teoría de Galois.

Teorema 1.11. *(Kronecker)(Teorema 7.2.1 [5]) Sea K un cuerpo y $f \in K[X]$ un polinomio no constante. Entonces existe una extensión L/K y un elemento $\alpha \in L$ tal que $f(\alpha) = 0$.*

Este teorema es clave ya que nos da la solución a cómo construir extensiones de cuerpos que incluyan las soluciones de cualquier ecuación algebraica.

Definición 1.12. Dadas extensiones de cuerpos L_1/K_1 y L_2/K_2 y homomorfismos $\tau : L_1 \to L_2$ y $\sigma : K_1 \to K_2$, se dice que τ es una extensión de σ si, $\forall a \in K_1$ se tiene que $\tau(a) = \sigma(a)$.

Si $\sigma = id_k$ y τ es una extensión de σ se dice que τ es un K-homomorfismo y se denota poniendo $\tau : L_1/K \to L_2/K$.

Proposición 1.13. *(Corolario 7.5.2 [5]) Dadas dos extensiones L_1/K y L_2/K, si $[L_1 : K] = n$, entonces hay como mucho n homomorfismos de L_1 a L_2.*

Proposición 1.14. *(Proposición 2 [7]) Sea L/K una extensión de cuerpos y sea $\alpha \in L$ un elemento algebraico sobre K. Consideremos $Aut(L/K)$ el grupo de automorfismos de la extensión. Entonces, para cualquier $\sigma \in Aut(L/K)$ tenemos que $\sigma(\alpha)$ es una raíz del polinomio irreducible de α sobre K.*

Veamos un ejemplo de cómo se calculan todos los automorfismos de una extensión:

Ejemplo 1.15. Veamos cuáles son todos los automorfismos de $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$. Observamos que $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. Lo hacemos en dos partes:

1. Consideramos $\sigma = id_{\mathbb{Q}}$, $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ y sus dos raíces $-\sqrt{2}$, $\sqrt{2}$, tenemos dos extensiones de σ:

$$\tau_1 : \mathbb{Q}(\sqrt{2}) \underset{\sqrt{2}\to\sqrt{2}}{\to} \mathbb{Q}(\sqrt{2}) \qquad \tau_2 : \mathbb{Q}(\sqrt{2}) \underset{\sqrt{2}\to-\sqrt{2}}{\to} \mathbb{Q}(\sqrt{2})$$

2. Ahora para cada una de ellas considerando $Irr(i, \mathbb{Q}(\sqrt{2})) = x^2 + 1$ y sus dos raíces i,$-i$ tenemos dos extensiones:

$$\tau_{11} : \mathbb{Q}(\sqrt{2})(i) \underset{\substack{i\to i \\ \sqrt{2}\to\sqrt{2}}}{\to} \mathbb{Q}(\sqrt{2})(i) \qquad \tau_{12} : \mathbb{Q}(\sqrt{2})(i) \underset{\substack{i\to -i \\ \sqrt{2}\to\sqrt{2}}}{\to} \mathbb{Q}(\sqrt{2})(i)$$

$$\tau_{21} : \mathbb{Q}(\sqrt{2})(i) \underset{\substack{i\to i \\ \sqrt{2}\to-\sqrt{2}}}{\to} \mathbb{Q}(\sqrt{2})(i) \qquad \tau_{22} : \mathbb{Q}(\sqrt{2})(i) \underset{\substack{i\to -i \\ \sqrt{2}\to-\sqrt{2}}}{\to} \mathbb{Q}(\sqrt{2})(i)$$

asi que los 4 automorfismos de $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ están dados sobre los generadores en la tabla

	τ_{11}	τ_{12}	τ_{21}	τ_{22}
$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
i	i	$-i$	i	$-i$

Ahora bien, ¿qué pasa si queremos añadir al cuerpo base todas las raíces de un polinomio dado? Esta pregunta nos conduce a la definición de cuerpo de descomposición, que es la extensión minimal del cuerpo base donde un polinomio se descompone completamente en factores lineales. Formalmente:

Definición 1.16. Un cuerpo de extensión L/K se dice que es un **cuerpo de descomposición** (c.d.d) de un polinomio $f \in K[X]$ si existen $a_n, \alpha_1 \cdots \alpha_n \in L$ tales que $f = a_n(X - \alpha_1) \cdots (X - \alpha_n)$ y $L = K(\alpha_1 \cdots \alpha_n)$. Notemos que si E es un cuerpo de descomposición de $f \in K[X]$ y se tiene una torre $K \subset L \subset E$ entonces E también es un cuerpo de descomposición de $f \in L[X]$ pues si $\alpha_1 \cdots \alpha_n \in E$ son las raíces de f se tiene que $E = K(\alpha_1 \cdots \alpha_n) \subset L(\alpha_1 \cdots \alpha_n) \subset E$, por tanto $E = L(\alpha_1 \cdots \alpha_n)$

Teorema 1.17. *(Teorema 7.2.3 [5]) Si K es un cuerpo, para todo polinomio $f \in K[X]$ de grado $n > 0$, existe un cuerpo de descomposición F de f sobre K y se verifica que $[F : K] \leq n!$*

Teorema 1.18. *(Teorema 7.2.3 [5]) Sea $\sigma : K_1 \longrightarrow K_2$ un isomorfismo de cuerpos, $f_1 \in K_1[X]$ y $f_2 = \sigma(f_1)$. Si F_1 y F_2 son, respectivamente, cuerpos de descomposición de f_1 y f_2, entonces existe un isomorfismo $\tau : F_1 \longrightarrow F_2$ extensión de σ. En particular, si $\sigma = Id_K$, se tiene que dos cuerpos de descomposición cualesquiera de un polinomio $f \in K[X]$ son K-isomorfos.*

Estos dos teoremas nos aseguran que el cuerpo de descomposición siempre existe y que además es único.

Ejemplo 1.19.

1. Si $f = (X^2-2)(X^2-3) \in \mathbb{Q}[X]$ el c.d.d de f sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ya que contiene todas las raíces de f pues su descomposición lineal es $(X - \sqrt{2})(X + \sqrt{2})(X - \sqrt{3})(X + \sqrt{3})$, y, además, la extensión tiene grado 4 sobre $\mathbb{Q}$.
2. Si $f = X^6 - 1 \in \mathbb{Q}[X]$ tenemos que el c.d.d de f sobre $\mathbb{Q}[X]$ es $\mathbb{Q}(w)$ donde w es la raíz cubica primitiva de la unidad ya que las raíces de f son $\pm 1, \pm w, \pm w^2$ y todas están contenidas en $\mathbb{Q}(w)$. Además la extensión tiene grado 2 sobre $\mathbb{Q}$ ya que $irr(w, \mathbb{Q}) = X^2 + X + 1$.
3. Si $f = (X^2 - 2)(X^3 - 2) \in \mathbb{Q}[X]$ su c.d.d es $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, w)$ que tiene

grado 12 sobre $\mathbb{Q}$.

4. Sea $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, su polinomio irreducible es X^3-2, pero este no descompone en factores lineales sobre $\mathbb{Q}(\sqrt[3]{2})$ ya que no contiene w, luego no es su c.d.d. Obtenemos su cuerpo de descomposición si añadimos w llegando a $\mathbb{Q}(\sqrt[3]{2}, w)$.

Este último ejemplo nos ha mostrado una idea clave, una extensión de cuerpos no siempre contiene todas las raíces de un polinomio, es decir, no siempre es su cuerpo de descomposición. Esta observación nos lleva a una nueva forma de caracterizar las extensiones, en función de si incluyen o no todas las raíces de los polinomios que tienen al menos una raíz en la extensión.

Definición 1.20. Una extensión finita E/K se dice que es **normal** si E es el cuerpo de descomposición de algún polinomio $f \in K[X]$.

Ejemplo 1.21.
1. Sea $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ que es el c.d.d de $f = x^2-2$ ya que sus todas sus raíces son $\sqrt{2}$ y $-\sqrt{2}$, por tanto es normal.

2. Sea $\mathbb{Q}(\sqrt[3]{2}, w)/\mathbb{Q}$, con w raíz cubica de la unidad. Tenemos que es el c.d.d de $f = X^3-2$ luego es normal.

3. Sea $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$. Tenemos que $Irr(\sqrt[3]{5}, \mathbb{Q}) = X^3-5$ que no descompone en $\mathbb{Q}(\sqrt[3]{5})$ ya que tiene dos raíces complejas, luego no es normal.

Proposición 1.22. *Toda extensión de grado 2 es una extensión normal.*

Teorema 1.23 (Caracterización de extensiones normales)**.** *(Teorema 3.3 [13]) Sea E/K una extensión finita. Entonces son equivalentes:*

1. *E/K es normal.*

2. *Cualquier polinomio $f \in K[X]$ irreducible que tenga una raíz en E descompone completamente en E.*

Teorema 1.24. *(Página 199 [5]) Si E/K es finita, existe su clausura normal y es única salvo K-isomorfismo.*

1.3. Extensiones separables. Automorfismos de extensiones

Hasta ahora hemos visto que las extensiones de cuerpos pueden clasificarse dependiendo de la existencia de las raíces de los polinomios irreducibles con coeficientes en el cuerpo base. Sin embargo, las raíces pueden ser múltiples o no; por eso podemos introducir una nueva propiedad: la separabilidad.

Veremos la definición formal más adelante, pero intuitivamente una extensión es separable si los polinomios irreducibles involucrados tienen raíces simples, es decir, con multiplicidad igual a 1. Esta condición en característica cero se da siempre, pero cuando es positiva puede haber polinomios irreducibles con raíces múltiples, lo que hace que no todas las extensiones sean separables.

Definición 1.25. Un cuerpo K se dice que es **perfecto** si todo polinomio irreducible sobre K tiene sus ceros simples. Entonces se tiene:

1. Un cuerpo K con $car(K) = p$ es perfecto si el endomorfismo de Frobenius ($F : K \longrightarrow K$ $F(a) = a^p$) es un automorfismo.
2. Si $car(K) = 0$ entonces K es perfecto.
3. Si K es algebraicamente cerrado entonces es perfecto.
4. Si K es finito entonces es perfecto (pues el endomorfismo de Frobenius es automorfismo).
5. El cuerpo $\mathbb{Z}_p(t)$ no es perfecto pues $X^p - t \in \mathbb{Z}_p(t)[X]$ es irreducible y tiene derivada nula así que no todos sus ceros son simples.

Definición 1.26.

1. Un polinomio $f \in K[X]$ se dice separable sobre K si sus factores irreducibles sobre K solo tienen ceros simples.
2. Un elemento α algebraico sobre K se dice separable sobre K si $Irr(\alpha, K)$ es separable.
3. Una extensión algebraica E/K se dice que es separable si todo elemento de E es separable sobre K.

Teorema 1.27. *(Corolario 39 [7]) Sea K un cuerpo. Son equivalentes:*

1. *K es perfecto.*
2. *Cualquier E/K algebraica es separable.*
3. *Cualquier E/K finita es separable.*

Proposición 1.28. *Dada una torre $K \subset F \subset E$ con E/K algebraica, se tiene que si E/K es separable, entonces E/F y F/K son separables.*

Corolario 1.29. *Toda extensión algebraica de un cuerpo perfecto es un cuerpo perfecto.*

Teorema 1.30 (del elemento primitivo)**.** *(Teorema 4.6 [13]) Una extensión finita E/K es simple (tiene un elemento primitivo) si y solo si existe un número finito de cuerpos intermedios entre K y E. En particular esto ocurre cuando E/K es separable.*

1.4. Extensiones de Galois. El teorema fundamental. Ejemplos e ilustraciones

A lo largo del capítulo hemos identificado las propiedades que nos ayudan a clasificar las extensiones. Fundamentalmente, hemos visto la normalidad y la separabilidad. A continuación, veremos que si se cumplen ambas, estaremos ante una extensión de Galois. Este tipo de extensión es especialmente interesante porque permite definir una estructura adicional llamada el grupo de Galois, formado por los automorfismos del cuerpo extendido que fijan el cuerpo base. Este grupo refleja las simetrías algebraicas de la extensión y establece una relación entre la teoría de cuerpos y la teoría de grupos.

Definición 1.31. Una extensión finita E/K es una **extensión de Galois** si existe un subgrupo $G < Aut(E)$ tal que $E^G = K$, es decir, si K es el cuerpo fijo bajo un cierto subgrupo del grupo de automorfismos de E.

Nota. Notemos que al ser E/K finita el grupo $Aut_K(E)$ de K-automorfismos de E es finito y, como $G < Aut_K(E)$, tenemos que G es finito.

Teorema 1.32. *(Proposición 7.6.1 [5]) Sea E/K una extensión finita. Entonces, E/K es de Galois si y solo si E/K es normal y separable.*

Gracias a este resultado, tenemos una manera muy sencilla de identificar si estamos ante una extensión de Galois o no. Ambas propiedades son

necesarias y suficientes para que las simetrías entre sus elementos puedan describirse mediante un grupo de automorfismos.

Definición 1.33. Si E/K es una extensión de Galois, se llama **grupo de Galois** de la extensión, denotado $\mathrm{Gal}(E/K)$, al grupo $\mathrm{Aut}_k(E)$ de K-automorfismos de E, esto es,

$$\mathrm{Gal}(E/K) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma(a) = a \quad \forall a \in K\}$$

Lema 1.34. *Dada la torre de extensiones finita $K \subset F \subset E$, si E/K es de Galois entonces E/F es de Galois y $Gal(E/F) < Gal(E/K)$.*

Ahora vamos a denotar por $S(G)$ el retículo de subgrupos de G y al retículo de subextensiones de E/K por $\mathcal{F}(E/K)$ y vamos a ver que entre ellos podemos definir aplicaciones que definen la llamada **conexión de Galois** de la extensión de Galois E/K. En efecto, se tienen aplicaciones bien definidas:

$$\begin{aligned} S(G) &\longmapsto \mathcal{F}(E/K) \\ H &\longmapsto E^H = \{\alpha \in E \mid \sigma(\alpha) = \alpha \, \forall \sigma \in H\} \end{aligned}$$

$$\begin{aligned} \mathcal{F}(E/K) &\longmapsto S(G) \\ F &\longmapsto G^F = Gal(E/F) \end{aligned}$$

Y sus principales propiedades quedan definidas en el siguiente resultado:

Proposición 1.35. *Sean $F, F_1, F_2 \in \mathcal{F}(E/K)$ y $H, H_1, H_2 \in \mathcal{S}(G)$. Entonces se tiene:*

i) $F_1 \subseteq F_2 \implies G^{F_1} \supseteq G^{F_2}$, $H_1 \subseteq H_2 \implies E^{H_1} \supseteq E^{H_2}$.

ii) $F \subseteq E^{G^F}$; $H \subseteq G^{E^H}$.

iii) $E^{G^{E^H}} = E^H$, $G^{E^{G^F}} = G^F$.

Las propiedades expresadas en la proposición anterior no exigen que E/K sea una extensión de Galois, pero para el siguiente resultado, que es fundamental, sí es necesario que E/K sea de Galois.

Teorema 1.36. *(Teorema Fundamental de la Teoría de Galois).(Teorema 1.4 [7]) Sea E/K una extensión finita de Galois con grupo de Galois $G = Gal(E/K)$. Entonces:*

i) La conexión de Galois establece una biyección entre los retículos de ***subgrupos de*** *G y de* ***subextensiones de*** *E/K:*

$$S(G) \cong \mathcal{F}(E/K)$$

$$H \longrightarrow E^H$$

$$G^F \longleftarrow F$$

ii) La conexión de Galois invierte el orden de inclusión:

$$F_1 \subseteq F_2 \iff G^{F_1} \supseteq G^{F_2} \quad y \quad H_1 \subseteq H_2 \iff E^{H_1} \supseteq E^{H_2}.$$

iii) La conexión de Galois es un antisimorfismo de retículos, es decir, es una biyección que lleva supremos en ínfimos y viceversa:

$$G^{(F_1F_2)} = G^{F_1} \cap G^{F_2} \quad (i.e., \ \ Gal(E/F_1F_2) = Gal(E/F_1) \vee Gal(E/F_2))$$

$$G^{(F_1 \cap F_2)} = G^{F_1} \vee G^{F_2} \quad (i.e., \ \ Gal(E/F_1 \cap F_2) = Gal(E/F_1) \cap Gal(E/F_2)).$$

iv) Las subextensiones F_1/K y F_2/K son conjugadas (bajo algún $\sigma \in G$) si y solo si G^{F_1} y G^{F_2} son conjugados en G (esto es, $\sigma G^{F_2}\sigma^{-1} = G^{F_1} \iff F_1 = \sigma(F_2)$).

v) Si $F \in \mathcal{F}(E/K)$, entonces F/K es de Galois $\iff G^F \triangleleft G$, y en tal caso $Gal(F/K) \cong G/G^F$ (i.e., $Gal(F/K) \cong Gal(E/K)/Gal(E/F)$).

vi) $\forall H \in S(G) \implies |H| = [E : E^H]$ *y* $[G : H] = [E^H : K]$.

$$\forall F \in \mathcal{F}(E/K) \implies [E : F] = |G^F| \ y \ [F : K] = [G : G^F].$$

Vamos a ilustrar el teorema fundamental con un ejemplo:

Ejemplo 1.37. Consideremos la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. La torre:

$$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

asegura que $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$, así que se trata de una extensión finita que es normal (es el c.d.d. del polinomio $((X^2-2)(X^2-3)\in\mathbb{Q}(X))$ y además es separable porque $\mathrm{car}(\mathbb{Q})=0$ y por tanto toda extensión finita suya es separable). Por tanto, $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ es una extensión de Galois con

$$|\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})|=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4.$$

y donde los elementos de $G=\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ son los $\mathbb{Q}$-automorfismos $\varphi_1,\varphi_2,\varphi_3,\varphi_4$, donde $\varphi_1=\mathrm{id}_{\mathbb{Q}(\sqrt{2},\sqrt{3})}$ y φ_i, $i=2,3,4$, están determinados como sigue:

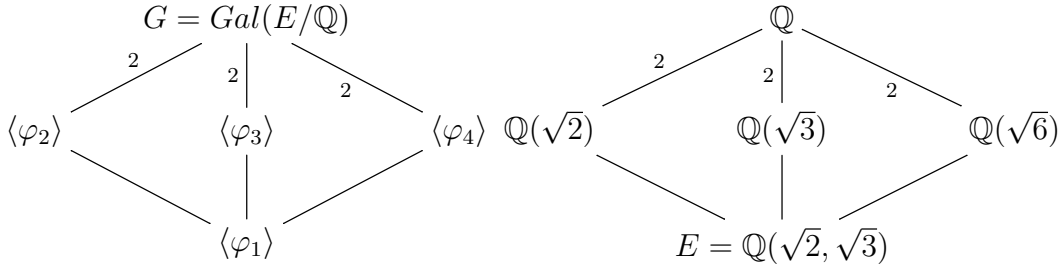
$$\begin{aligned}
\varphi_2:&\quad \sqrt{3}\mapsto-\sqrt{3},\quad \sqrt{2}\mapsto\sqrt{2},\\
\varphi_3:&\quad \sqrt{3}\mapsto\sqrt{3},\quad \sqrt{2}\mapsto-\sqrt{2},\\
\varphi_4:&\quad \sqrt{3}\mapsto-\sqrt{3},\quad \sqrt{2}\mapsto-\sqrt{2}.
\end{aligned}$$

Como $|G|=4$, sabemos que G es abeliano y que, salvo isomorfismo, $G\cong\mathbb{Z}_4$ o $G\cong\mathbb{Z}_2\times\mathbb{Z}_2$. Ahora, es inmediato observar que ninguno de los elementos de G tiene orden 4, de hecho, todos salvo φ_1 (que tiene orden 1) tienen orden 2, de donde $G\cong\mathbb{Z}_2\times\mathbb{Z}_2$.

Para establecer la conexión de Galois debemos reconocer en principio el retículo de subgrupos de G y luego, con el cálculo de los correspondientes cuerpos fijos, obtendremos el retículo de subextensiones y podremos visualizar la conexión de Galois.

En el caso que nos ocupa en que $G=\{\varphi_1,\varphi_2,\varphi_3,\varphi_4\}\cong\mathbb{Z}_2\times\mathbb{Z}_2$ el retículo es sencillo, lo vemos más abajo.

Para el cálculo de los cuerpos fijos $E^{\langle\varphi_2\rangle}$, $E^{\langle\varphi_3\rangle}$, $E^{\langle\varphi_4\rangle}$, con $E=\mathbb{Q}(\sqrt{2},\sqrt{3})$, podemos recurrir al método general ya conocido de expresar cualquier elemento de E en función de la $\mathbb{Q}$-base $\{1,\sqrt{2},\sqrt{3},\sqrt{2}\sqrt{3}\}$ e imponer que quede fijo bajo el correspondiente subgrupo. En este caso, es bastante sencillo de calcular pues basta observar que ciertamente se tiene que $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq E^{\langle\varphi_2\rangle}$ y como $[E^{\langle\varphi_2\rangle}:\mathbb{Q}]=[G:\langle\varphi_2\rangle]=2$ se sigue que $E^{\langle\varphi_2\rangle}=\mathbb{Q}(\sqrt{2})$. Análogamente $E^{\langle\varphi_3\rangle}=\mathbb{Q}(\sqrt{3})$ y $E^{\langle\varphi_4\rangle}=\mathbb{Q}(\sqrt{6})$, así que la conexión de Galois puede visualizarse en los diagramas:



Notemos que todas las subextensiones tienen grado 2 sobre $\mathbb{Q}$, así que son normales (y por tanto de Galois), lo que está en consonancia con el hecho de corresponder a subgrupos de índice 2 y por tanto normales. Se tiene así que

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \frac{\mathrm{Gal}(E/\mathbb{Q})}{\mathrm{Gal}(E/\mathbb{Q}(\sqrt{2}))} = \frac{G}{\langle\varphi_2\rangle} \cong \mathbb{Z}_2$$

y análogamente:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \cong \frac{\mathrm{Gal}(E/\mathbb{Q})}{\mathrm{Gal}(E/\mathbb{Q}(\sqrt{3}))} = \frac{G}{\langle\varphi_3\rangle} = \{\varphi_1\langle\varphi_3\rangle, \varphi_2\langle\varphi_3\rangle\} \cong \mathbb{Z}_2.$$

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{6})/\mathbb{Q}) \cong \frac{\mathrm{Gal}(E/\mathbb{Q})}{\mathrm{Gal}(E/\mathbb{Q}(\sqrt{6}))} = \frac{G}{\langle\varphi_4\rangle} = \{\varphi_1\langle\varphi_4\rangle, \varphi_2\langle\varphi_4\rangle\} \cong \mathbb{Z}_2.$$

Capítulo 2

Introducción a las álgebras de Hopf

Ahora, que hemos sentado las bases de la teoría de Galois, estamos en condiciones de adentrarnos en su generalización. Primero, introduciremos los conceptos necesarios para entender lo que es un álgebra de Hopf, para así poder dar su definición exacta. En este capítulo introduciremos las álgebras como espacios vectoriales dotados de dos operaciones lineales que satisfacen varias propiedades, y las coálgebras como su dual categórico. Luego, veremos las biálgebras como espacios vectoriales que son a la vez álgebras y coálgebras con condiciones de compatibilidad. Así, llegaremos a definir las álgebras de Hopf, que son biálgebras dotadas de un operador llamado antípoda, la cual permite definir un comportamiento que emula el inverso de los elementos de un grupo. Además, ilustraremos estos objetos dando algunos ejemplos.

Según [8], Heinz Hopf, pionero en topología algebraica, introdujo estas álgebras en 1941 en conexión con los grupos de Lie, combinando aspectos algebraicos y coalgebraicos en una sola estructura. Al final de los años 70, Rota introdujo las álgebras de Hopf en combinatoria, y ahora hay muchos ejemplos de familias de objetos de este área, conocidas como álgebras de Hopf combinatorias. Además, en estos últimos años, las álgebras de Hopf han adquirido bastante relevancia debido a su aplicación en los grupos cuánticos de la física.

Al final de este capítulo, habremos adquirido los conocimientos necesarios para introducirnos en el estudio que nos ocupa: La teoría de Hopf-Galois.

2.1. Producto tensorial

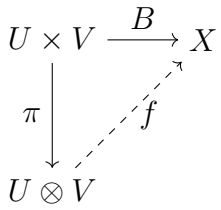
Para poder definir las álgebras de Hopf, tenemos que definir primero el producto tensorial, ya que es un concepto clave que proporciona una estructura adecuada para definir las operaciones fundamentales que caracterizan un álgebra de Hopf. Para desarrollar esta sección nos basaremos en la referencia [6], los prestigiosos apuntes universitarios del profesor Keith Conrad.

Definición 2.1. Dados dos espacios vectoriales U, V sobre un cuerpo K definimos su producto tensorial como el par $(U \otimes V, \pi)$, donde $U \otimes V$ es un K-espacio vectorial y $\pi : U \times V \to U \otimes V$ es una aplicación bilineal, tales que:

- $Im(\pi)$ genera $U \otimes V$
- Para toda aplicación bilineal $B : U \times V \longmapsto X$, existe una única transformación lineal $f : U \otimes V \longmapsto X$ tal que:

$$f \circ \pi = B.$$

A esta última propiedad se la conoce como la propiedad universal del producto tensorial y se puede expresar en forma de diagrama conmutativo de la siguiente manera:



En definitiva, el producto tensorial es el espacio vectorial $U \otimes V$ cuyos objetos son de la forma:

$$u_1 \otimes v_1 + u_2 \otimes v_2 + \cdots + u_k \otimes v_k,$$

donde $u_i \in U$ y que satisfacen:

Propiedades 2.2. *Sean $u, u_1, u_2 \in U, v, v_1, v_2 \in V, \alpha, \beta \in \mathbb{K}$ entonces:*

- $(\alpha u_1 + \beta u_2) \otimes v = \alpha(u_1 \otimes v) + \beta(u_2 \otimes v)$.
- $u \otimes (\alpha v_1 + \beta v_2) = \alpha(u \otimes v_1) + \beta(u \otimes v_2)$.
- $\alpha(u \otimes v) = (\alpha u) \otimes v = u \otimes (\alpha v)$.

Demostración. Es evidente ya que π es una forma bilineal. □

Proposición 2.3. *(Teorema 4.9 [5]) Dadas bases de U y V, suponiendo que son espacios vectoriales finitos, una base de $U \otimes V$ viene dada por los productos tensoriales de sus elementos. Es decir, si una base de U es $\{u_1, u_2, \ldots, u_j\}$ y una de V $\{v_1, v_2, \ldots, v_i\}$ una base de $U \otimes V$ es $\{v_n \otimes v_m | 1 \leq n \leq i, 1 \leq m \leq j\}$.*

Demostración. Primero comprobemos que el conjunto $S := \{v_n \otimes v_m | 1 \leq n \leq i, 1 \leq m \leq j\}$ forma un sistema generador.

Para ello, sean

$$u = \sum_{n=1}^{i} \alpha_n u_n,\ v = \sum_{m=1}^{j} \beta_m v_m,\ \alpha_n, \beta_m \in K.$$

Por las propiedades del producto tensorial tenemos

$$u \otimes v = \left(\sum_{n=1}^{i} \alpha_n u_n \right) \otimes \left(\sum_{m=1}^{j} \beta_m v_m \right) = \sum_{n=1}^{i} \sum_{m=1}^{j} \alpha_n \beta_m (u_n \otimes v_m),\ \alpha_n, \beta_m \in K,$$

y como cualquier elemento de $U \otimes V$ es combinación lineal de elementos de la forma $u \otimes v$ con $u \in U$, $v \in V$, tenemos lo que queríamos.Ahora, falta comprobar la independencia lineal de S, para ello supongamos que:

$$\sum_{i,j} c_{ij} u_i \otimes v_j = 0.$$

Queremos probar que todos los $c_{ij} = 0$. Para ello, escogemos un par de índices (i_0, j_0) y veamos que $c_{ij} = 0$.

Sea la aplicación bilineal $g : U \times V \longrightarrow X$ dada por $(u, v) \longmapsto u_{i_0} v_{i_0}$. Por la propiedad universal del producto tensorial existe una aplicación $f_0 : U \otimes V \longrightarrow X$ dada por $f_0(u \otimes v) = u_{i_0} v_{i_0}$ para todo $u \otimes v \in U \otimes V$.

En particular, para los elementos de la base $f_0(u_{i_0} \otimes v_{j_0}) = 1$ y $f_0(u_i \otimes v_j) = 1$ si $(i,j) \neq (i_0, j_0)$. Aplicando f_0 a $\sum_{i,j} c_{ij} u_i \otimes v_j = 0$, tenemos que $c_{i_0 j_0} = 0$. Como los índices i_0 y j_0 eran arbitrarios, tenemos que todos los coeficientes son cero. □

Corolario 2.4. *Sean U, V espacios vectoriales de dimensiones n y m sobre K respectivamente, entonces*

$$dim(U \otimes V) = nm.$$

Proposición 2.5. *El producto tensorial es único salvo isomorfismo.*

Demostración. Sean E, F dos K-espacios vectoriales. Supongamos que $E \otimes F$ y $E \tilde{\otimes} F$ son dos productos tensoriales de E y F. Veamos que son isomorfos. Sean

$$\begin{array}{cc} \varphi_1 : E \times F \longmapsto E \otimes F & \qquad \varphi_2 : E \times F \longmapsto E \tilde{\otimes} F \\ \varphi_1(x,y) = x \otimes y, & \qquad \varphi_2(x,y) = x \tilde{\otimes} y. \end{array}$$

Ahora bien, como φ_1 y φ_2 son aplicaciones bilineales, sean $f : E \otimes F \to X$ y $g : E \tilde{\otimes} F \to X$ las aplicaciones dadas por la definición de producto tensorial tal que $f \circ \varphi_1 = \varphi_2$ y $g \circ \varphi_2 = \varphi_1$.
Si combinamos ambas relaciones, obtenemos que:

$$(g \circ f)(\varphi_1(x,y)) = (g \circ f)(x \otimes y) = x \otimes y$$

y

$$(f \circ g)(\varphi_2(x,y)) = (f \circ g)(x \tilde{\otimes} y) = x \tilde{\otimes} y.$$

Vemos que $f \circ g = id_{E \otimes F}$ y $g \circ f = id_{E \tilde{\otimes} F}$ y como $im\varphi_1 = E \otimes F$ e $im\varphi_2 = E \tilde{\otimes} F$ obtenemos que $E \otimes F \cong E \tilde{\otimes} F$. □

Proposición 2.6. $E \otimes F \cong F \otimes E$.

Demostración. Sean las aplicaciones bilineales definidas como:

$$\begin{array}{cc} \varphi_1 : E \times F \longmapsto E \otimes F & \qquad \varphi_2 : E \times F \longmapsto F \otimes E \\ \varphi_1(x,y) = x \otimes y, & \qquad \varphi_2(x,y) = y \otimes x \end{array}$$

Como φ_2 es bilineal, por la propiedad universal del producto tensorial existe una aplicación $f : E \otimes F \longmapsto F \otimes E$ lineal tal que $f \circ \varphi_1 = \varphi_2$. Esto es $f(x \otimes y) = y \otimes x$.

Análogamente, existe una aplicación $g : F \otimes E \longmapsto E \otimes F$ que cumple que $g \circ \varphi_2 = \varphi_1$, esto es $g(y \otimes x) = x \otimes y$.

Entonces $g \circ f \circ \varphi_1 = g \circ \varphi_2 = \varphi_1$, lo que significa que $(g \circ f)(x \otimes y) = (x \otimes y)$. Ahora, como $im\varphi_1 = E \otimes F$ tenemos que $g \circ f = id$. Procediendo análogamente llegamos a que $f \circ g = id$. Por lo tanto, una es inversa de la otra, lo que concluye que $E \otimes F \cong F \otimes E$. □

Proposición 2.7. *(Teorema 5.2 [6])* $(E \otimes F) \otimes G \cong E \otimes (F \otimes G)$.

Demostración. Definamos la aplicación

$$\alpha : E \times F \times G \longmapsto E \otimes (F \otimes G) \tag{2.1}$$
$$\alpha(x, y, z) = x \otimes (y \otimes z) \tag{2.2}$$

Esta aplicación es trilineal, es decir, lineal en cada componente x, y, z por separado.

Ahora, por la propiedad universal del producto tensorial, existe una única aplicación lineal ta que:

$$\tilde{\alpha} : (E \otimes F) \otimes G \longmapsto E \otimes (F \otimes G) \tag{2.3}$$
$$\tilde{\alpha}((x \otimes y) \otimes z) = x \otimes (y \otimes z). \tag{2.4}$$

De manera análoga, definimos:

$$\beta : E \times F \times G \longmapsto (E \otimes F) \otimes G \tag{2.5}$$
$$\beta(x, y, z) = (x \otimes y) \otimes z. \tag{2.6}$$

y como antes, por la propiedad universal del producto tensorial existe una única aplicación lineal tal que:

$$\tilde{\beta} : E \otimes (F \otimes G) \longmapsto (E \otimes F) \otimes G \tag{2.7}$$
$$\tilde{\beta}(x, y, z) = (x \otimes y) \otimes z. \tag{2.8}$$

Veamos que $\tilde{\alpha}$ y $\tilde{\beta}$ son inversas.

Claramente $\beta \circ \alpha = id$ y $\alpha \circ \beta = id$ ya que

$$\tilde{\beta}(\tilde{\alpha}((x \otimes y) \otimes z)) = \tilde{\beta}(x \otimes (y \otimes z)) = (x \otimes y) \otimes z,$$

$$\tilde{\alpha}(\tilde{\beta}(x \otimes (y \otimes z))) = \tilde{\alpha}((x \otimes y) \otimes z) = x \otimes (y \otimes z).$$

Concluimos que $\tilde{\alpha}$ y $\tilde{\beta}$ son inversas entre sí, luego son isomorfismos. □

Definición 2.8. Sean $\varphi : U_1 \longrightarrow V_1$ y $\Phi : U_2 \longrightarrow V_2$ dos aplicaciones lineales entre espacios vectoriales. Definimos el producto tensorial de φ y Φ como la aplicación lineal tal que:

$$(\varphi \otimes \Phi) : U_1 \otimes U_2 \longrightarrow V_1 \otimes V_2 \tag{2.9}$$
$$(\varphi \otimes \Phi)(x \otimes y) = \varphi(x) \otimes \Phi(y) \tag{2.10}$$

2.2. Álgebras, coálgebras y biálgebras

2.2.1. Álgebras

Nota. Antes de empezar, vamos a aclarar una cuestión con la notación. A lo largo del capítulo, para la acción de un anillo sobre un módulo y para la multiplicación interna del anillo, unas veces usaremos la notación infija (yuxtaposición para el anillo y con punto para la acción) y otras veces notación prefija, usando una letra para la operación.

En esta sección presentamos la definición de álgebra de dos maneras; la manera usual, en la que todos conocemos el concepto, y la definición categórica mediante diagramas conmutativos.

Introducimos primero la manera usual:

Definición 2.9. Un **álgebra** sobre un cuerpo K es un espacio vectorial A provisto de un producto interno

$$m : A \times A \to A \tag{2.11}$$
$$(a, b) \mapsto ab, \tag{2.12}$$

que es una aplicación bilineal:

1. $a(b + c) = ab + ac$.

2. $(a+b)c = ac + bc$.

3. $(\lambda a)b = \lambda(ab) = a(\lambda b), \quad \forall \lambda \in K$.

Nota. Vamos a trabajar siempre con álgebras asociativas con unidad, es decir, $(ab)c = a(bc)$ $\forall a, b, c \in A$ y existe $1 \in A$ tal que $1a = a1$ para todo $a \in A$.

Para llegar a la definición categórica, antes vamos a dar una definición intermedia (que es claramente equivalente a la usual), entre la usual y la categórica, gracias a la propiedad universal del producto tensorial, de la siguiente manera:

Un álgebra asociativa y unitaria sobre un cuerpo es un espacio vectorial A provisto de una aplicación lineal que podemos definir por yuxtaposición como sigue:

$$m : A \otimes A \to A \tag{2.13}$$
$$m(a \otimes b) = ab \tag{2.14}$$

tal que

$$m(a \otimes m(b \otimes c)) = m(m(a \otimes b) \otimes c)$$

y

$$m(a \otimes 1) = m(1 \otimes a) = a$$

es decir, tal que

$$a(bc) = (ab)c$$

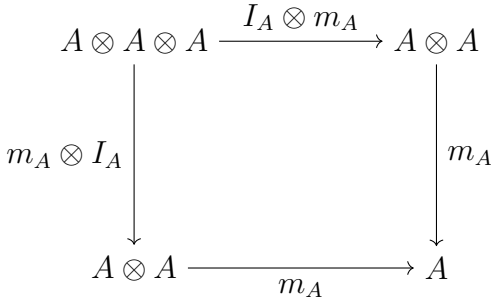
y

$$1a = a = a1.$$

Ahora veamos la definición categórica:[17]

Definición 2.10. Sea K un cuerpo. Una **K-álgebra** es una terna (A, m_A, λ_A) que consiste en un K-espacio vectorial y dos aplicaciones lineales $m_A : A \otimes A \to A$ y $\lambda_A : K \to A$ que satisfacen las siguientes condiciones:

1. El siguiente diagrama conmuta:



Donde hemos denotado por $I_A : A \longrightarrow A$ a la aplicación identidad.

Equivalentemente, para todo $a, b, c \in A$:

$$m_A(I_A \otimes m_A)(a \otimes b \otimes c) = m_A(m_A \otimes I_A)(a \otimes b \otimes c)$$

desarrollamos

$$m_A(I_A \otimes m_A)(a \otimes b \otimes c) = m_A(a \otimes m(b \otimes c)) = a(bc)$$

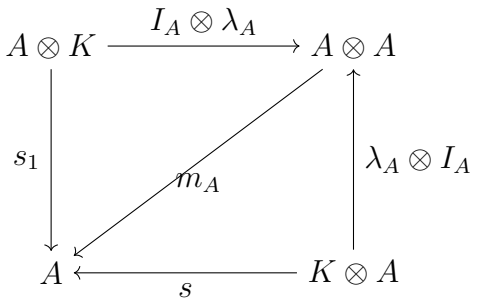
$$= m_A(m_A \otimes I_A)(a \otimes b \otimes c) = m_A(m(a \otimes b) \otimes c) = (ab)c.$$

donde, como antes hemos denotado el producto por yuxtaposición.

Efectivamente define la propiedad asociativa.

El diagrama se llama diagrama de multiplicación y la propiedad equivalente se llama propiedad asociativa.

2. El siguiente diagrama conmuta:



Donde $s : K \otimes A \longmapsto A$ con $s(r \otimes a) = ra$ y s_1 se define de manera análoga.

Equivalentemente, tenemos que para todo $r \in K$, $a \in A$,

$m_A(I_A \otimes \lambda_A)(a \otimes r) = m_A(I_A(a) \otimes \lambda_A(r)) = m_A(a \otimes (r \cdot 1)) = a(r \cdot 1) =$

$= m_A(\lambda_A \otimes I_A)(r \otimes a) = m_A(\lambda_A(r) \otimes I_A(a)) = m_A((r \cdot 1) \otimes a) = (r \cdot 1)a.$

La aplicación λ_A se llama unidad y la propiedad equivalente se llama propiedad de la unidad.

La K-álgebra es **conmutativa** sí $m_A\tau = m_A$, donde la aplicación lineal $\tau : A \otimes A \longrightarrow A \otimes A$ definida por $\tau(a \otimes b) = b \otimes a$ denota la permutación de dos elementos.

Ejemplo 2.11. El cuerpo K es un álgebra sobre sí mismo con las aplicaciones $m_K : K \otimes K \longrightarrow K$ definida por $m_K(r \otimes s) = rs$ y $\lambda_K : K \longrightarrow K$ dada por $\lambda_K(r) = r$.

Ejemplo 2.12. Sea G un grupo con 1 su elemento unidad. El anillo de grupo $K[G] = \left\{\sum_{g \in G} r_g g : r_g \in K, r_g \neq 0\right\}$ es el espacio vectorial sobre K con base G; cada elemento de G es un elemento de la base de $K[G]$. Esta estructura define un álgebra llamada álgebra de grupo. Veamos sus operaciones:

Su multiplicación se define como:

$$m_{K[G]} : K[G] \otimes K[G] \longrightarrow K[G]$$
$$m_{K[G]}(\sum_{g,h} a_g b_h (g \otimes h)) = \sum_{g,h} a_g b_h (gh).$$

y su unidad:

$$\lambda_{K[G]} : K \to K[G]$$
$$\lambda_{K[G]}(r) = r \cdot 1.$$

Claramente $K[G]$ es conmutativa si, y solo si, G es abeliano.

Ejemplo 2.13. Sea, A, B dos $K-$álgebras. El producto tensorial de ambas es una K-álgebra junto con:

- Multiplicación:

$$m_{A \otimes B} : (A \otimes B) \otimes (A \otimes B) \longmapsto A \otimes B,$$

definida como

$$m_{A \otimes B}((a \otimes b) \otimes (c \otimes d)) = (m_A \otimes m_B)(I_A \otimes \tau \otimes I_B)(a \otimes (b \otimes c) \otimes d)$$

$$= (m_A \otimes m_B)(a \otimes (c \otimes b) \otimes d) = (m_A \otimes m_B)((a \otimes c) \otimes (b \otimes d)) = ac \otimes bd,$$
$$\forall a, c \in A \quad b, d \in B$$

- Unidad
$$\lambda_{A\otimes B} : K \longmapsto A \otimes B,$$
definida por
$$\lambda_{A\otimes B}(r) = \lambda_A(r) \otimes 1_B \quad \forall r \in K$$

2.2.2. Módulos sobre álgebras

Los módulos son una generalización de los espacios vectoriales, en la que en vez de definir la operación externa sobre un cuerpo, la definimos sobre un anillo, es decir, de acuerdo a [14] tenemos:

Definición 2.14. Supongamos que R es un anillo unitario y M un grupo aditivo. Decimos que M es un R**-módulo** (por la izquierda) si existe una aplicación llamada **acción** de R sobre M

$$R \times M \to M \tag{2.15}$$
$$(r, x) \longmapsto r \cdot x \tag{2.16}$$

que verifica las siguientes propiedades:

1. $(r + s) \cdot x = r \cdot x + s \cdot x$.
2. $r(x + y) = r \cdot x + r \cdot y$.
3. $(rs) \cdot x = r \cdot (sx)$.
4. $1_R \cdot x = x$.

Definición 2.15. Sean M, N dos R-módulos donde R es un anillo. Un **homomorfismo de módulos** es una aplicación lineal $\varphi : M \to N$ que satisface las siguientes propiedades:

1. Compatibilidad con la suma
$$\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2) \ \ \forall m_1, m_2 \in M.$$

2. Compatibilidad con la multiplicación por escalares (acción de R):
$$\varphi(r \cdot m) = r \cdot \varphi(m) \ \ \forall r \in R \ \ y \ \ m \in M.$$

Ahora bien, como un álgebra es un anillo con una operación adicional de multiplicación por escalares, podemos definir un módulo sobre un álgebra de la misma manera, usando la estructura de anillo del álgebra.

Vemos la definición categórica:

Definición 2.16. Sea A una K-álgebra. Un **A-módulo por la izquierda** es un par (M, μ_M) que está formado por un K-espacio vectorial M y una aplicación lineal $\mu_M : A \otimes M \longmapsto M$ que satisface:

- La propiedad de asociatividad $\mu_M(I_A \otimes \mu_M) = \mu_M(m_A \otimes I_M)$: denotando $m_A(a \otimes b) = ab$ y $\mu_M(a \otimes m) = a \cdot m$; desarrollando a ambos lados tenemos:

$$\mu_M(I_A \otimes \mu_M)(a \otimes b \otimes r) = \mu_M(a \otimes (b \cdot r)) = a \cdot (b \cdot r)$$

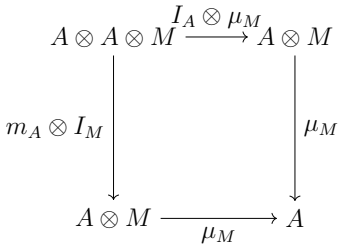
$$= \mu_M(m_A \otimes I_M)(a \otimes b \otimes r) = \mu_M((ab) \otimes r) = (ab) \cdot r.$$

- La unidad $\mu_M(\lambda_A \otimes I_M) = \eta$ donde $\eta : K \otimes M \longmapsto M$ está dada por la identificación natural $\eta(1_K \otimes m) = m$

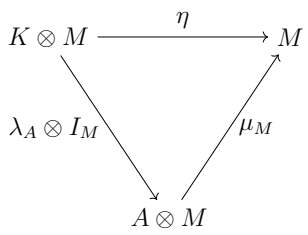
  Desarrollamos:

$$\mu_M(\lambda_A \otimes I_M)(k \otimes m) = \mu_M(k \cdot 1_A \otimes m) = (k \cdot 1_A) \cdot m = k \cdot m.$$

En forma de diagrama conmutativo



Asociatividad

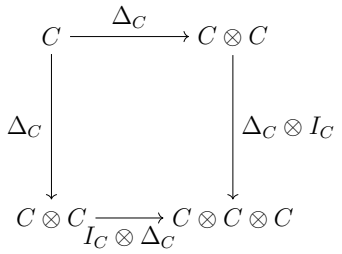


Unidad

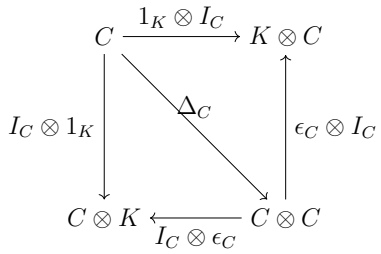
2.2.3. Coálgebras

El concepto de coálgebra es dual al concepto de álgebra. Queremos operaciones duales a las de multiplicación y unidad de un álgebra; por ejemplo, en vez de una aplicación que multiplique dos elementos, queremos una que tome un elemento y lo "parta en dos", obteniendo así una operación que se denomina comultiplicación.

Veamos ahora la definición de coálgebra, que como acabamos de decir, es dual a la de álgebra asociativa. Esto es, invierte los diagramas conmutativos de asociatividad y unidad que hemos visto antes en la definición categórica, dándoles el nombre de coasociatividad y counidad:



Coasociatividad



Counidad

Donde $I_C : C \longmapsto C$ es la identidad en C. De aquí obtenemos la definición:

Definición 2.17. Una **coálgebra** sobre un cuerpo K es un K-espacio vectorial C tal que:

1. Existe una transformación lineal $\Delta : C \to C \otimes C$ llamada **coproducto** tal que $(\Delta_C \otimes I_C)\Delta_C = (I_C \otimes \Delta_C)\Delta_C$ (**coasociatividad**)

2. Existe una transformación lineal $\epsilon_C : C \to K$ tal que $(I_C \otimes \epsilon_C)\Delta_C(c) = c \otimes 1$ y $(\epsilon_C \otimes I_C)\Delta_C(c) = 1 \otimes c$ (**counidad**)

Una coálgebra se dice **coconmutativa** si $\tau\Delta_C = \Delta_C$ siendo τ la permutación de los factores de $C \otimes C$, es decir, $\tau : C \otimes C \longmapsto C \otimes C$ tal que $\tau(a \otimes b) = b \otimes a$

Definimos la notación de Sweedler como:

$$\Delta_C(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}.$$

Con esta notación la propiedad de coasociatividad queda:

$$(I_C \otimes \Delta_C)\Delta_C(c) = (I_C \otimes \Delta_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right)$$

$$= \sum_{(c)} c_{(1)} \otimes \Delta_C(c_{(2)}) = \sum_{(c)} c_{(1)} \otimes c_{(2)(1)} \otimes c_{(2)(2)},$$

y del otro lado

$$(\Delta_C \otimes I_C)\Delta_C(c) = (\Delta_C \otimes I_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right)$$

$$= \sum_{(c)} \Delta_C(c_{(1)}) \otimes c_{(2)} = \sum_{(c)} c_{(1)(1)} \otimes c_{(1)(2)} \otimes c_{(2)}$$

por tanto, gracias a la coasociatividad podemos extender la notación de Sweedler sin ambigüedad:

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

Para la counidad, la notación de Sweedler quedaría como:

$$(I_C \otimes \epsilon_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) = \sum_{(c)} c_{(1)} \otimes \epsilon_c(c_{(2)}) = \sum_{(c)} \epsilon_c(c_{(2)})c_{(1)} \otimes 1 = c \otimes 1,$$

lo que equivale a,

$$\sum_{(c)} \epsilon_c(c_c(c_{(2)})c_{(1)} = c.$$

y del otro lado:

$$(\epsilon_C \otimes I_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) = \sum_{(c)} \epsilon_c(c_{(1)}) \otimes c_{(2)} = \sum_{(c)} 1 \otimes \epsilon_c(c_{(1)})c_{(2)} = 1 \otimes c,$$

lo que equivale a

$$\sum_{(c)} \epsilon_c(c_{(1)})c_{(2)} = c.$$

Ejemplo 2.18. K es una coálgebra con $\Delta_K(\lambda) = \lambda(1 \otimes 1)$ y $\epsilon(\lambda) = \lambda$ para todo $\lambda \in K$. Verifiquemos las propiedades:

- Coasociatividad: $(\Delta_K \otimes I_K) \circ \Delta_K(\lambda) = (I_K \otimes \Delta_K) \circ \Delta_K(\lambda)$

  Lado izquierdo:

  $$\Delta_K(\lambda) = \lambda(1 \otimes 1) \implies (\Delta_K \otimes I_K)(\lambda(1 \otimes 1)) = \lambda(\Delta_K(1) \otimes 1) = \lambda(1 \otimes 1 \otimes 1)$$

  Lado derecho:

  $$(I_K \otimes \Delta_K)(\lambda(1 \otimes 1)) = \lambda(1 \otimes \Delta_K(1)) = \lambda(1 \otimes 1 \otimes 1)$$

- Counidad: $(\epsilon_K \otimes I_K) \circ \Delta_K = 1 \otimes \lambda \ \ (I_K \otimes \epsilon_K) \circ \Delta_K = \lambda \otimes 1$.

  Lado izquierdo:

  $$(\epsilon_K \otimes I_K)(\lambda(1 \otimes 1)) = \lambda(1 \otimes 1) = 1 \otimes \lambda.$$

  Lado derecho:

  $$(I_K \otimes \epsilon_K)(\lambda(1 \otimes 1)) = \lambda(1 \otimes 1) = \lambda \otimes 1.$$

Por tanto, se cumplen las propiedades de coálgebra.

Ejemplo 2.19. Sea G un grupo y $K[G]$ el álgebra de grupo sobre el cuerpo K. Entonces $K[G]$ es una coálgebra coconmutativa con las operaciones:

- $\Delta_G(g) = g \otimes g$, $\forall g \in G$,
- $\epsilon_G(g) = 1$, $\forall g \in G$.

En efecto, si $\sum_{g \in G} r_g g \in K[G]$,

$$\Delta_G \otimes I_G \left(\Delta_G \left(\sum_{g \in G} r_g g \right) \right) = \Delta_G \otimes I_G \left(\sum_{g \in G} r_g (g \otimes g) \right)$$

$$= \sum_{g\in G} r_g(\Delta_G(g\otimes g) = \sum_{g\in G} r_g(g\otimes g\otimes g)$$

$$= I_G \otimes \Delta_G\left(\Delta_G\left(\sum_{g\in G} r_g g\right)\right).$$

Así, Δ es coasociativa. También,

$$I_G \otimes \epsilon_G\left(\Delta_G\left(\sum_{g\in G} r_g g\right)\right) = I_G \otimes \epsilon_G\left(\sum_{g\in G} r_g(g\otimes g)\right)$$

$$= \sum_{g\in G} r_g(g\otimes \epsilon_G(g)) = \sum_{g\in G} r_g(g\otimes 1)$$

$$= \left(\sum_{g\in G} r_g g\right)\otimes 1$$

y del otro lado, operando igual

$$\epsilon_G \otimes I_G\left(\Delta_G\left(\sum_{g\in G} r_g g\right)\right) = 1\otimes\left(\sum_{g\in G} r_g g\right).$$

Por lo tanto, ϵ cumple con la condición de la counidad.

Veamos por último que es coconmutativa.

$$\tau\left(\Delta_G\left(\sum_{g\in G} r_g g\right)\right) = \tau\left(\sum_{g\in G} r_g(g\otimes g)\right)$$

$$= \sum_{g\in G} r_g(g\otimes g) = \Delta_G\left(\sum_{g\in G} r_g g\right).$$

Ejemplo 2.20. Sean A, B dos K-coálgebras. El producto tensorial $A\otimes B$ es una K-coálgebra junto con:

- Comultiplicación

$$\Delta_{A\otimes B} : A \otimes B \longrightarrow (A \otimes B) \otimes (A \otimes B) \tag{2.17}$$
$$\Delta_{A\otimes B}(a \otimes b) = I_A \otimes \tau_{A,B} \otimes I_B \circ \Delta_A \otimes \Delta_B(a \otimes b) \tag{2.18}$$

Donde $\tau_{A,B} : A\otimes B \to B\otimes A$ es la aplicación lineal tal que $\tau(a\otimes b) = b\otimes a$ para todos $a \in A$, $b \in B$.

Verificamos la coasociatividad: $(\Delta_{A\otimes B} \otimes I_{A\otimes B}) \circ \Delta_{A\otimes B} = (I_{A\otimes B} \otimes \Delta_{A\otimes B}) \circ \Delta_{A\otimes B}$

Lado izquierdo:

$$(\Delta_{A\otimes B} \otimes I_{A\otimes B})(a \otimes b \otimes a \otimes b) = \Delta_{A\otimes B}(a \otimes b) \otimes I_{A\otimes B}(a \otimes b) =$$

$$= a \otimes b \otimes a \otimes b \otimes a \otimes b.$$

Lado derecho:

$$(I_{A\otimes B} \otimes \Delta_{A\otimes B})(a \otimes b \otimes a \otimes b) = I_{A\otimes B}(a \otimes b) \otimes \Delta_{A\otimes B}(a \otimes b) =$$

$$= a \otimes b \otimes a \otimes b \otimes a \otimes b.$$

Ambos lados son iguales por la coasociatividad de Δ_A y Δ_B, por tanto $\Delta_{A\otimes B}$ es coasociativa

- Counidad:

$$\epsilon_{A\otimes B} : A \otimes B \longrightarrow K \tag{2.19}$$
$$\epsilon_{A\otimes B}(a \otimes b) := \epsilon_A(a) \cdot \epsilon_B(b) \tag{2.20}$$

Verificamos la propiedad $(\epsilon_{A\otimes B} \otimes I_{A\otimes B}) \circ \Delta_{A\otimes B} = I_{A\otimes B} \otimes 1$

$(I_{A\otimes B} \otimes \epsilon_{A\otimes B}) \circ \Delta_{A\otimes B} = 1 \otimes I_{A\otimes B}$

$$(\epsilon_{A\otimes B} \otimes I_{A\otimes B}) \circ \Delta_{A\otimes B}(a \otimes b) = \sum_{(a,b)} \epsilon_A(a_{(1)}) \cdot \epsilon_B(b_{(1)}) \otimes (a_{(2)} \otimes b_{(2)})$$

$$= \sum_{(a,b)} 1 \otimes \epsilon_A(a_{(1)})a_{(2)} \otimes \epsilon_B(b_{(1)})b_{(2)} = 1 \otimes a \otimes b.$$

El otro lado se cálcula de manera ánaloga llegando a lo mismo. Por tanto, la propiedad de counidad se cumple.

Definición 2.21. Sean $(C, \Delta_C, \epsilon_C)$ y $(D, \Delta_D, \epsilon_D)$ coálgebras. Un homomorfismo de coálgebras es una transformación lineal $\phi : C \to D$ tal que:

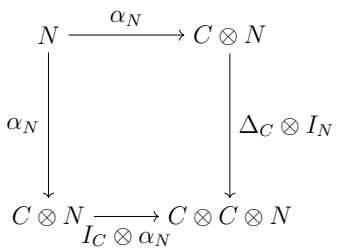
i) $(\phi \otimes \phi)\Delta_C(c) = \Delta_D(\phi(c))$ para todo $c \in C$.

ii) $\epsilon_C(c) = \epsilon_D(\phi(c))$ para todo $c \in C$.

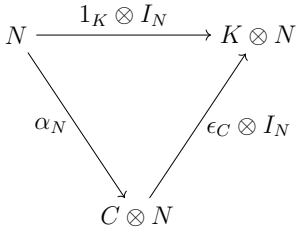
2.2.4. Comódulos sobre coálgebras

Dualizando la noción de módulos para álgebras, podemos definir los **comódulos de coálgebras**,

Definición 2.22. Sea C una coálgebra. Un **C-comódulo por la izquierda** es un par (N, α_N) formado por un K-espacio vectorial y una transformación lineal $\alpha_N : N \to C \otimes N$ llamada **coacción** de C en N que satisface:



Coasociatividad



Counidad

Antes de ver las propiedades, vamos a explicar cómo funciona la notación de Sweedler para esta estructura.

Tenemos la aplicación $\alpha : N \longrightarrow C \otimes N$ que en notación de Sweedler se expresa como $\alpha_N(a) = \sum_{(a)} a_{(1)} \otimes a_{(0)}$ y en el diagrama aparece el producto tensorial $I_C \otimes \alpha_N : C \otimes N \longrightarrow C \otimes C \otimes N$ que quedaría como

$$(I_C \otimes \alpha_N)(a_{(1)} \otimes a_{(0)}) = \sum_{(a)} a_{(1)} \otimes a_{(2)} \otimes a_{(0)}.$$

Por tanto, con esta notación diferenciamos con los índices positivos los elementos que pertenecen a la coálgebra C y con el índice 0 al elemento que

pertenece al comódulo N. En los casos en los que aparece más de un elemento del comódulo N en la operación, se van usando índices con números negativos sucesivos: $(-1), (-2)$, etc.

Ya estamos en condiciones de poder desarrollar las propiedades:

- La coasociatividad. $(\Delta_C \otimes I_N)\alpha_N = (I_C \otimes \alpha_N)\alpha_N$. Desarrollamos ambos lados:

  $$(\Delta_C \otimes I_N)\alpha_N(k) = (\Delta_C \otimes I_N)(\sum_{(k)} k_{(1)} \otimes k_{(0)}) = \sum_{(k)} k_{(1)(1)} \otimes k_{(1)(2)} \otimes k_{(0)}$$

  El otro lado;

  $$(I_C \otimes \alpha_N)\alpha_N(k) = (I_C \otimes \alpha_N)(k_{(1)} \otimes k_{(0)}) = \sum_{(a)} k_{(1)} \otimes k_{(0)(1)} \otimes k_{(0)(0)}$$

  De esta manera, gracias a esta propiedad afirmamos que:

  $$\sum_{(a)} k_{(1)} \otimes k_{(0)(1)} \otimes k_{(0)(0)} = \sum_{(k)} k_{(1)(1)} \otimes k_{(1)(2)} \otimes k_{(0)} = \sum_{(k)} k_{(1)} \otimes k_{(2)} \otimes k_{(0)}$$

- La counidad. $(\epsilon_C \otimes I_N)\alpha_N = 1_K \otimes I_N$.

  Desarrollando:

  $$(\epsilon_C \otimes I_N)\alpha_N(k) = (\epsilon_C \otimes I_N) \sum_{(k)} k_{(1)} \otimes k_{(0)} = \sum_{(k)} \epsilon_C(k_{(1)}) \otimes k_{(0)} = 1_K \otimes k$$

Definición 2.23. Sea C una K-coálgebra . Un elemento $c \in C$ distinto de cero se dice **grupal (group-like)** si $\Delta_C(c) = c \otimes c$.

Proposición 2.24. *([17]Proposición 1.2.16) Sea c un elemento grupal de una K-coálgebra C. Entonces satisface $\epsilon_C(c) = 1$.*

Demostración. Como c es un elemento grupal,

$$c = m\left((\epsilon_C \otimes I_C)\Delta_C(c)\right) = m\left((\epsilon_C \otimes I_C)(c \otimes c)\right) = m\left(\epsilon_C(c) \otimes c\right)$$
$$= \epsilon_C(c)c \Rightarrow \epsilon_C(c)c = c = 1c \Rightarrow (\epsilon_C(c) - 1)c = 0.$$

donde m es la aplicación definida por $m(a \otimes b) = ab$ y la primera igualdad se da por la propiedad de counidad de coálgebra.

Como $c \neq 0$ tenemos que $\epsilon_C(c) - 1 = 0 \Rightarrow \epsilon_C(c) = 1$. □

Proposición 2.25. *(Proposición 1.2.20 [17]) Sea $\phi : C \longmapsto D$ un homomorfismo de coálgebras. Si c es un elemento grupal de C, entonces $\phi(c)$ es un elemento grupal de D.*

Demostración. Como ϕ es un homomorfismo de coálgebras, y además c es un elemento grupal, sabemos que

$$\Delta(\phi(c)) = \phi \otimes \phi(\Delta(c)) = \phi \otimes \phi(c \otimes c) = \phi(c) \otimes \phi(c).$$

□

Definición 2.26. Sea C una coálgebra. Un elemento **primitivo** de C es un elemento $c \in C$ tal que $\Delta(c) = 1 \otimes c + c \otimes 1$.

Nota. Recordemos que **el espacio dual** V^* de un K-espacio vectorial V es el conjunto de todas las aplicaciones lineales de V en K, $V^* = Hom_K(V, K)$. Aunque en este trabajo no vamos a profundizar en esto, en el contexto en el que estamos de álgebras y coálgebras, este espacio toma gran importancia ya que el dual de una coálgebra se puede dotar de una estructura de álgebra y, de manera casi recíproca, el espacio de un álgebra de dimensión finita se puede dotar de una estructura de coálgebra (véase Sección 1.2,[15])

2.2.5. Biálgebras

Veamos ahora las biálgebras, esto son, espacios vectoriales que a la vez son álgebras y coálgebras, donde las operaciones de coálgebra son homomorfismos de las de álgebra. Para desarrollar este apartado nos basamos en las referencias [8] y [17].

Definición 2.27. Una **biálgebra** es un espacio vectorial B que verifica las siguientes condiciones:

1. B es un álgebra.
2. B es coálgebra.
3. $\Delta : B \to B \otimes B$ y $\epsilon : B \to K$ son homomorfismos de álgebras.

Una biálgebra B es **conmutativa** si es un álgebra conmutativa; B es coconmutativa si es una coálgebra coconmutativa.

Nota. Si B es una biálgebra, sus operaciones como álgebra también son homomorfismos de coálgebras.

Ejemplo 2.28. El cuerpo K como espacio vectorial sobre sí mismo es una K-biálgebra conmutativa y coconmutativa. Se llama la K-biálgebra trivial. Para demostrarlo solo nos resta ver que la counidad y la comultiplicación que hemos definido en el ejemplo 2.18 son homomorfismos de álgebras, es decir:

$$1)\ \Delta_K(ab) = \Delta_K(a)\Delta_K(b)\ \ \forall\ a, b \in K$$

Desarrollamos

$$\Delta(a)\Delta(b) = (a \otimes a)(b \otimes b) = (ab) \otimes (ab) = \Delta(ab).$$

y además $\Delta_K(1) = 1 \otimes 1$.

$$2)\ \epsilon(ab) = \epsilon(a)\epsilon(b).$$

Esta es clara ya que $\epsilon(ab) = 1$ y $\epsilon(a)\epsilon(c) = 1 \cdot 1 = 1$.

Ejemplo 2.29. Sea G un grupo. Ya hemos visto en el ejemplo 2.19 que $K[G]$ tiene estructura de coálgebra. Vemos ahora que la comultiplicación y la counidad son homomorfismos de álgebras. Es decir, definiendo las operaciones de coálgebra como:

- Coproducto:

  Sean $x = \sum_{g\in G} a_g g$, $y = \sum_{h\in G} b_h h$ dos elementos de $K[G]$.

  Queremos ver que

  $$\Delta(xy) = \Delta(x)\Delta(y)$$

  Desarrollemos ambos lados.

  Lado izquierdo:

  $$\Delta(xy) = \sum_{g,h} a_g b_h \Delta(gh) = \sum_{g,h} a_g b_h (gh \otimes gh).$$

  Lado derecho:

  $$\Delta(x)\Delta(y) = \sum_{g} a_g \Delta(g) \sum_{h} b_h \Delta(h) = \sum_{g} a_g (g \otimes g) \sum_{h} b_h (h \otimes h)$$

$$= \sum_{g,h} a_g b_h (gh \otimes gh).$$

Veamos además que $\Delta(1_{K[G]}) = 1_{K[G]\otimes K[G]}$.

$$\Delta(1_{K[G]}) = 1_{K[G]} \otimes 1_{K[G]} = 1_{K[G]\otimes K[G]},$$

ya que $\Delta(e) = e \otimes e$ donde e es el elemento neutro.

- Counidad

  Queremos ver que

  $$\epsilon(xy) = \epsilon(x)\epsilon(y).$$

  Desarrollando ambos lados

  $$\epsilon(xy) = \sum_{g,h} a_g b_h \epsilon(gh) = \sum_{g,h} a_g b_h$$

  y

  $$\epsilon(x)\epsilon(y) = \sum_{g} a_g \sum_{h} b_h = \sum_{g,h} a_g b_h.$$

  Por último, se tiene por definición que $\epsilon(1_{K[G]}) = 1$.

  $K[G]$ se llama biálgebra de grupo. Es conmutativa si, y solo si, G es abeliano.

Definición 2.30. Sean B, B' dos K-biálgebras. Un homomorfismo de biálgebras es una aplicación $\phi : B \to B'$ que es a la vez un homomorfismo de K-álgebras y un homomorfismo de K-coálgebras.

2.2.6. Álgebras y coálgebras de módulos y comódulos

En esta sección veremos cómo una biálgebra B puede actuar sobre un álgebra o una coálgebra dotándolos con una estructura de B-módulo sobre álgebras o coálgebras, respectivamente. Las referencias principales para esta sección es [15] y [1].

Definición 2.31. Sea B una K-biálgebra. Una K-**álgebra** de un B-**módulo por la izquierda** (B-module álgebra) es un K-espacio vectorial M junto con las aplicaciones lineales $m_M : M \otimes M \to M$, $\lambda_M : K \to M$, y una acción $\mu_M : B \otimes M \to M$ que satisface:

1. (M, μ_M) es un B-módulo.
2. (M, m_M, λ_M) es una K-álgebra.
3. La acción de B sobre M es compatible con la operación de M como álgebra, esto es:

   $$\underline{Multiplicación} : b \cdot (mn) = \sum_{(b)} (b_{(1)} \cdot m)(b_{(2)} \cdot n), \ \ \forall b \in B, \ \ m, n \in M.$$

   Equivalentemente, el siguiente diagrama es conmutativo:

   $$\begin{array}{ccccc} B \otimes M \otimes M & \xrightarrow{I_B \otimes m_M} & B \otimes M & \xrightarrow{\mu_M} & M \\ \downarrow{\scriptstyle \Delta_B \otimes I_{M\otimes M}} & & & & \uparrow{\scriptstyle m_M} \\ B \otimes B \otimes M \otimes M & \xrightarrow[I_B \otimes \tau \otimes I_M]{} & B \otimes M \otimes B \otimes M & \xrightarrow[\mu_M \otimes \mu_M]{} & M \otimes M \end{array}$$

   $\underline{Unidad} : b \cdot 1_M = \epsilon_B(b) 1_M, \ \ \forall b \in B.$

   Equivalentemente el siguiente diagrama es conmutativo:

   $$\begin{array}{ccc} B \otimes M & \xrightarrow{\mu_M} & M \\ & {\scriptstyle \epsilon_B \otimes I_M} \searrow \quad \nearrow {\scriptstyle \eta} & \\ & K \otimes M & \end{array}$$

   donde $\eta : K \otimes M \longmapsto M$ representa la identificación natural $\eta(1 \otimes m) = m$.

Definición 2.32. Sean M, M' K-álgebras de B-módulos por la izquierda. Un homomorfismo de K-álgebras de $B-$módulos por la izquierda de M a

M' es una aplicación lineal $\phi : M \to M'$ que es la vez un homomorfismo de álgebras y un homomorfismo de B-módulos por la izquierda

Si dualizamos los conceptos de módulo y de álgebra, obtenemos otras 3 definiciones similares que vemos a continuación.

Definición 2.33. Sea B una K-biálgebra. Una **K-coálgebra** de B-**módulo** por la izquierda *(B-module coalgebra)* es un K-espacio vectorial M junto con las aplicaciones lineales $\Delta_M : M \to M \otimes M$, $\epsilon_M : B \otimes M \to K$, y una acción $\mu_M : B \otimes M \to M$ que satisface:

1. (M, μ_M) es un B-módulo,
2. $(M, \Delta_M, \epsilon_M)$ es una K-coálgebra,
3. La acción de B sobre M es compatible con la operación de M como coálgebra, esto es:

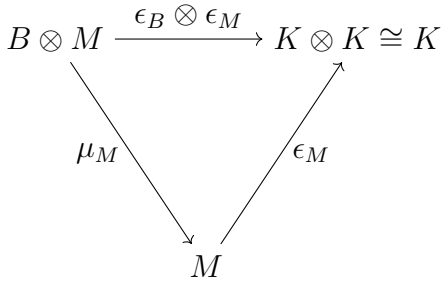
   $$\underline{Comultiplicacin} : \Delta_M(b{\cdot}m) = \sum_{(b,m)} (b_{(1)}{\cdot}m_{(1)}) \otimes (b_{(2)}{\cdot}m_{(2)}), \ \ \forall b \in B, \ \ m \in M.$$

   Equivalentemente, el siguiente diagrama es conmutativo:

$$\begin{array}{ccccc} B \otimes M & & \xrightarrow{\quad\mu_M\quad} & & M \xrightarrow{\quad\Delta_M\quad} M \otimes M \\ \Big\downarrow{\scriptstyle \Delta_B \otimes \Delta_M} & & & & \Big\uparrow{\scriptstyle \mu_M \otimes \mu_M} \\ B \otimes B \otimes M \otimes M & & \xrightarrow[I_B \otimes \tau \otimes I_M]{} & & B \otimes M \otimes B \otimes M \end{array}$$

   $$\underline{Counidad} : \epsilon_M(b \cdot m) = \epsilon_B(b)\epsilon_M(m), \ \ \forall b \in B.$$

   Equivalentemente el siguiente diagrama es conmutativo:



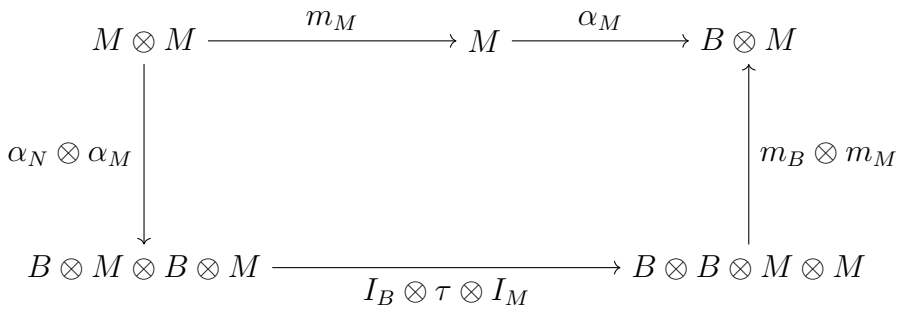
Definición 2.34. Sean M, M' K-álgebras de B-módulo por la izquierda. Un homomorfismo de K-coálgebras de B-módulo por la izquierda de M a M' es una aplicación lineal $\phi : M \to M'$ que es la vez un homomorfismo de coálgebras y un homomorfismo de B-módulos por la izquierda.

Definición 2.35. Sea B una K-biálgebra. Una **K-álgebra** de **B-comódulo por la izquierda** es un K-espacio vectorial M junto con las aplicaciones lineales $m_M : M \otimes M \to M$, $\lambda_M : K \to M$, y una coacción $\alpha_M : M \to B \otimes M$ que satisface:

1. (M, α_M) es un B-comódulo.
2. (M, m_M, λ_M) es una K-álgebra.
3. La coacción de B sobre N es compatible con la operación de M como álgebra, esto es:

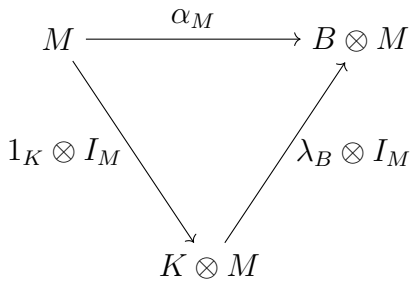
   $$\underline{Multiplicación} : \alpha_N(mn) = \sum_{(n,m)} (n_{(-1)} \cdot m_{(-1)}) \otimes (n_{(0)} \cdot m_{(0)}), \ \ \forall n, m \in M$$

   Equivalentemente, el siguiente diagrama es conmutativo:



Unidad : $\alpha_M(1_M) = 1_B \otimes 1_K$.

Equivalentemente el siguiente diagrama es conmutativo:



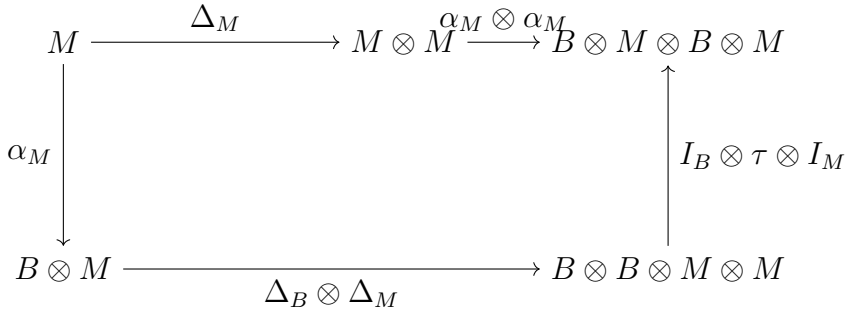
Definición 2.36. Sean M, M' K-álgebras de B-comódulos por la izquierda. Un homomorfismo de K-álgebras de $B-$comódulos por la izquierda de M a M' es una aplicación lineal $\phi : M \to M'$ que es a la vez un homomorfismo de álgebras y un homomorfismo de B-comódulos por la izquierda.

Definición 2.37. Sea B una K-biálgebra. Una **K-coálgebra** de **B-comódulo por la izquierda** es un K-espacio vectorial M junto con aplicaciones lineales $\Delta_M : M \to M \otimes M$, $\epsilon_M : M \to K$, y una acción $\alpha_M : M \to B \otimes M$, que satisface:

1. (M, α_M) es un B-comódulo.
2. $(M, \Delta_M, \epsilon_M)$ es una K-coálgebra.
3. La coacción de B sobre M es compatible con la operación de M como coálgebra, esto es:

$$\textit{Comultiplicación} : \alpha_M \otimes \alpha_M \left(\sum_{(m)} m_{(1)} \otimes m_{(2)} \right) =$$

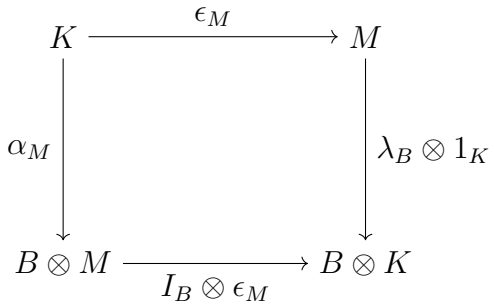
$$\sum_{(m)} (m_{(-1)} \otimes m_{(1)}) \otimes (m_{(0)} \otimes m_{(2)}), \quad \forall m \in M.$$



Counidad: $(I_B \otimes \epsilon_M)\alpha_M(m) = (\lambda_B \otimes 1_K)\epsilon_M(m)$

y por tanto $\sum_{(m)} \epsilon_M(m_{(0)})m_{(1)} \otimes 1_K$,

lo que lleva a $\sum_{(m)} \epsilon_M(m_{(0)})m_{(1)} = \lambda_B\epsilon_M(m)$, $\forall m \in M$.



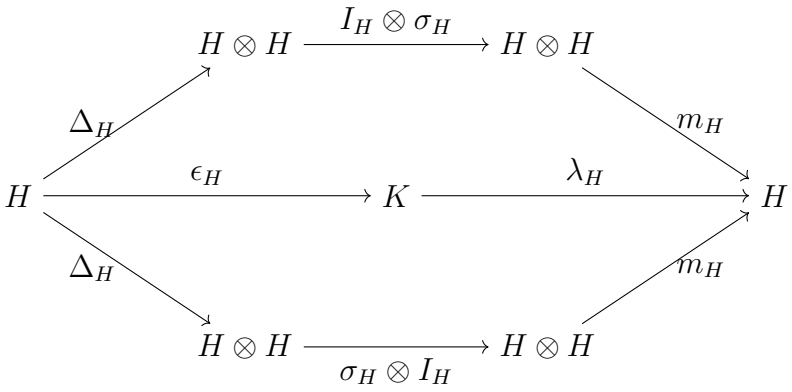
Definición 2.38. Sean M, M' K-coálgebras de B-comódulos por la izquierda. Un homomorfismo de K-coálgebras de B-comódulos por la izquierda de M a M' es una aplicación lineal $\phi : M \to M'$ que es a la vez un homomorfismo de coálgebras y un homomorfismo de B-comódulos por la izquierda.

2.3. Álgebras de Hopf

Finalmente, en esta sección introducimos el concepto de álgebra de Hopf. Estas son biálgebras con una aplicación lineal más que se llama antípoda. Veremos también, que esta antípoda es un anti-endomorfismo de coálgebras y un anti-endomorfismo de álgebras.

Definición 2.39. Una K-**álgebra de Hopf** es una K-biálgebra $(H, m_H, \lambda_H, \Delta_H, \epsilon_H)$

junto con una aplicación lineal $\sigma_H : H \to H$ de tal manera que el siguiente diagrama conmuta:



esto es

$$\lambda_H \circ \epsilon_H = m_H \circ (I_H \otimes \sigma_H) \circ \Delta_H = m_H \circ (\sigma_H \otimes I_H) \circ \Delta_H$$

que desarrollando y usando la notación de Sweedler quedaría como:

$$\lambda_H(\epsilon_H(a)) = \epsilon_H(a) \cdot 1_H = \sum_{(a)} a_{(1)}\sigma_H(a_{(2)}) = \sum_{(a)} \sigma_H(a_{(1)})a_{(2)}.$$

La aplicación σ_H se llama **antípoda**, que en caso de existir es única. Por ello, una biálgebra puede admitir a lo sumo una estructura de álgebra de Hopf, dependiendo de si existe antípoda o no. En consecuencia, ser un álgebra de Hopf es una propiedad que puede tener una biálgebra, y no una estructura adicional.

Las álgebras de Hopf generalizan las álgebras de grupo. En particular, los módulos sobre un álgebra de Hopf se comportan de manera análoga a los módulos sobre un álgebra de grupo, los cuales coinciden con las representaciones del grupo original.Esto es posible, gracias a la antípoda que generaliza el papel del inverso en un grupo. Así, la antípoda es lo que hace posible extender muchas construcciones del álgebra de grupo, al contexto más amplio de las álgebras de Hopf.

Ejemplo 2.40. El cuerpo K sobre sí mismo es una K-álgebra de Hopf. Como ya hemos visto antes, cumple las condiciones de biálgebra, por tanto, solo nos falta definir la antípoda y ver que cumple la propiedad. Lo vemos:

Sea:

$$\sigma_K : K \longrightarrow K$$
$$a \longmapsto a$$

Veamos que cumple la propiedad de la antípoda $m_K(\sigma_K \otimes I_K)\Delta_K(a) = \lambda_K \circ \epsilon_H(a)$:

$$m_K(\sigma_K \otimes I_K)\Delta_K(a) = m_K(\sigma_K \otimes I_K)(a \otimes 1) = a1_K,$$
$$\lambda_K(\epsilon_K(a)) = \lambda_K(a) = a \cdot 1_K.$$

La propiedad por el otro lado es análoga. Luego coinciden, por tanto cumple la propiedad de antípoda, luego K es álgebra de Hopf.

Ejemplo 2.41. Sea G un grupo. Ya hemos visto anteriormente que $K[G]$ tiene estructura de biálgebra coconmutativa. Ahora, si definimos una antípoda como:

$$\sigma_{K[G]} : K[G] \to K[G] \tag{2.21}$$
$$g \longmapsto g^{-1} \tag{2.22}$$

Demostramos que cumple la propiedad de la antípoda $m_{K[G]} \circ (I_{K[G]} \otimes \sigma_{K[G]}) \circ \Delta_{K[G]} = \lambda_{K[G]} \circ \epsilon_H = m_{K[G]} \circ (\sigma_{K[G]} \otimes I_{K[G]}) \circ \Delta_{K[G]} = \lambda_{K[G]}$.

$$m_{K[G]} \circ (I_{K[G]} \otimes \sigma_{K[G]})(\sum_g r_g g \otimes g) = m_{K[G]}(\sum_g r_g g \otimes g^{-1}) = \sum_g r_g 1.$$

Del otro lado:

$$\lambda_{K[G]} \circ \epsilon_H \left(\sum_g r_g g \right) = \lambda_{K[G]} \left(\sum_g r_g 1 \right) = \sum_g r_g 1.$$

La otra igualdad es análoga. Luego se cumple la propiedad.

Tenemos que $K[G]$ tiene estructura de K-álgebra de Hopf a la cual llamamos **álgebra de grupo de Hopf**

Ejemplo 2.42. Sea $K[X]/(X^n - a)$ el álgebra de polinomios con la relación $x^n = a$ para todo $n \in \mathbb{N}$ y $a \in K$. Los elementos de $K[X]/(x^n - a)$ son polinomios de grado menor que n, por lo que una base es $\{1, \overline{X}, \overline{X^2} \ldots, \overline{X^{n-1}}\}$. Veamos que podemos definir un álgebra de Hopf.

- Multiplicación

$$m(\overline{X} \otimes \overline{Y}) = \overline{XY}.$$

- Unidad
$$\lambda(c) = \overline{c},\ \ \forall\ c \in K.$$

- Comultiplicación:

  Definimos $\Delta(\overline{X^k}) = \overline{X^k} \otimes \overline{X^k}$ para todo $0 \leq k < n$.

  Veamos que cumple la coasociatividad $(\Delta \otimes I) \circ \Delta = (I \otimes \Delta) \circ \Delta$:

$$(\Delta \otimes I)(\overline{X^k} \otimes \overline{X^k}) = \Delta(\overline{X^k}) \otimes \overline{X^k} = \overline{X^k} \otimes \overline{X^k} \otimes \overline{X^k},\ \ \forall\, 0 \leq k < n$$

$$(I \otimes \Delta)(\overline{X^k} \otimes \overline{X^k}) = \overline{X^k} \otimes \Delta(\overline{X^k}) = \overline{X^k} \otimes \overline{X^k} \otimes \overline{X^k}.$$

- Counidad. Definimos:

$$\epsilon(\overline{X^k}) = 1 \quad \forall\ 0 \leq k < n.$$

  Comprobamos laa propiedades de counidad $(\epsilon \otimes I)\Delta = 1 \otimes I (I \otimes \epsilon)\Delta = I \otimes I$:

$$(\epsilon \otimes I)(\overline{X^k} \otimes \overline{X^k}) = \epsilon(\overline{X^k}) \otimes \overline{X^k} = 1 \otimes \overline{X^k}$$

$$(I \otimes \epsilon)(\overline{X^k} \otimes \overline{X^k}) = \overline{X^k} \otimes 1.$$

- Antípoda:

$$\sigma(\overline{X^k}) = \frac{\overline{X^{n-k}}}{a}$$

  Verificamos que se cumple la propiedad de la antípoda $m(\sigma \otimes I)\Delta = \lambda \circ \epsilon = m(I \otimes \sigma)\Delta$:

$$m(\sigma \otimes I)(\overline{X^k} \otimes \overline{X^k}) = \sigma(\overline{X^k})\overline{X^k} = \left(\frac{\overline{X^{n-k}}}{a}\right)\overline{X^k} = \frac{\overline{X^n}}{a} = \frac{a}{a} = 1$$

  y

$$(\lambda \circ \epsilon)(\overline{X^k}) = 1.$$

  El otro lado es análogo.

  Por último, veamos que las operaciones de coálgebra son homomorfismos de álgebras.

$$1)\ \ \Delta(\overline{X^k Y^k}) = \Delta(\overline{X^k})\Delta(\overline{Y^k}),$$

$$\Delta(\overline{X^k})\Delta(\overline{Y^k}) = (\overline{X^k}\otimes\overline{X^k})(\overline{Y^k}\otimes\overline{Y^k}) = (\overline{X^kY^k})\otimes(\overline{X^kY^k}) = \Delta(\overline{X^kY^k}).$$

$$2)\quad \epsilon(\overline{X^kY^k}) = \epsilon(\overline{X^k})\epsilon(\overline{Y^k}).$$

Es obvio por la definición de la counidad.

Por tanto, es álgebra de Hopf.

Vamos a definir ahora una operación que necesitaremos más adelante para la demostración de las propiedades de la antípoda de una K-álgebra de Hopf. Vamos a considerar para ello C una K-coálgebra y A una K-álgebra y el conjunto $Hom_K(C, A)$ de todas las aplicaciones lineales de C a A. Con esto definimos el producto de convolución como:

Definición 2.43. Sean $f, g \in Hom_K(C, A)$. Llamamos **producto de convolución** a la aplicación lineal $f * g : C \longrightarrow A$ tal que:

$$f * g(a) = m_A(f \otimes g)\Delta_C(a) = \sum_{(a)} f(a_{(1)})g(a_{(2)}) \;\; a \in C.$$

Propiedades 2.44. *([17] Proposición 3.1.6) Sean $f, g, h \in Hom_K(C, A)$.*

1. *El producto de convolución es asociativo, esto es, $f*(g*h) = (f*g)*h$.*
2. *El elemento identidad en $Hom_K(C, A)$ para el producto de convolución es $\lambda_A\epsilon_C$.*

Demostración. 1. Veamos que * es asociativo:

$$f * (g * h)(a) = m_A(f \otimes (g * h))\Delta_C(a) = \sum_{(a)} f(a_{(1)})(g * h)(a_{(2)})$$

$$= \sum_{(a)} f(a_{(1)})m_A(g \otimes h)\Delta_C(a_{(2)}) = \sum_{(a)} f(a_{(1)}) \sum_{(a_{(2)})} g(a_{(2)(1)})h(a_{(2)(2)}),$$

que con la notación de Sweedler y la coaociatividad de Δ_C podemos escribir como:

$$\sum_{(a)} f(a_{(1)})g(a_{(2)})h(a_{(3)}) = \sum_{(a)} \sum_{(a_{(1)})} f(a_{(1)(1)})g(a_{(1)(2)})h(a_{(2)})$$

$$= \sum_{(a)} (f * g)(a_{(1)})h(a_{(2)}) = m_A((f * g) \otimes h)\Delta_C(a)$$

$$= (f * g) * h(a).$$

2. Veamos que $\lambda_A \epsilon_C$ hace de elemento identidad en $Hom(C, A)$.

$$(\lambda_A \epsilon_C * f)(a) = m_A(\lambda_A \epsilon_C \otimes f)\Delta_C(a)$$

$$= m_A \left(\sum_{(a)} \lambda_A(\epsilon_C(a_{(1)})) \otimes f(a_{(2)}) \right) = \sum_{(a)} \lambda_A(\epsilon_C(a_{(1)}))f(a_{(2)})$$

$$= \sum_{(a)} e_C(a_{(1)})\lambda_A(1_K)f(a_{(2)}) = \sum_{(a)} \epsilon_C(a_{(1)})1_A f(a_{(2)})$$

$$= \sum_{(a)} f(\epsilon_C(a_{(1)})a_{(2)}) = f(a).$$

Por la propiedad de la counidad $((\epsilon_C \otimes I_C)\Delta_C(c) = c \Rightarrow$
$(\epsilon_C \otimes I_C)\left(\sum_{(c)} c_{(1)} \otimes c_{(2)}\right) = \sum_{(c)} \epsilon_c(c_{(1)})c_{(2)} = c$ (donde hemos usado la identificación natural $K \otimes C \cong C$).

□

Proposición 2.45. *[17](Proposiciones 3.1.8 y 3.1.10) Sea H una K-álgebra de Hopf con antípoda σ_H. Se cumple lo siguiente:*

1. *$m_H(\sigma_H \otimes \sigma_H)\tau = \sigma_H m_H$, esto es $\sigma_H(ab) = \sigma_H(b)\sigma_H(a)$, para todo $a, b \in H$ (σ_H es antiendomorfismo de K-álgebra).*
2. *$\sigma_H \lambda_H = \lambda_H$, esto es $\sigma_H(1_H) = 1_H$.*
3. *$\tau(\sigma_H \otimes \sigma_H)\Delta_H = \Delta_H \sigma_H$, esto es, $\sum_{(a)} \sigma_H(a_{(1)}) \otimes \sigma_H(a_{(2)})$ $= \sum_{(a)} \sigma_H(a_{(2)}) \otimes \sigma_H(a_{(1)})$.*
4. *$\epsilon_H \sigma_H = \epsilon_H$.*

Demostración. En esta demostración trabajaremos con el producto de convolución de $Hom(H \otimes H, H)$ (con el álgebra H y la coálgebra $H \otimes H$).

1. Primero veamos que $m_H * m_H(\sigma_H \otimes \sigma_H)\tau = \lambda_H \epsilon_{H \otimes H}$ y que $m_H * \sigma_H m_H = \lambda_H \epsilon_{H \otimes H}$.

Primera igualdad: Sean $a, b \in H$:

$$m_H * m_H(\sigma_H \otimes \sigma_H)\tau(a \otimes b) = m_H(m_H \otimes m_H(\sigma_H \otimes \sigma_H)\tau)\Delta_{H\otimes H}(a \otimes b)$$

$$= m_H\left(\sum_{(a,b)} m_H(a_{(1)} \otimes b_{(1)}) \otimes m_H(\sigma_H \otimes \sigma_H)\tau(a_{(2)} \otimes b_{(2)})\right)$$

$$= \sum_{(a,b)} a_{(1)}b_{(1)}\sigma_H(b_{(2)})\sigma_H(a_{(2)}) = \sum_{(a)} a_{(1)}\epsilon_H(b)\sigma_H(a_{(2)})$$

$$\text{(ya que } \sum_{(b)} b_{(1)}\sigma_H(b_{(2)}) = m_H(\sum_{(b)} I_H(b_{(1)}) \otimes \sigma_H(b_{(2)})) =$$

$$= m_H(I_H \otimes \sigma_H)\Delta_H(b) = \lambda_H(\epsilon_H(b)) = \epsilon_H(b)1_H$$

$$= \sum_{(a)} \epsilon_H(b)a_{(1)}\sigma_H(a_{(2)}) = \epsilon_H(b)\epsilon_H(a) \cdot 1_H$$

$$= \lambda_H\epsilon_{H\otimes H}(a \otimes b).$$

Para la segunda igualdad:

$$(m_H * \sigma_H m_H)(a \otimes b) = m_H(m_H \otimes \sigma_H m_H)\Delta_{H\otimes H}(a \otimes b)$$

$$= \left(\sum_{(a,b)} m_H(a_{(1)} \otimes b_{(1)}) \otimes \sigma_H m_H(a_{(2)} \otimes b_{(2)})\right)$$

$$= \sum_{(a,b)} a_{(1)}b_{(1)}\sigma_H(a_{(2)}b_{(2)}) = m_H(I_H\otimes\sigma_H)\Delta_H(a)\Delta_H(b) = m_H(I_H\otimes\sigma_H)\Delta_H(ab).$$

(Donde la última igualdad es cierta ya que H es biálgebra y entonces Δ_H es homomorfismo de álgebras)

$$= \epsilon_H(ab)1_H = \epsilon_H(a)\epsilon_H(b)1_H = \lambda_H\epsilon_{H\otimes H}.$$

Y ahora juntando las dos igualdades tenemos que

$$m_H * (m_H(\sigma_H \otimes \sigma_H)\tau = m_H * \sigma_H m_H,$$

$$(m_H(\sigma_H\otimes\sigma_H)\tau * m_H) * m_H(\sigma_H\otimes\sigma_H)\tau = (m_H(\sigma_H\otimes\sigma_H)\tau * m_H) * \sigma_H m_H,$$

$$\lambda_H\epsilon_{H\otimes H} * (m_H(\sigma_H \otimes \sigma_H)\tau = \lambda_H\epsilon_{H\otimes H} * \sigma_H m_H$$

Y como $\lambda_H \epsilon_{H\otimes H}$ es el elemento neutro de $Hom(H \otimes H, H)$,

$$(m_H(\sigma_H \otimes \sigma_H)\tau = \sigma_H m_H.$$

2.

$$1_H = 1_K 1_H = \epsilon_H(1_H) \cdot 1_H = m_H(I_H \otimes \sigma_H)\Delta_H(1_H)$$
$$= m_H(I_H \otimes \sigma_H)(1_H \otimes 1_H) = \sigma_H(1_H).$$

donde hemos usado la propiedad de álgebra de Hopf $\lambda_H \circ \epsilon_H = m_H \circ (I_H \otimes \sigma_H) \circ \Delta_H$.

3. Vamos a usar la misma idea que en 1. Tomando ahora H como coálgebra y $H \otimes H$ como álgebra y trabajando con la convolución en $Hom(H, H \otimes H)$, denotemos $\phi = \tau(\sigma_H \otimes \sigma_H)\Delta_H$.

Queremos ver que $\Delta_H * \phi = \lambda_{H\otimes H}\epsilon_H$ y que $\Delta_H * \Delta_H \sigma_H = \lambda_{H\otimes H}\epsilon_H$

La primera igualdad: Sea $a \in H$,

$$(\Delta_H * \phi)(a) = m_{H\otimes H}(\Delta_H \otimes \phi)\Delta_H(a)$$

$$= m_{H\otimes H}(\Delta_H \otimes \phi)\left(\sum_{(a)} a_{(1)} \otimes a_{(2)}\right) = m_{H\otimes H}\left(\sum_{(a)} \Delta_H(a_{(1)}) \otimes \phi(a_{(2)})\right)$$

$$= m_{H\otimes H}\left(\sum_{(a)} a_{(1)} \otimes a_{(2)} \otimes \sigma_H(a_{(4)}) \otimes \sigma_H(a_{(3)})\right)$$

$$= \sum_{(a)} a_{(1)}\sigma_H(a_{(4)}) \otimes a_{(2)}\sigma_H(a_{(3)}) = \sum_{(a)} a_{(1)}\sigma_H(a_{(3)}) \otimes \epsilon_H(a_{(2)})1_H$$

(donde hemos usado la propiedad de la antípoda).

$$= \sum_{(a)} \epsilon_H(a_{(2)})a_{(1)}\sigma_H(a_{(3)}) \otimes 1_H = \sum_{(a)} a_{(1)}\sigma_H(a_{(2)}) \otimes 1_H$$

(donde hemos usado la propiedad de la counidad).

$$= \epsilon_H(a)1_H \otimes 1_H$$

$$= (\lambda_{H\otimes H}\epsilon_H)(a) \quad \text{por la propiedad de la antípoda}$$

Para la segunda igualdad:

$$\Delta_H * \Delta_H\sigma_H(a) = m_{H\otimes H}(\Delta_H \otimes \Delta_H\sigma_H)\Delta_H(a)$$

$$= m_{H\otimes H}\left(\sum_{(a)} \Delta_H(a_{(1)}) \otimes \Delta_H\sigma_H(a_{(2)})\right)$$

$$= m_{H\otimes H}\left(\sum_{(a)} a_{(1)} \otimes a_{(2)} \otimes \sigma_H(a_{(3)}) \otimes \sigma_H(a_{(4)})\right)$$

$$= \sum_{(a)} a_{(1)}\sigma_H(a_{(3)}) \otimes a_{(2)}\sigma_H(a_{(4)}) = \sum_{(a)} a_{(1)}\sigma_H(a_{(3)}) \otimes \epsilon_H(a_{(2)})1_H$$

(donde hemos usado la propiedad de la antípoda).

$$= \sum_{(a)} \epsilon_H(a_{(2)})a_{(1)}\sigma_H(a_{(3)}) \otimes 1_H = \sum_{(a)} a_{(1)}\sigma_H(a_{(2)}) \otimes 1_H$$

(donde hemos usado la propiedad de la counidad).

$$= \epsilon_H(a)1_H \otimes 1_H$$

$$= \lambda_{H\otimes H}\epsilon_H(a) \quad \text{por la propiedad de la antípoda}$$

Ahora juntando ambas igualdades,

$$\phi * \Delta_H * \phi = \phi * \Delta_H * \Delta_H\sigma_H$$

$$\Rightarrow \lambda_{H\otimes H}\epsilon_H * \phi = \lambda_{H\otimes H}\epsilon_H * \Delta_H\sigma_H$$

$$\Rightarrow \phi = \Delta_H\sigma_H.$$

4. En esta demostración vamos a usar la misma idea que en 2:

$$\epsilon_H(a) = \epsilon_H(a)\epsilon_H(1_H) = \epsilon_H(\epsilon_H(a)1_H)$$

$$= \epsilon_H(m_H(I_H \otimes \sigma_H)\Delta_H(a))$$

$$= \epsilon_H\left(\sum_{(a)} a_{(1)}\sigma_H(a_{(2)})\right) = \sum_{(a)} \epsilon_H(a_{(1)})\epsilon_H(\sigma_H(a_{(2)}))$$

$$= \sum_{(a)} \epsilon_H(\sigma_H(\epsilon_H(a_{(1)})a_{(2)}) = \epsilon_H(\sigma(a)).$$

La última igualdad es cierta por la propiedad de la counidad.

□

Corolario 2.46. *([17] Proposición 3.1.9) Sea H una K-álgebra de Hopf con antípoda σ_H. Si H es tanto conmutativa como coconmutativa, entonces σ_H tiene orden 2 i.e, $\sigma_H^2 = I_H$.*

Demostración. Sea $Hom_K(H, H)$ y * el producto de convolución. Para $a \in H$,

$$(\sigma_H * \sigma_H^2)(a) = \sum_{(a)} \sigma_H(a_{(1)})\sigma_H^2(a_{(2)})$$

$$= \sum_{(a)} \sigma_H(a_{(1)})\sigma_H(\sigma_H(a_{(2)})) = \sum_{(a)} \sigma_H(a_{(2)}\sigma_H(a_{(1)}))$$

ya que σ_H es un antiendomorfismo. Y por la propiedad de la antípoda, lo anterior es igual a:

$$= \sigma_H(\epsilon_H(a) \cdot 1_H) = \epsilon_H(a) \cdot \sigma_H(1_H) = \epsilon_H(a) \cdot 1_H = \lambda_H(\epsilon_H(a))$$

Ahora, como $\lambda_H\epsilon_H$ es el elemento identidad de * tenemos:

$$I_H * (\sigma_H * \sigma_H^2) = I_H * (\lambda_H\epsilon_H) = I_H$$

Entonces, por la asociatividad de *:

$$I_H * (\sigma_H * \sigma_H^2) = (I_H * \sigma_H) * \sigma_H^2$$

$$= (m_H(\sigma_H \otimes I_H)\Delta_H) * \sigma_H^2 = \lambda_H\epsilon_H * \sigma_H^2 = \sigma_H^2$$

Por tanto $\sigma_H^2 = I_H$. □

Ejemplo 2.47. Sea H, H' dos K-álgebras de Hopf. Entonces $H \otimes H'$ tiene estructura de K-álgebra de Hopf con antípoda definida de la siguiente manera:

$$\sigma_{H\otimes H'} : H \otimes H' \to H \otimes H',$$

$$a \otimes b \mapsto \sigma_H(a) \otimes \sigma_{H'}(b).$$

Veamos que cumple la propiedad de la antípoda:

$$m_{H\otimes H}(\sigma_{H\otimes H'}\otimes I_{H\otimes H})\Delta_{H\otimes H'}(a\otimes b)=\epsilon_{H\otimes H'}(a\otimes b)\cdot 1_{H\otimes H}$$

Desarrollamos:

$$m_{H\otimes H}(\sigma_{H\otimes H'}\otimes I_{H\otimes H})\Delta_{H\otimes H'}(a\otimes b)=m_{H\otimes H}(\sigma_{H\otimes H'}\otimes I_{H\otimes H})(\sum_{(a,b)}a_{(1)}\otimes b_{(1)}\otimes a_{(2)}\otimes b_{(2)})$$

$$=m_{H\otimes H'}\sum_{(a,b)}\sigma_H(a_{(1)})\otimes\sigma_{H'}(b_{(1)})\otimes a_{(2)}\otimes b_{(2)}=\sum_{(a,b)}\sigma_H(a_{(1)})a_{(2)}\otimes\sigma_{H'}(b_{(1)})b_{(2)}.$$

Ahora aplicamos la propiedad de la antípoda de H y H' ya que ambas son álgebras de Hopf.

$$=\epsilon_H(a)\cdot 1_H\otimes\epsilon_{H'}(b)\cdot 1_{H'}=\epsilon_H(a)\otimes\epsilon_{H'}(b)(1_H\otimes 1_{H'})$$

$$=\epsilon_{H\otimes H'}(a\otimes b)\cdot 1_{H\otimes H'}.$$

Nota. Sea L/K una extensión de cuerpos, y V un espacio vectorial sobre K. Como L es un K-espacio vectorial, $V\otimes_K L$ es claramente un K-espacio vectorial. Además, podemos ver que $V\otimes_K L$ es un L-espacio vectorial con producto escalar definida por $\lambda(v\otimes_K r)=v\otimes_K\lambda r$ para todo $\lambda\in L$, $v\otimes_K r\in V\otimes_K L$.Por lo tanto, si $f:V_1\to V_2$ es una aplicación lineal entre K-espacios vectoriales entonces $f\otimes I_L:V_1\otimes_K L\to V_2\otimes_K L$ es una aplicación lineal entre L-espacios vectoriales.

Proposición 2.48. *([8] Proposición 2.3.14) Sea H una K-álgebra de Hopf y sea L una extensión finita de K. Entonces $H\otimes_K L$ es una L-álgebra de Hopf.*

Demostración. Por la asociatividad del producto tensorial tenemos:

$$(H\otimes_K L)\otimes_L(H\otimes_K L)\cong$$

$$\cong H\otimes_K(L\otimes_L(H\otimes_K L))\cong$$

$$H\otimes_K(H\otimes_K L)\cong H\otimes_K L.$$

Donde el tercer isomorfismo se debe a que $L\otimes_L V\cong V$ para todo L-espacio vectorial V, con isomorfismo dado por $r\otimes v\longmapsto rv$, para todo $r\in L$, $v\in V$ y $v\longmapsto 1_L\otimes v$ para todo $v\in H, r\in E$.

Por construcción, esto es un isomorfismo de K-espacios vectoriales, pero además, también lo es de L-espacios vectoriales. Ahora, definamos la multiplicación, la unidad, la comultiplicación, la counidad y la antípoda sin demostrar sus propiedades ya que es fácil comprobarlo debido a que lo hacen $m_H, \lambda_H, \Delta_H, \epsilon_H, \sigma_H$.

1. $m_{H\otimes_K L} : (H \otimes_K L) \otimes_L (H \otimes_K L) \to H \otimes_K L$ definida como

$$m_{H\otimes_K L} = m_H \otimes I_L.$$

2. $\lambda_{H\otimes_K L} : L \to H \otimes_K L$ dada por

$$\lambda_{H\otimes_K L} = \lambda_H \otimes I_L.$$

3. $\Delta_{H\otimes_K L} : H \otimes_K L \to (H \otimes_K L) \otimes_L (H \otimes_K L)$ definida como

$$\Delta_{H\otimes_K L} = \Delta_H \otimes I_L.$$

4. $\epsilon_{H\otimes_K L} : H \otimes_K L \to L$ dada por

$$\varepsilon_{H\otimes_K L} = \varepsilon_H \otimes I_L.$$

5. $\sigma_{H\otimes_K L} : H \otimes_K L \to H \otimes_K L$ definida como

$$\sigma_{H\otimes_K L} = \sigma_H \otimes I_L.$$

□

Nota. Anteriormente mencionamos que el dual de un álgebra de dimensión finita puede verse como una coálgebra, y viceversa. Esta idea también se aplica a las álgebras de Hopf: si H es un álgebra de Hopf de dimensión finita, entonces su dual H^* hereda una estructura de álgebra de Hopf, intercambiando los papeles de multiplicación y comultiplicación. En este caso, las operaciones del álgebra original se reflejan en el dual de manera compatible, manteniendo la estructura de álgebra de Hopf. En particular, la antípoda se define como la composición de $f \in H^*$ con la antípoda original, es decir, $\sigma^*_{H^*} : H^* \longrightarrow H^*$ está dada por $\sigma^*_{H^*}(f) = f \circ \sigma_H$.

Capítulo 3

Estructuras de Hopf-Galois. Teorema de Greither-Pareigis

Ya estamos en condiciones de presentar la teoría de Hopf-Galois. Vamos a ver cómo pasamos de la teoría de Galois a su generalización mediante álgebras de Hopf. Primero, reescribiremos la condición de Galois de una extensión de cuerpos usando el álgebra de grupo que hemos visto en el capítulo anterior, de manera que la estructura de Hopf-Galois aparezca de manera natural y a partir de ahí podremos generalizar a cualquier álgebra de Hopf y poder dar así los resultados fundamentales de esta teoría.

Vamos a ver cómo la teoría de Galois se puede generalizar gracias a los resultados de Hopf-Galois, aunque esta generalización no es completa. A diferencia del caso clásico donde hay una correspondencia biyectiva entre los cuerpos intermedios de la extensión y los subgrupos del grupo de Galois, en el contexto de Hopf-Galois no se da esa biyectividad entre los cuerpos intermedios y las subálgebras de Hopf. Esto nos llevará a establecer una condición bajo la cual sí se puede lograr dicha correspondencia, la de extensión de Galois casi clásica. También veremos que hay extensiones que no son de Galois, pero que sí admiten una estructura Hopf-Galois.

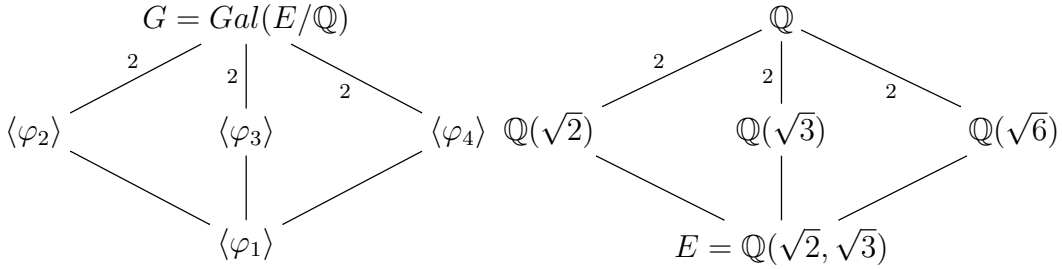
Otro resultado importante que descubriremos es que las estructuras de Hopf-Galois no son únicas, por lo que será interesante estudiar cómo encontrar todas las posibles estructuras. Para ello, veremos el importante teorema de Greither-Pareigis, que transforma el problema de encontrar estas estruc-

turas en una cuestión de teoría de grupos. Por último, estudiaremos los resultados que introdujo Byott, que mejoran el problema que tiene el teorema de Greither-Pareigis para extensiones de grado alto y también estableció cuándo la estructura de Galois de una extensión de Galois es la única estructura de Hopf-Galois que tiene la extensión.

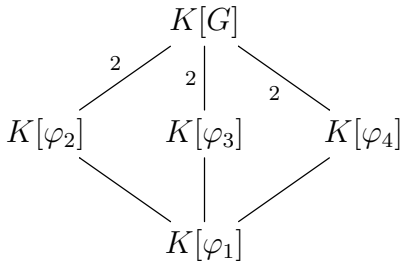
Este capítulo se basa principalmente en las fuentes [2], [3], [4], [10], [16] entre otras. Además, la autora está muy agradecida a Daniel Gil Muñoz por compartir en privado sus extensas notas "Introduction to Hopf-Galois theory", que también han sido consultadas frecuentemente.

3.1. Estructuras de Hopf-Galois

Rescatemos el ejemplo 1.37 del Capítulo 1 donde representábamos el retículo de subgrupos de G el grupo de Galois de la extensión de cuerpos $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$



Observando estos diagramas, podemos pensar ¿qué pasaría si en vez de considerar grupos consideráramos sus correspondientes álgebras de Hopf de grupo? Vemos la respuesta en el siguiente diagrama:



Resulta que obtenemos un diagrama similar, pues se puede probar que estas son todas las subálgebras de Hopf de $K[G]$

Viendo esto, podemos pensar que puede haber una generalización de los resultados que veíamos en el capítulo 1 sobre las extensiones de Galois, pero ahora en vez de usar grupos, usando álgebras de Hopf. Este pensamiento no es para nada erróneo; veamos lo siguiente:

Consideremos L/K una extensión de cuerpos finita y G un subgrupo de $Aut_K L$ el grupo de automorfismos de L que fijan K. Entonces, tenemos que claramente L es una K-álgebra y como ya hemos visto anteriormente, el anillo de grupo $K[G]$ es un álgebra de Hopf. Si definimos ahora la acción de $K[G]$ sobre L

$$\left(\sum_{g\in G} r_g g\right)\cdot x = \sum_{g\in G} r_g g(x)$$

tenemos el siguiente resultado:

Proposición 3.1. *[17](Proposición 4.5.1) L es una K-álgebra de $K[G]$-módulo por la izquierda con la acción anterior.*

Demostración. Veamos que cumple L las condiciones de álgebra de módulo.

Multiplicación: Sea $h = \sum_{g\in G} r_g g \in K[G]$ y $x, y \in L$. Entonces $\Delta_H(h) = \sum_{g\in G} r_g g \otimes g$. Luego:

$$h \cdot (xy) = \sum_{g\in G} r_g g(xy) = \sum_{g\in G} r_g g(x)g(y)$$

$$= \sum_{g\in G} r_g (g\cdot x)(g\cdot y) = \sum_{(h)} (h_{(1)}\cdot x)(h_{(2)}\cdot y)$$

Unidad:

$$h \cdot 1_L = \sum_{g\in G} r_g g(1_L) = \sum_{g\in G} r_g \text{ ya que } g(1_L) = 1_L \text{ para todo } g \in G$$

$$\epsilon(h)\cdot 1_L = \epsilon\left(\sum_{g\in G} r_g g\right) = \sum_{g\in G} r_g \epsilon(g) = \sum_{g\in G} r_g.$$

Por tanto, se cumplen las condiciones de álgebra de módulo. □

Lema 3.2. *([17]Lema 4.5.2) Los elementos de $G \leq Aut_K(L)$ son linealmente independientes sobre L.*

Demostración. Como L/K es una extensión finita, hay un número finito de automorfismos y por tanto G es finito. Escribamos $G = \{g_1 \dots g_n\}$ y razonemos por reducción al absurdo; supongamos que G no es linealmente independiente sobre L, entonces existe un $1 \leq m \leq n$ mínimo y un conjunto de índices $0 \leq i_1, i_2, \dots, i_m \leq n$ tal que:

$$a_1 g_{i_1} + \dots + a_m g_{i_m} = 0 \quad a_1, \dots, a_m \neq 0.$$

Como $g_{i_{m-1}} \neq g_{i_m}$ también existe $y \in L$ tal que $g_{i_{m-1}}(y) \neq g_{i_m}(y)$ con $g_{i_m}(y) \neq 0$. Ahora para cualquier $x \in L$:

$$a_1 g_{i_1}(yx) + \dots + a_m g_{i_m}(yx) = 0.$$

Como g_i son homomorfismos:

$$a_1 g_{i_1}(y)g_{i_1}(x) + \cdots + a_m g_{i_m}(y)g_{i_m}(x) = 0.$$

Y como se cumple para todo $x \in L$:

$$a_1 g_{i_1}(y)g_{i_1} + \cdots + a_m g_{i_m}(y)g_{i_m} = 0.$$

Dividimos entre $g_{i_m}(y)$:

$$a_1 \frac{g_{i_1}(y)}{g_{i_m(y)}} g_{i_1} + \cdots + a_{m-1} \frac{g_{i_{m-1}}(y)}{g_{i_m(y)}} g_{i_{m-1}} + a_m g_{i_m} = 0.$$

Restando $a_1 g_{i_1} + \cdots + a_m g_{i_m} = 0$ obtenemos:

$$\left(a_1 \left(\frac{g_{i_1}(y)}{g_{i_m}(y)}\right) - a_1\right) g_{i_1} + \cdots + \left(a_{m-1} \left(\frac{g_{i_{m-1}}(y)}{g_{i_m}(y)}\right) - a_{m-1}\right) g_{i_{m-1}} = 0.$$

Como $g_{i_m}(y) \neq g_{i_{m-1}}(y)$ implica que $\frac{g_{i_{m-1}}(y)}{g_{i_m}(y)} \neq 1$, $a_{m-1}\frac{g_{i_{m-1}}(y)}{g_{i_m}(y)} - a_{m-1} \neq 0$, llegamos a una contradicción y por tanto G es linealmente independiente sobre L. □

Lema 1. *Sea L/K una extensión de cuerpos con $[L : K] = n$. Entonces:*

$$dim_K(End_K(L)) = n^2.$$

Demostración. Tenemos que L es una extensión de K de grado n, por tanto L es un espacio vectorial de dimensión n sobre K.

Ahora, sea $\{e_1, \ldots, e_n\}$ una base de L como K-espacio vectorial y consideremos una aplicación lineal $f : L \longrightarrow L$, que queda totalmente determinada por los valores que toma su imagen en los elementos de la base. Es decir:

$$f(e_i) = \sum_{j=1}^{n} a_{ji} e_j$$

Por tanto, necesitamos n vectores en L y cada uno de estos vectores tiene n coordenadas en K. Luego en total necesitamos n^2 parámetros distintos para definir f. En consecuencia $dim_K(End_K(L)) = n^2$.

□

Teorema 3.3. *[17](Proposición 4.5.3) Sea L/K una extensión finita y separable de cuerpos y sea G un subgrupo de $Aut_K(L)$. Entonces, L/K es de Galois con grupo de Galois G si y solo si, la aplicación*

$$\begin{aligned} j : L \otimes_K K[G] &\to End_K(L) \\ x \otimes h \quad &\mapsto j(x \otimes h)(y) = x(h \cdot y) \end{aligned}$$

es biyectiva.

Demostración. Supongamos primero que L/K es de Galois. Tenemos que la aplicación j es un homomorfismo de K-espacios vectoriales. Sea $x \otimes h \in Ker(j)$. Entonces:

$$0 = j(x \otimes h)(y) = x(h \cdot y) \quad \forall\, y \in L$$

Veamos que $x \otimes y = 0$. Como h es un elemento de $K[G]$ podemos escribir $h = \sum_{g \in G} a_g g$. Entonces,

$$\left(\sum_{g \in G} x a_g g \right) \cdot y = \sum_{g \in G} x a_g g(y) = 0 \quad \forall\, y \in L.$$

Por lo tanto,$\sum_{g \in G} x a_g g = 0$.Como G es linealmente independiente sobre L, $x a_g = 0$ para todo $g \in G$. Por consiguiente:

$$x \otimes h = x \otimes \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g (x \otimes g) = \sum_{g \in G} (x\, a_g \otimes g) = 0.$$

Esto prueba que j es inyectiva.

Para ver que es sobreyectiva, es suficiente con probar que $dim_K(L \otimes K[G]) = dim_K(End_K(L))$

Como L/K es de Galois con grupo de Galois G, tenemos que $[L : K] = |G|$, y sabemos que $dim_K(End_K(L)) = (dim_K L)^2$. Entonces:

$$dim_K(L \otimes_K K[G]) = dim_K(L) dim_K(K[G]) = [L : K]|G| = [L : K]^2 = dim_K(End_K(L))$$

.

Ya que $dim_K L = [L : K]$ y $K[G]$ es el álgebra de grupo, un K-espacio vectorial de dimensión $|G|$ Por tanto, j es inyectiva y sobreyectiva, j es biyectiva.

Ahora supongamos que j es biyectiva. La dimensión del espacio de salida y el espacio de llegada son la misma, entonces:

$$dim_K(L \otimes_K K[G]) = [L : K]|G| = dim_K(End_K(L)) = [L : K]^2.$$

De aquí deducimos que $|G| = [L : K]$. Por el teorema del elemento primitivo 1.30, existe $\alpha \in L$ tal que $L = K(\alpha)$ con $p = irr(\alpha, K)$ de grado $[L : K]$. Para ver que la extensión es de Galois, tenemos que ver que es normal y separable.

La separabilidad la tenemos asegurada por hipótesis, por lo que solo falta ver que es normal. Como $L = K(\alpha)$ y $G \leq Aut_K L$ los elementos de G están determinados por la imagen de α a través de un automorfismo de G. Pero sabemos que cada automorfismo de G lleva α una raíz distinta de p, de las cuales hay $[L : K] = |G|$ por tanto L es el cuerpo de descomposición de p sobre K, lo cual nos asegura, que L/K es normal, es decir, $Aut_K L = Gal(L/K)$.

Ahora bien, como $G \leq Aut_K L = Gal(L/K)$, y como $|Gal(L/K)| = |L : K| = |G|$, concluimos que $G = Gal(L/K)$. □

La K-álgebra de Hopf $K[G]$ nos ha ayudado a obtener una definición equivalente de extensión de cuerpos de Galois en términos de una aplicación que, junto con la acción de Galois clásica, dota al cuerpo de extensión L con una estructura de $K[G]$-álgebra de módulo. Esto es generalizable a cualquier K-álgebra de Hopf coconmutativa H y cualquier acción que dote a L con una estructura de K-álgebra de H-módulo H. Gracias a esto, llegamos a la siguiente definición:

Definición 3.4. Sea L/K una extensión finita. Llamamos **estructura de Hopf-Galois** de L/K a un par $(H, \cdot)$ donde H es una K-álgebra de Hopf de dimensión finita coconmutativa y donde $\cdot : H \otimes_K L \to L$ es una acción que dota a L con la estructura de una K-álgebra de H-módulo, de manera que la aplicación:

$$\begin{aligned} j : L \otimes_K H &\longrightarrow \mathrm{End}_K(L) \\ x \otimes h &\longmapsto j(x \otimes h)(y) = x(h \cdot y) \end{aligned}$$

es biyectiva.

Definición 3.5. Una extensión finita L/K se dice que es de Hopf-Galois si admite una estructura de Hopf-Galois.

Corolario 3.6. *Si L/K es de Galois, también es de Hopf-Galois.*

El opuesto no se cumple, hay extensiones que son de Hopf-Galois que no son de Galois, lo que demuestra que las extensiones de Hopf-Galois son una generalización de las de Galois. Veamos un ejemplo:

Ejemplo 3.7. Sea $\alpha = \sqrt[3]{2}$. Consideramos la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$, es finita de grado 3 ya que $\mathrm{irr}(\alpha, \mathbb{Q})(x) = x^3 - 2$, pero sabemos que no es de Galois ya que no es una extensión normal. Veamos que sí es de Hopf-Galois.

Lo primero que tenemos que hacer para encontrar una estructura de Hopf-Galois es considerar un álgebra de Hopf H que actúe sobre $\mathbb{Q}$. En este caso, vamos a considerar $H = \mathbb{Q}[c, s]/(3s^2 + c^2 - 1, (2c + 1)s, (2c + 1)(c - 1)$ descrita en [10]. Su base está dada por $\{1, c, s\}$. Veamos que efectivamente sí que es un álgebra de Hopf definiendo sus operaciones sobre los elementos de su base:

- Comultiplicación: $\Delta(1) = 1 \otimes 1$, $\Delta(c) = c \otimes c - 3s \otimes s$, $\Delta(s) = c \otimes s + s \otimes c$

  Queremos verificar que el coproducto Δ es coasociativo, es decir, que se cumple:
  $$(\Delta \otimes I) \circ \Delta = (I \otimes \Delta) \circ \Delta.$$
  Verificamos esta propiedad en los generadores 1, c y s.

  1. Para el 1:
  $$(\Delta \otimes I)(\Delta(1)) = \Delta(1) \otimes 1 = 1 \otimes 1 \otimes 1,$$
  $$(I \otimes \Delta)(\Delta(1)) = 1 \otimes \Delta(1) = 1 \otimes 1 \otimes 1.$$
  Se cumple coasociatividad en 1.

  2. Para s:

  Lado izquierdo:
  $$(\Delta \otimes I)(\Delta(s)) = \Delta(c) \otimes s + \Delta(s) \otimes c$$
  $$= (c \otimes c - 3s \otimes s) \otimes s + (c \otimes s + s \otimes c) \otimes c$$
  $$= c \otimes c \otimes s - 3s \otimes s \otimes s + c \otimes s \otimes c + s \otimes c \otimes c.$$

Lado derecho:

$$(I \otimes \Delta)(\Delta(s)) = c \otimes \Delta(s) + s \otimes \Delta(c)$$

$$= c \otimes (c \otimes s + s \otimes c) + s \otimes (c \otimes c - 3s \otimes s).$$

$$= c \otimes c \otimes s + c \otimes s \otimes c + s \otimes c \otimes c - 3s \otimes s \otimes s$$

Ambos lados coinciden, se cumple coasociatividad en s.

3. Para c:

Lado izquierdo:

$$(\Delta \otimes I)(\Delta(c)) = \Delta(c) \otimes c - 3\Delta(s) \otimes s$$

$$= (c \otimes c - 3s \otimes s) \otimes c - 3(c \otimes s + s \otimes c) \otimes s$$

$$= c \otimes c \otimes c - 3s \otimes s \otimes c - 3c \otimes s \otimes s - 3s \otimes c \otimes s.$$

Lado derecho:

$$(I \otimes \Delta)(\Delta(c)) = c \otimes \Delta(c) - 3s \otimes \Delta(s)$$

$$= c \otimes (c \otimes c - 3s \otimes s) - 3s \otimes (c \otimes s + s \otimes c)$$

$$= c \otimes c \otimes c - 3c \otimes s \otimes s - 3s \otimes c \otimes s - 3s \otimes s \otimes c$$

Ambos lados coinciden, se cumple coasociatividad en c.

- Counidad: $\epsilon(1) = 1$, $\epsilon(c) = 1$, $\epsilon(s) = 0$ Probemos la propiedad de counidad, es decir:

$$(\epsilon \otimes I) \circ \Delta = 1 \otimes I, \ \ (I \otimes \epsilon) \circ \Delta = I \otimes 1.$$

Probamos esta igualdad en los generadores $1, c, s$.

1. Para el 1:

$$(\epsilon \otimes I)(\Delta(1)) = \epsilon(1) \otimes 1 = 1 \otimes 1$$

$$(I \otimes \epsilon)(\Delta(1)) = 1 \otimes \epsilon(1) = 1 \otimes 1.$$

Por tanto, se cumple la counidad en 1.

2. Para c:

   Evaluamos,

   $$(\epsilon \otimes I)(\Delta(c)) = \epsilon(c) \otimes c - 3\epsilon(s) \otimes s = 1 \otimes c - 3 \cdot 0 \otimes s = 1 \otimes c,$$

   $$(I \otimes \epsilon)(\Delta(c)) = c \otimes \epsilon(c) - 3s \otimes \epsilon(s) = c \otimes 1 - 3s \otimes 0 = c \otimes 1.$$

   Por tanto, se cumple la counidad en c.

3. Para s:

   Evaluamos,

   $$(\epsilon \otimes I)(\Delta(s)) = \epsilon(c) \otimes s + \epsilon(s) \otimes c = 1 \otimes s + 0 \otimes c = 1 \otimes s,$$

   $$(I \otimes \epsilon)(\Delta(s)) = c \otimes \epsilon(s) + s \otimes \epsilon(c) = c \otimes 0 + s \otimes 1 = s \otimes 1.$$

   Por tanto, se cumple la counidad en s.

- La antípoda $\sigma(1) = 1$, $\sigma(c) = c$, $\sigma(s) = -s$. Queremos demostrar que:

  $$m \circ (\sigma \otimes I) \circ \Delta = \eta \circ \epsilon = m \circ (I \otimes \sigma) \circ \Delta,$$

  donde m es la multiplicación y η la unidad del álgebra. Verificamos esta igualdad para los generadores.

  1. Para el 1:

     $$\Delta(1) = 1 \otimes 1, \quad m \circ (\sigma \otimes I)(\Delta(1)) = m(1 \otimes 1) = 1,$$

     $$\eta \circ \epsilon(1) = \eta(1) = 1.$$

  2. Para c:

     $$\Delta(c) = c \otimes c - 3s \otimes s,$$

     $$(\sigma \otimes I)(\Delta(c)) = \sigma(c) \otimes c - 3\sigma(s) \otimes s = c \otimes c + 3s \otimes s,$$

     $$m(c \otimes c + 3s \otimes s) = c^2 + 3s^2.$$

     Por las relaciones sabemos que $c^2 + 3s^2 = 1$

     $$\eta \circ \epsilon(c) = \eta(1) = 1.$$

3. Para s:

$$\Delta(s) = c \otimes s + s \otimes c,$$
$$(\sigma \otimes I)(\Delta(s)) = \sigma(c) \otimes s + \sigma(s) \otimes c = c \otimes s - s \otimes c,$$
$$m(c \otimes s - s \otimes c) = cs - sc.$$

Como el álgebra es conmutativa ($cs = sc$), entonces:

$$cs - sc = 0,$$

$$\eta \circ \epsilon(s) = \eta(0) = 0.$$

Se cumple para todos los casos.

Ahora veamos que cumple la condición de que $\mathbb{Q}(\alpha)$ es una álgebra de H-módulo con la acción dada por:

$$c \cdot 1 = 1, \quad c \cdot \alpha = -\frac{1}{2}\alpha, \quad c \cdot \alpha^2 = -\frac{1}{2}\alpha^2,$$
$$s \cdot 1 = 0, \quad s \cdot \alpha = \frac{1}{2}\alpha, \quad s \cdot \alpha^2 = -\frac{1}{2}\alpha^2.$$

$$c \cdot (xy) = (c \cdot x)(c \cdot y) - 3(s \cdot x)(s \cdot y), \qquad c \cdot 1_{\mathbb{Q}(\alpha)} = c \cdot 1 = 1 = \varepsilon(c) \cdot 1,$$
$$s \cdot (xy) = (c \cdot x)(s \cdot y) + (s \cdot x)(c \cdot y), \qquad s \cdot 1_{\mathbb{Q}(\alpha)} = s \cdot 1 = 0 = \varepsilon(s) \cdot 1.$$

Se demuestra que la aplicación $j : \mathbb{Q}(\alpha) \otimes H \longrightarrow End_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ definida por $j(x \otimes h)(y) = x(h \cdot y)$ es un isomorfismo

Hacia el final del capítulo retomaremos este ejemplo y veremos una manera más explícita de describir el álgebra de Hopf H gracias al teorema de Greither-Pareigis.

3.2. Correspondencia del teorema fundamental de la teoría de Galois

En el Capítulo 1 veíamos el teorema fundamental de la teoría de Galois 1.36 que recordamos que decía que los subgrupos de G se corresponden con los cuerpos intermedios de la extensión L/K (siendo G el grupo de Galois de L/K) cambiando el sentido de la contención.

Anteriormente, obtuvimos un resultado que generaliza la definición de extensiones de Galois en términos del álgebra de grupo $K[G]$ y una aplicación

j y de ahí hemos obtenido la definición de estructura de Hopf-Galois. Ahora, resulta natural preguntarnos si es posible realizar una generalización similar con el teorema fundamental de la teoría de Galois en este contexto.

Pero aún no podemos responder a esta pregunta ya que falta definir un elemento clave que teníamos en la teoría clásica de Galois: el cuerpo fijo bajo la acción de Galois. En el contexto de Hopf-Galois, no tenemos una manera literal de traducirlo. Por ello, es necesario introducir una definición alternativa que cumpla un papel similar:

Definición 3.8. Sea W una K-álgebra de Hopf. Definimos **el cuerpo fijo de L bajo la acción de W** como

$$L^W = \{x \in L \mid w \cdot x = \epsilon(w)x \text{ para todo } w \in W\}$$

Entonces, si L/K es de Galois, tenemos que $\epsilon_{K[G]}(g) = 1$ para todo $g \in G$, recuperando el cuerpo fijo en sentido Galois clásico.

Pero entonces, ¿existe tal correspondencia?

Teorema 3.9. *(Teorema 1.1 [16]) Sea L/K una extensión de Hopf-Galois. Entonces la aplicación*

$$\begin{aligned}\{W \subset H \mid W \text{ subálgebra de Hopf de } H\} &\longrightarrow \{E \subset L \mid E \text{ cuerpo intermedio de } L/K\} \\ W &\longmapsto L^W\end{aligned}$$

es inyectiva e invierte inclusiones.

Esto lo demostraron Chase y Sweedler en [3] teorema 7.6. .

Este teorema no nos asegura que exista tal correspondencia ya que no hay biyectividad en general, sino que es solo inyectiva. De hecho más adelante, cuando tengamos las herramientas adecuadas para ello, veremos un ejemplo en el que la correspondencia es inyectiva pero no sobreyectiva. Ahora veremos distintos resultados que recuperan la biyectividad en contextos más concretos.

Teorema 3.10. *(Teorema 5.3 [10]) Dada una extensión de Galois L/K existe un álgebra de Hopf H tal que L/K es Hopf-Galois y existe una correspondencia biyectiva entre las subálgebras de Hopf de H y las subextensiones normales de L/K.*

Este teorema evidencia que, dependiendo del álgebra de Hopf que tomemos, aparecerán distintos "trozos" del retículo de subcuerpos.

3.3. Teoría de Hopf-Galois para extensiones separables

Es importante saber que una extensión de Galois determina el grupo de Galois de manera única, pero una extensión de Hopf-Galois puede tener varias estructuras de Hopf-Galois no isomorfas. Por eso resulta interesante contarlas; desgraciadamente, el conteo exacto resulta muy complicado en general, pero en el caso en que las extensiones son separables, existe una caracterización en términos de grupos que lo facilita.

En esta sección vamos a estudiar el importante teorema de Greither-Pareigis [10], que nos permite determinar de manera teórica todas las estructuras de Hopf-Galois que tiene una extensión finita y separable, convirtiendo una cuestión algebraica, encontrar estructuras de Hopf-Galois, en un problema de teoría de grupos, pero no es muy eficiente para extensiones de grado alto. Introduciremos además la técnica de la traducción de Byott que solucionará parcialmente este problema.

Nuestro objetivo es, fijada una extensión L/K, encontrar todas las K-álgebras de Hopf y todas las acciones $\cdot : L \otimes_K H \to H$ tales que $(H, \cdot)$ es una estructura de Hopf-Galois de L/K.

También, vamos a definir las estructuras casi Galois clásicas en las cuales el Teorema 3.9 se cumple en su forma fuerte, es decir, además de cumplirse la inyectividad, se cumple la sobreyectividad.

Veamos esto último primero:

Definición 3.11. Sea L/K una extensión de cuerpos y sea $\tilde{L}$ la clausura normal de L. Sean $G' = Gal(\tilde{L}/L)$ y $G = Gal(L/K)$, y sea $X = G/G'$. Definimos la aplicación:

$$\begin{aligned} \lambda : G &\longrightarrow \mathrm{Perm}(X) \cong S_n \\ \tau &\mapsto \lambda_G(\tau)(\sigma) = \tau \circ \sigma \end{aligned}$$

que identifica G como subgrupo de S_n y se llama traslación por la izquierda.

Si L/K es Galois tenemos $X = G$ y definimos la aplicación:

$$\begin{aligned} \rho : G &\longrightarrow \mathrm{Perm}(G) \cong S_n \\ \tau &\mapsto \rho_G(\tau)(\sigma) = \sigma \circ \tau^{-1} \end{aligned}$$

que se llama traslación por la derecha.

Nota. Ambas aplicaciones son homomorfismos de grupos.

Definición 3.12. Sea G un grupo, y $H, K \subseteq G$ dos subgrupos. Decimos que H está normalizado por K si:

$$kHk^{-1} = H \quad \forall\ k \in K.$$

Ejemplo 3.13. Sea $G = D_3 = \{1, g, g^2, s, gs, g^2s\}$ tal que $g^3 = 1$, $s^2 = 1$, $sg = g^{-1}s = g^2s$, sea $H = \{1, g, g^2\}$ y $K = \{1, s\}$ subgrupos de G. Veamos que H está normalizado por K:

$$sgs^{-1} = g^{-1} = g^2 \in H,$$

$$sg^2s^{-1} = (sgs^{-1})^2 = (g^2)^2 = g \in H.$$

y evidentemente

$$s1s^{-1} = 1 \in H.$$

Definición 3.14. Un subgrupo $N \leq \mathrm{Perm}(X)$ se dice que es regular si se satisfacen dos de las tres siguientes condiciones:

1. $|N| = |X|$.
2. N actúa en X transitivamente. Esto es, para par de elementos $x, y \in X$ existe $n \in N$ tal que $x \cdot n = y$.
3. Para todo $x \in X$, el estabilizador de x, $\mathrm{Sta}_N = \{g \in N \mid g \cdot x = x\}$ es trivial. Cuando pasa esto, decimos que N actúa en X de manera libre o demanera simple.

Nota. Solo hace falta que se cumplan dos de las tres condiciones, ya que se puede asegurar que si se cumplen dos, la tercera siempre se cumple automáticamente (véase definición 6.2 [4]). Cuando N es regular, equivale a decir que N actúa simple y transitivamente sobre X.

Ejemplo 3.15. Sean S_3 y su subgrupo $A_3 = \{id, (123), (132)\}$ y $X = \{1, 2, 3\}$. Veamos que A_3 es regular.

Tomemos cualquier par $i, j \in \{1, 2, 3\}$. Como los elementos (123) y (132) permutan cíclicamente los tres elementos de X, siempre existe un elemento de A_3 que lleva a i en j. Por tanto, la acción es transitiva.

Veamos ahora que sí $\sigma \in A_3$ y $\sigma(i) = i$ para algún $i \in \{1, 2, 3\}$ entonces $\sigma = id$. Tenemos que de los elementos de A_3 no hay ningún elemento, excepto la identidad, que fije algún elemento; por tanto, tenemos lo que queríamos. Decimos que A_3 actúa de manera libre y transitiva en S_3.

Definición 3.16. Decimos que una extensión de cuerpos L/K es casi Galois clásica si existe un subgrupo regular N de S_n normalizado por G y contenido en G, donde G está identificado como subgrupo de S_n por la aplicación λ anterior.

Teorema 3.17. *(Teorema 1.3 [16]) Sea L/K una extensión separable de grado n y sea $\tilde{L}/K$ su clausura de Galois, $G = Gal(\tilde{L}/K)$ y $G' = Gal(\tilde{L}/L)$. Entonces L/K es casi Galois clásica si y solo si G' tiene un complemento normal N en G, esto es, $G = G' \cdot N$, $G' \cap N = e$ y $N \trianglelefteq G$ es un subgrupo normal de G.*

Demostración. Sea N un complemento normal de G' en G. Entonces $\lambda(N) \subset \lambda(G)$ es un subgrupo de S_n. Como N es un subgrupo normal de G, $\lambda(N)$ está normalizado por $\lambda(G)$. Probemos que $\lambda(N)$ es regular.

Primero veamos que es transitivo, es decir dados cualquier $\sigma, \tau \in G$, existe $\rho \in N$ tal que $\sigma \circ \rho \in \tau G'$ (ya que $X = G/G'$) que es lo mismo que $\sigma \circ \rho \circ \tau^{-1} \in G'$

Sean $\sigma, \tau \in G$. Como $G = NG'$ el elemento $\sigma \circ \tau^{-1} \in G$ se puede escribir como $\sigma \circ \tau^{-1} = \sigma_1 \circ \sigma_2$ con $\sigma_1 \in N$, $\sigma_2 \in G'$

Despejamos de la igualdad y obtenemos: $\sigma^{-1} \circ \sigma = \sigma_2 \circ \tau \implies \sigma_1^{-1} \circ \sigma \in \tau G'$ lo que implica que $\lambda(\rho)(\sigma) = \rho \circ \sigma = \tau \circ g'$ donde identificamos ρ con $\sigma_1^{-1} \in N$, $g' \in G$.

Luego $\lambda(\rho)(\sigma) = \rho \circ \sigma = \tau$ en $G/G' = X$.

Dado que N es transitivo, todos los estabilizadores son conjugados, por lo que para probar que cada elemento de X tiene un estabilizador trivial, basta

probar que $\bar{1}$ tiene un estabilizador trivial. Como paso previo, probamos que $\lambda(G') = \mathrm{Sta}_{\lambda(G)}(\bar{1})$:

$$\lambda(\sigma) \in \mathrm{Sta}_{\lambda(G)}(\bar{1}) \iff \lambda(\sigma)(\bar{1}) = \bar{1} \iff \sigma\bar{1} = \bar{1} \iff \sigma = \bar{1} \iff \sigma \in G'$$

$$\iff \lambda(\sigma) \in \lambda(G').$$

Dado que $N \cap G' = \{1\}$, se sigue que $\lambda(N) \cap \lambda(G') = \{1\}$. Pero $\mathrm{Sta}_{\lambda(N)}(\bar{1}) \subset \lambda(N)$, y también $\mathrm{Sta}_{\lambda(G)}(\bar{1}) = \lambda(G')$, por lo que:

$$\mathrm{Sta}_{\lambda(N)}(\bar{1}) \subset \lambda(N) \cap \lambda(G') = \{1\}.$$

Concluimos que $\mathrm{Sta}_{\lambda(N)}(\bar{1}) = \{1\}$. Entonces, $N' \subset \lambda(G)$ es un subgrupo regular de $\mathrm{Perm}(X)$ normalizado por $\lambda(G)$ y queda probado.

Recíprocamente, sea $N \subset \lambda(G)$ un subgrupo regular de $\mathrm{Perm}(X)$ normalizado por $\lambda(G)$. Dado que N es regular, se tiene que $\mathrm{Sta}_N(\bar{1}) = \{1\}$, por lo que:

$$N \cap \lambda(G) = \mathrm{Sta}_N(\bar{1}) = \{1\}.$$

Además, se cumple que $N\lambda(G') \subset \lambda(G)$ entonces notamos que

$$|N\lambda(G')| = \frac{|N| \cdot |\lambda(G')|}{|N \cap \lambda(G')|}$$

pero como $N \cap \lambda(G) = \{1\}$, $|N| = |X| = |G/G'|$ tenemos que

$$|N\lambda(G')| = |N||\lambda(G')| = |X||G'| = |G/G'||G'| = |G| = |\lambda(G)|,$$

por lo que $N\lambda(G') = \lambda(G)$. Dado que λ es inyectiva, se sigue que $\lambda^{-1}(N) \cap G' = \{1\}$ y que $\lambda^{-1}(N)G' = G$. Entonces, $\lambda^{-1}(N)$ es un complemento normal de G' en G. □

En particular, si L/K es de Galois, entonces $G' = 1$ y su complemento normal $N = G$.

Gracias a esta noción, obtenemos el siguiente teorema:

Teorema 3.18. *(Teorema 5.2 [10]) Si L/K es casi Galois clásica, entonces existe un álgebra de Hopf H tal que L/K es de Hopf-Galois con álgebra H y el Teorema 3.9 se cumple en su forma fuerte, es decir, existe una biyección entre las subálgebras de Hopf de H y los subcuerpos de L.*

Demostración. No explicitamos la demostración ya que en ella se hace uso de conceptos que no se ven en este trabajo, pero se puede consultar en el Teorema 5.2 [10]. □

Volvamos a nuestro problema inicial, determinar todas las estructuras de Hopf-Galois que tiene una extensión de cuerpos finita y separable. La respuesta nos la ofrece el teorema de Greither-Pareigis que veremos a continuación sin demostración, ya que es demasiado extensa y técnica.

Definición 3.19. Dada una extensión de cuerpos L/K y dos K-álgebras de Hopf H_1 y H_2, decimos que H_1 es una forma de L/K de H_2 si ambas álgebras de Hopf son isomorfas cuando extendemos escalares a L, es decir, si $H_1 \otimes_K L \cong H_2 \otimes_K L$.

Proposición 3.20. *(Teorema 2.5 [10]) Sea L/K una extensión finita y separable con clausura normal $\tilde{L}$, sea $G = Gal(\tilde{L}/K)$, $G' = Gal(\tilde{L}/L)$ y $X = G/G' = \{gG' : g \in G\}$. Si N es un subgrupo regular de S_n normalizado por $\lambda(G)$, entonces L/K es Hopf-Galois, donde H es una forma de L/K de $K[N]$.*

Teorema 3.21 (Greither-Pareigis)**.** *Sea L/K una extensión separable de cuerpos con clausura normal $\tilde{L}$, sea $G = Gal(\tilde{L}/K), G' = Gal(\tilde{L}/L)$ y $X = G/G' = \{gG' : g \in G\}$. Existe una biyección entre los subgrupos regulares del grupo $Perm(X)$ normalizados por $\lambda(G)$ y las estructuras de Hopf-Galois de L/K.*

Este teorema simplifica la búsqueda de estructuras de Hopf-Galois de extensiones separables, ya que las conecta mediante una biyección con el conjunto de subgrupos de un cierto grupo de permutaciones. Traduce el problema de determinar todas las estructuras de Hopf-Galois a un problema de grupos, que generalmente es más sencillo de trabajar.

Ahora vamos a usar el teorema de Greither-Pareigis para aportar más ejemplos de estructuras de Hopf-Galois. Para ello, buscaremos subgrupos de $Perm(X)$ normalizados por $\lambda(G)$.

Ejemplo 3.22. Sea $K = \mathbb{Q}$ y $L = \mathbb{Q}(\sqrt[3]{2})$. Esta es una extensión separable que no es de Galois pero sí de Hopf-Galois y su clausura normal es $\tilde{L} = \mathbb{Q}(\sqrt[3]{2}, w)$, donde w es la raíz cúbica de la unidad. Tenemos que $G = Gal(\tilde{L}/K) = S_3$ y $G' = Gal(\tilde{L}/L) = C_2$. $|X| = 3$ siendo $X = G/G'$.

Consideramos la siguiente aplicación:

$$\lambda : S_3 \to Perm(X) = Perm(G/G') \cong S_3$$

Entonces los subgrupos de $Perm(G)$ normalizados por $\lambda(G)$ son exactamente los subgrupos normales de S_3. El único subgrupo normal de S_3 con el mismo orden que X es A_3, que ya hemos demostrado que es regular en 3.15; por tanto, la extensión es de Hopf-Galois.

Ejemplo 3.23. (sección 1.2 [16]) Ya podemos retomar el ejemplo 3.7 desde esta nueva perspectiva.

Podemos describir H a partir de una base. Tenemos la extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ y consideramos su clausura algebraica $\tilde{L} = \mathbb{Q}\ (w, \alpha)$, donde w es una raíz cúbica primitiva de la unidad. Una base para $\tilde{L}/\mathbb{Q}$ es $\{1, \alpha, \alpha^2, w, w\alpha, w\alpha^2\}$. Tenemos que el grupo de Galois $G \cong S_3$ está generado por las permutaciones

$$\begin{array}{rcl} \tau : \tilde{L} & \longrightarrow & \tilde{L} \\ w & \longmapsto & w^2 \\ \alpha & \longmapsto & \alpha \end{array} \qquad \begin{array}{rcl} \sigma : \tilde{L} & \longrightarrow & \tilde{L} \\ w & \longmapsto & w \\ \alpha & \longmapsto & w\alpha \end{array}$$

Luego $G = \{Id, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\}$. El grupo $G' = Gal(\tilde{L}/\mathbb{Q}(\alpha)) = \langle\tau\rangle \cong C_2$ y $N = \langle\sigma\rangle \cong C_3$ es un complemento normal de G' en G.

Con todo esto consideramos

$$\tilde{L}[N] = \{u_0 Id + u_1\sigma + u_2\sigma^2 | u_i \in \tilde{L}\}$$

y buscamos los elementos para los que $\tilde{L}[N]$ se queda fijo bajo los automorfismos de G. Queremos calcular $\tau \cdot (u_0 Id + u_1\sigma + u_2\sigma^2)$ y $\sigma \cdot (u_0 Id + u_1\sigma + u_2\sigma^2)$ esto es

$$\tau(u_o) \cdot \tau Id\tau^{-1} + \tau(u_1) \cdot \tau\sigma\tau^{-1} + \tau(u_2) \cdot \tau\sigma\tau^{-1}$$

$$\sigma(u_o) \cdot \sigma Id\sigma^{-1} + \sigma(u_1) \cdot \sigma\sigma\sigma^{-1} + \sigma(u_2) \cdot \sigma\sigma\sigma^{-1}.$$

ya que los automorfismos de G actúan por conjugación.

Tenemos que $\tau\sigma\tau^{-1} = \sigma^2$, $\tau\sigma^2\tau^{-1} = \sigma$, $\sigma\sigma\sigma^{-1} = \sigma$, y que $\sigma\sigma^2\sigma^{-1} = \sigma^2$. Entonces

$$\tau \cdot (u_0 Id + u_1\sigma + u_2\sigma^2) = \tau(u_o) \cdot Id + \tau(u_1) \cdot \sigma^2 + \tau(u_2) \cdot \sigma$$

y

$$\sigma \cdot (u_0 Id + u_1\sigma + u_2\sigma^2) = \sigma(u_o) \cdot Id + \sigma(u_1) \cdot \sigma + \sigma(u_2) \cdot \sigma^2$$

Ahora, igualando con el original llegamos a que

$$\tau(u_o) = u_0, \quad \tau(u_1) = u_2, \quad \tau(u_2) = u_1$$

y

$$\sigma(u_o) = u_0, \quad \sigma(u_1) = u_1, \quad \sigma(u_2) = u_2$$

y para $u_1 = a + bw$ con $a, b \in \mathbb{Q}$, tenemos que $u_2 = \tau(u_1) = a + bw^2$.

Poniendo toda esta información junta, obtenemos que el álgebra de Hopf de la extensión es

$$H_1 = \tilde{L}[N]^G = \{u_o Id + (a + bw)\sigma + (a + bw^2)\sigma^2 | u_0, a, b \in \mathbb{Q}\},$$

la cual se corresponde con el álgebra H que hemos dado antes, ya que si tomamos como una base para H_1 $e_1 = Id$, $e_2 = \sigma + \sigma^2$,$w\sigma + w^2\sigma^2$, que son los invariantes bajo τ, podemos identificar $c = e_1$ y $s = e_2$, y las relaciones descritas aparecen operando.

Vamos a ver ahora dos resultados que nos van a decir en qué casos las extensiones de grado bajo admiten o no estructuras de Hopf-Galois, así que en estos casos no necesitaremos hacer el cálculo explícito.

3.3.1. Estructuras de Hopf-Galois de órdenes 3 y 4

Teorema 3.24. *([4] Proposición 6.13) Sea L/K una extensión separable con $[L : K] \leq 4$. Entonces L/K es Hopf-Galois.*

Demostración. Consideremos $\tilde{L}$ la clausura normal de la extensión, $G = Gal(\tilde{L}/K)$ y $G' = Gal(\tilde{L}/L)$.

Para la demostración usaremos repetidamente el teorema de Greither-Pareigis. Por tanto, para demostrar que L/K es Hopf-Galois, esto es, que posee al menos una estructura de Hopf-Galois, mostraremos en cada caso un subgrupo N concreto de $Perm(G/G')$ que es regular y está normalizado por $\lambda(G)$.

Si L/K es una extensión normal, entonces es Galois y por tanto Hopf-Galois. Supongamos entonces que L/K no es normal, lo que implica que $[L : K] \neq 2$. Empezaremos estudiando el caso $[L : K] = 3$.

Como los automorfismos de $\tilde{L}/K$ actúan sobre las 3 raíces del polinomio irreducible de L/K permutándolas, tenemos que $Gal(\tilde{L}/K) \leq S_3$. Pero como además sabemos que $|G| > 3$ por no ser L/K una extensión normal, la única opción que nos queda es $|G| \cong S_3$.

Por el teorema del grado sabemos que $|G'| = \frac{[\tilde{L}:K]}{[L:K]} = \frac{6}{3} = 2$, así que $G' \cong C_2$. Por lo tanto, $\frac{|G|}{|G'|} = \frac{6}{2} = 3$ y entonces $\mathrm{Perm}(G/G') \cong S_3$. Pero entonces el homomorfismo $\lambda\colon G \to \mathrm{Perm}(G/G')$ es en realidad un isomorfismo.

Escogemos el subgrupo $N = \lambda(A_3)$ de $\mathrm{Perm}(G/G')$. Comprobemos que N es regular y normalizado por $\lambda(G)$.

Verifiquemos primero que N es regular. Sabemos que $|N| = |A_3| = 3$ y también que $|X| = |G/G'| = 3$, se da la primera condición de la definición. Falta ver que N actúa o bien transitivamente, o bien, de manera libre. Veamos que se cumple esto último. A_3 es el conjunto de las permutaciones pares; $A_3 = \{Id, (123), (132)\}$ donde los elementos distintos de la identidad permutan elementos de manera cíclica, no dejan ningún elemento fijo. Por tanto, al considerar la acción de $\lambda(A_3)$ en X tenemos que ningún elemento a excepción de la identidad queda invariante. Luego N es regular.

Como λ es un isomorfismo, N es normalizado por $\lambda(G)$ por ser A_3 normal en S_3 (pues $[S_3 : A_3] = 2$).

Por tanto concluimos que las extensiones de grado 3 son de Hopf-Galois.

Ahora, supongamos que $[L : K] = 4$. Como la extensión no es normal $|G| > 4$. Las posibilidades son $G \cong S_4$, $G \cong A_4$ o $G \cong D_4$.

Supongamos que $G \cong S_4$. Como $|S_4| = 24$, por el teorema del grado:

$$[\tilde{L} : K] = [\tilde{L} : L][L : K] = 4|G'|,$$

así que $|G'| = 6$. Entonces, $|G/G'| = 4$ y $\mathrm{Perm}(G/G') \cong S_4$. Deducimos que $\lambda\colon G \to \mathrm{Perm}(G/G')$ es un isomorfismo. Sea $N \subset \mathrm{Perm}(G/G')$ la imagen por λ del grupo de Klein V_4 de S_4 que tiene orden 4. Como $|N| = 4 = |G/G'|$, la regularidad de N se demuestra como en el caso $[L : K] = 3$. Además, N es normalizado por $\lambda(G)$ porque λ es un isomorfismo y el grupo de Klein es normal en S_4.

Supongamos que $G \cong A_4$. En este caso $|A_4| = 12$

$$[\tilde{L} : K] = [\tilde{L} : L][L : K] = 4|G'|,$$

así que $|G'| = 3$ y $|G/G'| = 4$, por lo tanto $\mathrm{Perm}(G/G') \cong S_4$. Así, el subgrupo de Klein N de S_4 es un subgrupo regular de $\mathrm{Perm}(G/G')$.

Finalmente, $G \cong D_4$ $|D_4| = 8$

$$[\tilde{L} : K] = [\tilde{L} : L][L : K] = 4|G'|,$$

lo cual implica que $|G'| = 2$. Entonces $|G/G'| = 4$ y $\mathrm{Perm}(G/G') \cong S_4$ como en los casos anteriores. Sea N un subgrupo de orden 4 de $\lambda(G)$. Entonces $|N| = 4 = |G/G'|$, así que la regularidad de N se demuestra como en los otros casos. Finalmente, es normalizado por $\lambda(G)$ porque tiene índice 2 en $\lambda(G)$. □

3.3.2. Estructuras de Hopf-Galois de grado 5

Nuestro objetivo ahora es analizar cuándo una extensión L/K con grado 5 admite una estructura de Hopf-Galois.Siguiendo el método de la sección anterior, es directo ver que si $G \neq A_5, S_5$ entonces L/K es de Hopf-Galois (Teorema 4.6 [10]). Nos centraremos en consecuencia en los casos $G = A_5, S_5$, que resultarán no ser de Hopf-Galois.

Por el teorema del grado sabemos que $[L : K]$ divide a $[\tilde{L} : K] = |G|$. En este caso, como $[L : K] = 5$, deducimos que $|G|$ es múltiplo de 5. El resultado que veremos a continuación establece que si $|G| > 20$, entonces la extensión L/K no admite estructura de Hopf-Galois.

Primero demostraremos dos lemas que necesitaremos para la demostración de esto último.

Definición 3.25. Sean G un grupo y N un subgrupo de G. Definimos:

- EL centralizador de $N en$G es el subgrupo $Cent_G(N) = \{g \in G \mid gn = ng \,\forall\, n \in N\}$
- El normalizador de N en G es el subgrupo $Norm_G(N) = \{g \in G \mid gNg^{-1} = N\}$

Lema 3.26. *Sea G un grupo y sea N un subgrupo de G. Entonces, $|Norm_G(N)|$ divide a $|Cent_G(N)||Aut(N)|$*

Demostración. Consideremos la aplicación

$$f\colon \mathrm{Norm}_G(N) \longrightarrow \mathrm{Aut}(N)$$

$$\gamma \longmapsto f(\gamma)(n) = \gamma n \gamma^{-1}.$$

Esta aplicación es un homomorfismo de grupos que actúa por conjugación ya que:

$$f(\gamma\mu)(n) = \gamma\mu n(\gamma\mu)^{-1} = \gamma\mu n\mu^{-1}\gamma^{-1} = f(\gamma)(f(\mu)(n)),$$

y está bien definida porque si $\gamma \in Norm_G(N)$, entonces $\gamma n \gamma^{-1} \in N$ para todo n, por la propia definición del normalizador.

Nuestro objetivo es aplicar el primer teorema de isomorfía a la aplicación f, luego verifiquemos que $\ker(f) = \mathrm{Cent}_G(N)$. En efecto,

$$\gamma \in \ker(f) \iff f(\gamma) = \mathrm{Id}_N \iff \gamma n \gamma^{-1} = n \text{ para todo } n \in N \iff \gamma \in \mathrm{Cent}_G(N).$$

Ahora, aplicando el primer teorema de isomorfía:

$$\mathrm{Norm}_G(N)/\mathrm{Cent}_G(N) \cong \mathrm{Im}(f) \leq \mathrm{Aut}(N).$$

Así,

$$\frac{|\mathrm{Norm}_G(N)|}{|\mathrm{Cent}_G(N)|} \leq |\mathrm{Aut}(N)|,$$

lo que implica que

$$|\mathrm{Norm}_G(N)| \leq |\mathrm{Cent}_G(N)||\mathrm{Aut}(N)|.$$

□

A continuación, introducimos la noción de opuesto de un grupo que necesitamos para el segundo lema técnico.

Definición 3.27. Sea N un grupo cualquiera. El *opuesto* de N es el grupo N^{opp} cuyo conjunto subyacente es N y cuya operación binaria se define por $ab = b \cdot a$ para $a, b \in N$, donde $\cdot$ es la operación binaria original de N.

Nota. Los grupos N y N^{opp} son isomorfos ya que la aplicación que envía cada elemento de $n \in N$ a su inverso n^{-1} es un isomorfismo de grupos.

Lema 3.28. *(Lema 2.4.2 [10])*

Sea N un subgrupo regular de S_n. Entonces

$$\mathrm{Cent}_{S_n}(N) = \{\phi_\sigma \mid \sigma \in N\} \cong N^{\mathrm{opp}},$$

donde para todo $\sigma \in N$ e $i \in \{1, \ldots, n\}$, $\phi_\sigma(i) = \mu_i(\sigma(1))$, y $\mu_i \in N$ está determinado por $\mu_i(1) = i$. Además, N^{opp} también es regular.

Demostración. Sea $N \leq S_n$ un subgrupo regular, es decir, que actúa de manera simple y transitiva sobre $\{1, \ldots, n\}$.

De aquí se deduce que $|N| = n$ y que para cada i hay un único $\mu_i \in N$ con $\mu_i(1) = i$.

Ahora, para cada $\sigma \in N$ definimos

$$\phi_\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}, \quad \phi_\sigma(i) := \mu_i(\sigma(1)).$$

Esta definición está bien dada ya que para cada i existe un único μ_i y $\sigma(1)$ es un elemento del conjunto $\{1, \ldots, n\}$

Ahora queremos ver que $\phi_\sigma \in S_n$. Para ello veamos que es inyectiva, ya que en conjuntos finitos esto muestra la biyectividad. Supongamos que $\phi_\sigma(i) = \phi_\sigma(j)$, es decir, $\mu_i(\sigma(1)) = \mu_j(\sigma(1))$.

Recordando que la acción de N es regular, cada elemento $\mu \in N$ está completamente determinado por su imagen de 1, entonces $\mu_i(\sigma(1)) = \mu_j(\sigma(1))$. lo que implica $\mu_i = \mu_j \implies i = j$. Esto demuestra que es inyectiva y por lo tanto biyectiva.

Verifiquemos que $\mathrm{Cent}_{S_n}(N) = \{\phi_\sigma \mid \sigma \in N\}$. Sea $\phi \in \mathrm{Cent}_{S_n}(N)$. Nuevamente, por la simplicidad de la acción de evaluación, existe una única $\sigma \in N$ tal que $\sigma(1) = \phi(1)$. Por tanto, para todo i

$$\phi(i) = \phi \circ \mu_i(1) = \mu_i \circ \phi(1) = \mu_i(\sigma(1)) = \phi_\sigma(i),$$

Donde hemos usado que ϕ conmuta con todos los μ_i, ya que ϕ está en el centralizador. Entonces $\phi = \phi_\sigma$, y así:

$$Cent_{S_n}(N) = \{\phi_\sigma : \sigma \in N\}$$

Recíprocamente, sea $\sigma \in N$ y veamos que $\phi_\sigma \in \mathrm{Cent}_{S_n}(N)$. Sea $\mu \in N$. Podemos probar que $\mu \circ \phi_\sigma = \phi_\sigma \circ \mu$. Observamos que

$$\mu \circ \mu_i(1) = \mu(i) = \mu_{\mu(i)}(1)$$

para todo $i \in \{1, \ldots, n\}$, así que $\mu \circ \mu_i = \mu_{\mu(i)}$. Por lo tanto, para todo i

$$\mu \circ \phi_\sigma(i) = \mu \circ \mu_i(\sigma(1)) = \mu_{\mu(i)}(\sigma(1)) = \phi_\sigma \circ \mu(i)$$

Obtenemos que ϕ_σ conmuta con todos los elementos de N

Finalmente, probamos que $\mathrm{Cent}_{S_n}(N) \cong N^{\mathrm{opp}}$. Definimos la aplicación

$$\begin{aligned} \Phi \colon N^{\mathrm{opp}} &\longrightarrow \mathrm{Cent}_{S_n}(N) \\ \sigma &\longmapsto \phi_\sigma \end{aligned}$$

Entonces Φ es sobreyectiva ya que antes demostramos que todo $\phi \in Cent_{S_n}(N)$ es de la forma ϕ_σ para un único $\sigma \in N$ y claramente $\sigma \neq \tau \Longrightarrow \phi_\sigma \neq \phi_\tau$, así que Φ es inyectiva. Ahora, dados $\sigma, \tau \in N^{\mathrm{opp}}$ y $i \in \{1, \ldots, n\}$,

$$\phi_{\tau\circ\sigma}(i) = \mu_i(\tau \circ \sigma(1)) = \mu_i \circ \tau(\sigma(1)) = \phi_\sigma(\mu_i(\tau(1))) = \phi_\sigma \circ \phi_\tau(i),$$

así que

$$\Phi(\sigma \circ \tau) = \phi_{\tau\circ\sigma} = \phi_\sigma \circ \phi_\tau = \Phi(\sigma) \circ \Phi(\tau).$$

Por lo tanto, Φ es un isomorfismo de grupos.

Resta comprobar que N^{opp} es regular.Para ver esto, supongamos que ϕ_σ está en el estabilizador de i, es decir, $\phi_\sigma(i) = i$, lo que implica

$$\mu_i(\sigma(1)) = \phi_\sigma(i) = i = \mu_i(1).$$

Como μ_i es biyectiva, $\sigma(1) = 1$. Pero σ está completamente determinada por $\sigma(1)$, así que $\sigma = 1$. Entonces, $\mathrm{Sta}_{N^{\mathrm{opp}}}(i)$ es trivial y además, como tiene orden n, tenemos que es regular y obtenemos que el centralizador $Cent_{S_n}(N)$ es isomorfo a N^{opp} y que es regular. □

Proposición 3.29. *([10] Corolario 4.8) Sea L/K una extensión separable de grado 5 con $G \cong A_5$ o a S_5. Entonces L/K no es Hopf-Galois.*

Demostración. Vamos a razonar por reducción al absurdo. Supongamos que $G \cong A_5$ o que $G \cong S_5$ y que L/K tiene una estructura de Hopf-Galois.

Por el teorema de Greither-Pareigis, esto equivale a la existencia de algún subgrupo regular N de $\mathrm{Perm}(G/G')$ normalizado por $\lambda(G)$. Como tenemos $|G/G'| = 5$, $Perm(G/G') \cong S_5$.

Como N es regular, $|N| = |G/G'| = 5$ entonces N es cíclico. Ahora, usando los lemas anteriores

$$|Norm_{S_5}(N)| \leq |Cent_{S_5}(N)||Aut(N)| = |N^{opp}||Aut(N)| = 5 \cdot 4 = 20.$$

Ya que

- $|Cent_{S_n}(N)| = |N^{opp}| = |N| = 5$.
- $Aut(N) \cong Aut(C_5) \cong C_4$ ya que los automorfismos de un grupo cíclico de orden primo son las unidades de $\mathbb{Z}_p \cong C_{p-1}$.

Pero $|Norm_{S_5}(N)| \geq |G|$ porque $\lambda(G) \subset Norm_{S_5}(N)$. Por hipótesis, $G \cong A_5$ o $G \cong S_5$, lo que implica que $|G| > 20$, lo cual es una contradicción.

Por tanto no es de Hopf-Galois □

Nota. Con estos argumentos junto con alguna otra estimación se puede generalizar el teorema anterior a grado mayor que 5: Si L/K es separable con $[L : K] \geq 5$ y $G \cong A_n$ o S_n entonces no es de Hopf-Galois (Corolario 4.8 [10]).

3.4. Traducción de Byott

En este punto ya hemos conseguido una técnica que nos proporciona una manera de determinar todas las estructuras de Hopf-Galois de una extensión L/K finita y separable. Esto se lo debemos a Cornelius Greither y Bodo Pareigis, que establecieron una correspondencia biyectiva entre las estructuras de Hopf-Galois y los subgrupos de $Perm(X)$ normalizados por $\lambda(G)$, donde consideramos $\tilde{L}$ la clausura normal de L, $G' = Gal(\tilde{L}/L)$, $G = Gal(L/K)$ y $X = G/G'$.

Como ya habíamos adelantado, Greither-Pareigis proponen una solución poco eficiente, pues el número de grupos regulares crece mucho con $n = [L : K]$, y se puede volver muy tedioso encontrarlos todos. Para ello el matemático Nigel P. Byott introdujo en [2] una técnica que solucionó este problema, que recibe el nombre de traducción de Byott. Esta técnica nos permitirá clasificar las estructuras de Hopf-Galois de L/K con un menor número de cálculos.

Para ello, vamos a trasladar el problema de buscar un subgrupo regular N de $Perm(X)$ a buscarlos sobre $Perm(N)$ que es un grupo mucho más

manejable y nos permitirá describir completamente las estructuras de Hopf-Galois de L/K en términos de grupos. Veamos cómo hacemos esta traducción: Primero definimos igual que con G las siguientes aplicaciones:

$$\begin{aligned} \lambda : N &\longrightarrow \mathrm{Perm}(N) \\ \nu &\mapsto \lambda_G(\nu)(\mu) = \nu \circ \mu \end{aligned}$$

$$\begin{aligned} \rho : N &\longrightarrow \mathrm{Perm}(N) \\ \nu &\mapsto \rho_G(\nu)(\mu) = \mu \circ \nu^{-1} \end{aligned}$$

que son inyectivas y generan una copia de N en $Perm(N)$.

Como N es un subgrupo regular de $Perm(G)$, tenemos que la aplicación

$$\begin{aligned} b : N &\longrightarrow G \\ \nu &\mapsto \nu(1) \end{aligned}$$

es biyectiva. Esto nos permite trasladar el estudio de permutaciones de G a permutaciones de N e induce un isomorfismo en la siguiente aplicación:

$$\begin{aligned} \varphi : \mathrm{Perm}(G) &\longrightarrow \mathrm{Perm}(N) \\ \pi &\mapsto b^{-1} \circ \pi \circ b \end{aligned}$$

Entonces, dado $\nu, \mu \in N$ tenemos que

$$\varphi(\nu)(\mu) = b^{-1} \circ \nu \circ b(\mu) = b^{-1}(\nu \circ \mu(1)) = \nu \circ \mu = \lambda_N(\nu)(\mu).$$

Acabamos de ver que $\varphi(\nu) = \lambda_N(\nu)$ para todo $\nu \in N$. Con esto, somos capaces de transformar cualquier acción sobre G a una acción sobre N. En particular, tenemos que $\varphi(N) = \lambda_N(N)$.

Sea $G_0 = \varphi(\lambda_G(G))$, como φ es un isomorfismo, tenemos que $N \cong \lambda_N(N)$ y $\lambda_G(G) \cong G_0$. Por tanto, N está normalizado por $\lambda_G(G)$ si y solo si $\lambda_N(N)$ está normalizado por G_0.

Definición 3.30. Definimos el holomorfo de N como el normalizador de $\lambda_N(N)$ en $Perm(N)$, esto es,

$$Hol(N) = \{\varphi \in Perm(N) \mid \varphi\lambda(N)\varphi^{-1} = \lambda(N)\}.$$

Por tanto, N está normalizado por $\lambda_G(G)$ si y solo si $G_0 \subset Hol(N)$. Pero $G_0 \subset Hol(N)$ es equivalente a la existencia de una inclusión $\beta : G \longmapsto Hol(N)$. Esta es la idea que hay detrás del teorema de Byott.

La siguiente proposición nos da una manera de caracterizar $Hol(N)$

Definición 3.31. Sean N y H dos subgrupos de G. Decimos que G es producto semidirecto de N y H, $G = N \rtimes H$, si:

$$N \trianglelefteq G, \quad N \cap H = \{1\} \quad y \quad N \cdot H = G$$

Proposición 3.32. *([4] Proposición 7.2)* $Hol(N) = \rho_N(N) \rtimes Aut(N)$.

Nota. Aunque escribimos $Hol(N) = \rho(N) \rtimes Aut(N)$, en la demostración escribiremos $\rho(n) \circ \alpha$ para indicar cómo actúa cada elemento sobre N.

Demostración. Probemos primero la primera inclusión $\rho(N) \rtimes Aut(N) \subseteq Hol(N)$

Veamos que $\forall\ \rho(n) \in \rho(N)$ y $\alpha \in Aut(N)$ $\varphi = \rho(n) \circ \alpha \in Hol(N)$ lo que quiere decir que $\varphi \circ \rho(m) \circ \varphi^{-1} \in \rho(N)$,

$$\varphi \circ \rho(m) \circ \varphi^{-1} = \rho(n) \circ \alpha \circ \rho(m) \circ \alpha^{-1} \circ \rho(n)^{-1}$$

Podemos reescribir $\alpha \circ \rho(m) \circ \alpha^{-1}$ si vemos cómo actúa sobre $x \in N$:

$$(\alpha \circ \rho(m) \circ \alpha^{-1})(x) = \alpha(\alpha^{-1}(x)m^{-1}) = x \cdot \alpha(m)^{-1} = \rho(\alpha(m))(x)$$

Donde hemos usado $\rho(n)(m) = mn^{-1}$.

Entonces:

$$\varphi \circ \rho(m) \circ \varphi^{-1} = \rho(n) \circ \rho(\alpha(m)) \circ \rho(n^{-1}) = \rho(n\alpha(m)n^{-1}) \in \rho(N)$$

ya que si evaluamos $\rho(n) \circ \rho(\alpha(m)) \circ \rho(n^{-1})$ en $x \in N$,

$$\rho(n) \circ \rho(\alpha(m)) \circ \rho(n^{-1})(x) = \rho(n) \circ \rho(\alpha(m))(xn) = \rho(n)((xn)\alpha(m)^{-1})$$

$$= ((xn)\alpha(m)^{-1})n^{-1} = xn\alpha(m)^{-1}n^{-1}.$$

Por tanto $\varphi\rho(m)\varphi^{-1} \in \rho(N)$ para todo $m \in N$ y entonces $\varphi \in Hol(N)$.

Veamos la otra contención $Hol(N) \subseteq \rho(N) \circ Aut(N)$.

Supongamos $\pi \in Hol(N)$. Entonces para todo $n \in N$ se tiene que $\pi\lambda(n)\pi^{-1} \in \lambda(N)$. Como λ_N es inyectiva, esto significa que existe un único $\gamma(n) \in N$ tal que $\pi\lambda(n)\pi^{-1} = \lambda(\gamma(n))$.

$\gamma : N \to N$ definida por $\gamma(n)$ como la única que $\pi\lambda(n)\pi^{-1} = \lambda(\gamma(n))$ que como está definida por conjugación se cumple que es un automorfismo. Lo comprobamos.

Es homomorfismo:

$$\gamma(n)(m) = \pi\lambda(n)\lambda(m)\pi^{-1} = (\pi\lambda(n)\pi^{-1})(\pi\lambda(m)\pi^{-1}) = \gamma(n) \cdot \gamma(m)$$

Es biyectiva:

Definimos la inversa $\gamma^{-1} : N \longrightarrow N$ por $\gamma^{-1}(n) = \gamma^{-1}\lambda(n)\gamma$ y componemos

$$\gamma(\gamma^{-1}(n)) = \gamma(\gamma^{-1}\lambda(n)\gamma)\gamma^{-1} = (\gamma\gamma^{-1})\lambda(n)(\gamma\gamma^{-1}) = n,$$

y análogamente para $\gamma^{-1}\gamma$.

Efectivamente es un homomorfismo biyectivo, es decir, un automorfismo.

Ahora evaluamos

$$\pi(n) = \pi\lambda(n)(e) \quad (\lambda(n)(e) = n)$$

$$= (\lambda(\gamma(n))\pi)(e) = \lambda(\gamma(n))(\pi(e)) = \gamma(n)\pi(e)$$

$$= \rho(\pi(e)^{-1})(\gamma(n)) \in \rho(N) \circ Aut(N).$$

□

Veamos ahora el teorema de Byott, que establece una correspondencia biyectiva entre las inclusiones $\alpha : N \longmapsto Perm(X)$ y $\beta : G \longmapsto Perm(N)$ de manera que $\beta(G') = Sta_N(1)$.

Teorema 3.33 (Byott)**.** *(Teorema 7.3 [4]) Sean G y G' grupos finitos con $G' \subset G$ y pongamos $X = G/G'$. Sea N un grupo tal que $|N| = |X|$. Existe una biyección entre los conjuntos:*

$$\mathcal{N} = \{\alpha : N \longmapsto Perm(X) \mid \alpha \, homomorfismo \, inyectivo, \alpha(N) \, regular\},$$

$$\mathcal{G} = \{\beta : G \longmapsto Perm(N) \mid \beta \, homomorfismo \, inyectivo, \beta(G') = Sta_N(1)\}.$$

Bajo esta biyección, si $\alpha \in \mathcal{N}$ se corresponde con $\beta \in \mathcal{G}$, entonces $\alpha(N)$ está normalizado por $\lambda(G)$ si y solo si $\beta(G')$ está contenido en $Hol(N)$.

Demostración. En este caso, no vamos a explicitar la demostración ya que es muy extensa, pero daremos la idea principal. Se puede encontrar la demostración detallada en [4] Teorema 7.3

El objetivo es encontrar una aplicación biyectiva $\Phi : \mathcal{N} \longrightarrow \mathcal{G}$, mediante la composición de de otras tres biyecciones.

La primera se construye tomando $\alpha \in \mathcal{N}$. Y se crea la biyección $\alpha(N) \longrightarrow \alpha(N) \cdot \overline{1}$ que demuestra que $X = \alpha(N) \cdot \overline{1}$.

Esta biyección induce otra $a : N \longrightarrow X$, que a su vez induce un isomorfismo $C(a) : Perm(N) \longrightarrow Perm(X)$. Ahora componiendo la inversa de C(a) y la aplicación $\lambda : G \longrightarrow Perm(X)$ que ya conocemos obtenemos la biyección Φ buscada.

□

Vamos a ilustrar el teorema con un ejemplo sencillo.

Ejemplo 3.34. (Daniel Gil Muñoz) Sea L/K una extensión separable de grado 4, $[L : K] = 4$, y supongamos que $[\tilde{L} : K] = 12$ donde $\tilde{L}$ es la clausura normal de L/K.

$G = Gal(\tilde{L}/K)$ tiene cardinal 12. Sea $G' = Gal(\tilde{L}/L)$, tenemos que

$$|G'| = \frac{[\tilde{L} : K]}{[L : K]} = \frac{12}{4} = 3.$$

Por tanto G/G' es de orden 4 y entonces $Perm(G/G') \cong S_4$

Ahora vamos a aplicar el teorema de Greither-Pareigis con la traducción de Byott que nos dice que hay una biyección entre las estructuras de Hopf-Galois de L/K y los homomorfismos inyectivos de grupos $\beta : G \to Hol(N) \subseteq Perm(N)$ tal que $\beta(G') = Sta_N(1)$ con N un grupo tal que $|N| = |G/G'|$

Los subgrupos de orden 4 de S_4 son C_4 y $C_2 \times C_2$. Calculamos ahora $Hol(N)$ en ambos casos:

- $N = C_4$,

$Hol(C_4) = C_4 \rtimes C_2$ ya que $Aut(C_4) \cong C_2$,

$|Hol(C_4)| = 4 \cdot 2 = 8$.

Entonces para que C_4 defina una estructura de Hopf-Galois G debería poder inyectarse en $Hol(N)$ lo cual es imposible ya que $|G| = 12$.

- $N = C_2 \times C_2$,

  $Hol(C_2 \times C_2) = (C_2 \rtimes C_2) \rtimes S_3$ ya que $Aut(C_2 \times C_2) \cong S_3$.

  En este caso si que podemos inyectar G en $Hol(C_2 \times C_2)$ ya que $|Hol(C_2 \times C_2)| = 4 \cdot 6 = 24$.

Falta ver que $Sta_G(1) = G'$, que es lo mismo que comprobar que $Sta_N(G') = \beta(G')$ ya que identificamos N y G/G' vía β.

Tenemos que G actúa sobre G/G' por multiplicación a izquierda, es decir, $g \cdot (xG') = (gx)G'$ para todo $g, x \in G$.

Ahora sí consideramos $x = 1$ tenemos que $1 \cdot G' = G' \in G/G'$. Su estabilizador está formado por los $g \in G$ tal que $gG' = G'$.

Esto ocurrirá si $g \in G'$ que $gG' = hG'$ si y solo si $g^{-1}h \in G'$. Por tanto,

$$Sta_G(1) = \{g \in G \mid gG' = G'\} = G'.$$

Por tanto, la extensión L/K tiene una única estructura de Hopf-Galois, dada por $C_2 \times C_2$

3.4.1. Contando estructuras de Hopf-Galois

Ya sabemos cómo encontrar todas las estructuras de Hopf-Galois de una extensión sin tener que hacer muchos cálculos. Ahora vamos a ver una manera de contar esas estructuras sin distinguir entre isomorfismos, es decir, si tenemos dos subgrupos N, N' de $Perm(X)$ isomorfos, contaremos una única estructura de Hopf-Galois.

Para ello, agruparemos los subgrupos N por clases de isomorfismo. Esta clasificación nos permitirá organizar las estructuras de Hopf-Galois de L/K según el tipo de grupo N al que están asociadas. Así llegaremos al número real de estructuras que tiene la extensión.

Denotamos por $e(G, G', N')$ la cantidad de subgrupos de $Perm(X)$ isomorfos a N que son regulares y están normalizados por λ_G. Por el teorema de Greither-Pareigis, esta cantidad es exactamente el número de estructuras de Hopf-Galois de tipo N.

Llamemos $\mathcal{S}$ al grupo de isomorfismos de todos los grupos de orden $|X|$, entonces el número total de estructuras de Hopf-Galois de la extensión L/K está dado por:

$$\sum_{[N]\in\mathcal{S}} e(G, G', N).$$

Sabemos teóricamente lo que es $e(G, G', N)$ pero necesitamos saber cuál es su valor numérico; por eso, nuestro siguiente paso es contar cuántos grupos isomorfos a N hay.

Sea $e'(G, G', N)$ el conjunto de subgrupos H de $Hol(N)$ tal que hay un isomorfismo de G a H que envía G' al estabilizador de 1 en H.

Proposición 3.35. *Sea L/K una extensión separable y sea N un grupo de orden $|X|$. Entonces,*

$$e(G, G', N) = \frac{|Aut(G, G')|}{|Aut(N)|} e'(G, G', N),$$

donde $Aut(g, G') = \{\varphi \in G \mid \varphi(G') = G'\}$.

Demostración. Denotemos

$$\mathcal{N} = \{\alpha : N \longrightarrow \mathrm{Perm}(X) \mid \alpha \text{ homomorfismo inyectivo, } \alpha(N) \text{ regular}\},$$

$$\mathcal{G} = \{\beta : G \longrightarrow \mathrm{Hol}(N) \mid \beta \text{ homomorfismo inyectivo }, \beta(G') = \mathrm{Sta}_N(1)\}.$$

Por el teorema de Byott, estos dos conjuntos son biyectivos. Dado $\alpha \in \mathcal{N}$, $\alpha(N)$ es un subgrupo regular de $\mathrm{Perm}(X)$ normalizado por $\lambda(G)$, todos esos subgrupos son de esta forma y su cantidad total es $e(G, G', N)$.

Dos elementos $\alpha, \alpha' \in \mathcal{N}$ dan lugar al mismo subgrupo si y solo si $\alpha^{-1} \circ \alpha' \in Aut(N)$, ya que si $\alpha(N) = \alpha'(N)$, entonces existe $\varphi \in Aut(N)$ tal que $\alpha' = \alpha \circ \varphi$. Entonces, $|\mathcal{N}| = |Aut(N)|\, e(G, G', N)$.

De manera similar, dada $\beta \in \mathcal{G}$, $\beta(G)$ es un subgrupo de $\mathrm{Hol}(N)$ que envía G' al estabilizador de 1 en $\beta(G)$. El número total de subgrupos de

este tipo es $e'(G, G', N)$. Además, por lo mismo que antes, si $\beta, \beta' \in \mathcal{G}$ dan lugar al mismo subgrupo, entonces $\beta^{-1} \circ \beta' \in \mathrm{Aut}(G, G')$. Luego, $|\mathcal{G}| = |\mathrm{Aut}(G, G')|\, e'(G, G', N)$.

Juntando las dos igualdades que hemos calculado, obtenemos

$$e(G, G', N) = \frac{|\mathrm{Aut}(G, G')|}{|\mathrm{Aut}(N)|}\, e'(G, G', N).$$

□

Así, obtenemos un conteo explícito del número de estructuras de Hopf-Galois.

Corolario 3.36. *Sea L/K una extensión separable. El número de estructuras de Hopf-Galois de L/K es*

$$\sum_{[N]\in\mathcal{S}} \frac{|Aut(G, G')|}{|Aut(N)|} e'(G, G', N).$$

Vamos a ver un ejemplo concreto del uso de este teorema.

Ejemplo 3.37. (Daniel Gil Muñoz) Sea L/K una extensión de cuerpos de grado 3, $[L : K] = 3$ con clausura normal $\tilde{L}$ tal que $[\tilde{L} : K] = 6$, $G = Gal(\tilde{L}/K) \cong S_3$. Entonces $G' = Gal(\tilde{L}/L) \cong C_2$, lo que implica que $|G/G'| = 3$.

Lo primero que vamos a hacer es buscar los posibles N. En este caso, $|N| = |G/G'| = 3$, luego el único candidato es el grupo cíclico de orden 3, C_3.

Ahora contaremos los automorfismos de G que dejan fijos G'. Tenemos que $S_3 = \{(12), (23), (13), (123), (132), id\}$ y $C_2 = \{id, (12)\}$; como los automorfismos de S_3 están definidos por conjugación, los únicos que dejan fijo C_2 son los formados por id y por (12). Luego $|Aut(G, G')| = 2$.

El siguiente paso es calcular $|Aut(N)|$. Esto es fácil ya que $|Aut(N)| = \varphi(|N|)$, donde φ es la función de Euler. Por tanto, $|Aut(C_3)| = \varphi(3) = 2$.

Por último, antes de aplicar la fórmula, tenemos que encontrar los monomorfismos $\beta : S_3 \longrightarrow Hol(C_3)$ tales que $\beta(G') = Sta_{C_3}(1)$. Sabemos que

$Hol(C_3) = C_3 \rtimes C_2 \cong S_3$, luego buscamos las inyecciones $\beta : S_3 \longrightarrow S_3$ tales que $\beta(C_2) = Sta_{C_3}(1)$.

En S_3 hay 3 subgrupos de orden 2, pero solo uno que fija el 1. Luego $e'(G, G', N) = 2$, ya que evidentemente la identidad también fija el 1.

Ahora, aplicando la fórmula, tenemos:

$$\sum_{[N]\in\mathcal{S}} \frac{|Aut(G, G')|}{|Aut(N)|} e'(G, G', N) = \frac{2}{2} \cdot 2 = 2.$$

Luego concluimos que tenemos 2 estructuras de Hopf-Galois para esta extensión.

Este ejemplo nos muestra que para un mismo subgrupo normalizado N, podemos tener distintas estructuras de Hopf-Galois. Esto es debido a que puede haber distintas maneras de inyectar G en $Hol(N)$, de forma que $\beta(G') = Sta_N(1)$. Por ello, en este caso, aunque tenemos un único subgrupo N, tenemos 2 estructuras de Hopf-Galois.

Para concluir esta memoria, vamos a comentar tres consecuencias de los potentes resultados de Greither-Pareigis y Byott, relacionadas con el número de estructuras de Hopf-Galois de una extensión y con la imposibilidad de conseguir una correspondencia biyectiva en general con el retículo de subcuerpos:

1) Extensiones de Galois con más de una estructura de Hopf-Galois:

A lo largo del trabajo hemos visto que si tenemos una extensión L/K que es Galois, con grupo de Galois G, esta tiene una estructura de Hopf-Galois natural, que obtenemos tomando su álgebra de grupo asociada $K[G]$. Pero no tiene por qué ser la única estructura Hopf-Galois que tenga la extensión. Usando el teorema de Greither-Pareigis se ve claro, ya que dice que hay una biyección entre los subgrupos de $Perm(G/G')$ normalizados por $\lambda(G)$ y las estructuras de Hopf-Galois. Lo que ocurre es que cuando la extensión es de Galois, G es uno de esos subgrupos, pero no tiene por qué ser único. Veamos un ejemplo sencillo.

Ejemplo 3.38. (Sección 2.2 [16]) Partamos del ejemplo 1.37, donde tenemos la extensión de cuerpos $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, que es una extensión de Galois con grupo de Galois G isomorfo al grupo de Klein. Aqui, tenemos que mediante $\lambda : G \longrightarrow Perm(G)$, podemos identificar G con S_4.

Ahora, vamos a buscar las estructuras de Hopf-Galois de L/K, haciendo uso del teorema de Greither-Pareigis, es decir, buscamos los subgrupos N de S_4 normalizados por el grupo de Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$. Tomando $N = \mathbb{Z}_2 \times \mathbb{Z}_2$, obtenemos la estructura clásica de Galois que corresponde al álgebra de grupo $K[G]$, pero este no es el único subgrupo, tenemos también:

$$N_1 = \langle (1,2,3,4) \rangle, \qquad N_2 = \langle (1,3,2,4) \rangle, \qquad N_3 = \langle (1,3,2,3) \rangle,$$

que están normalizados por $\mathbb{Z}_2 \times \mathbb{Z}_2$.

2) Estructura de Hopf-Galois con correspondencia no biyectiva:

Ahora, siguiendo los pasos que hemos dado en el ejemplo 3.23, construimos el álgebra de Hopf asociada al subgrupo N_1, es decir, $H = L[N_1]^G = \langle 1, g_1^2, g_1 + g_1^3, \sqrt{2}(g_1 - g_1^3) \rangle$, donde $g_1 = (1,2,3,4)$. Este álgebra de Hopf tiene una única subálgebra de Hopf, que corresponde al único subgrupo de N_1 generado por g_1^2. En este ejemplo, el teorema fundamental no se cumple en su forma fuerte, ya que con el álgebra de Hopf asociada a N_1 el retículo de cuerpos queda:

$$\begin{array}{c} \mathbb{Q} \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q}(\sqrt{2}, \sqrt{3}) \end{array}$$

3) Extensiones de Galois sin más estructuras de Hopf-Galois:

Hay veces que la extensión, cuando es de Galois, sí que tiene una única estructura de Hopf-Galois. ¿Cuándo ocurre esto? La respuesta está en el teorema de unicidad de Byott, que dice:

Teorema 3.39. *Una extensión de Galois L/K con grupo de Galois G tal que $|G| = n$ tiene una única estructura de Hopf-Galois si y solo si $|G|$ es un número de Burnside, es decir, cumple que $m.c.d(n, \varphi(n)) = 1$, con φ la función de Euler.*

Este es el teorema principal de [2] y se demuestra usando el corolario 3.36.

Bibliografía

[1] E. Abe. *Hopf Algebras*. Cambridge University Press, 1980. Original Japanese version published by Iwanami Shoten, Tokyo, 1977.

[2] N. P. Byott. Uniqueness of Hopf Galois structure for separable field extensions. *Comm. Algebra*, 24(10):3217–3228, 1996.

[3] S.U. Chase and M. E.Sweedler. *Hopf algebras and Galois theory*. Lecture Notes in Mathematics, Vol. 97. Springer-Verlag, Berlin-New York, 1969.

[4] L. N. Childs. *Taming Wild Extensions. Hopf Algebras and Local Galois Module Theory*. American Mathematical Society, 2000.

[5] P. M. Cohn. *Basic algebra. Groups, rings and fields*. Springer-Verlag London, Ltd., London, 2003.

[6] K. Conrad. *Tensor Products I*. Expository paper, https://kconrad.math.uconn.edu/blurbs/linmultialg/tensorprod.pdf.

[7] D. S. Dummit and R.M. Foote. *Abstract algebra*. John Wiley Sons, 2004.

[8] M. Salguero García. *Algorithmic Hopf Galois theory*. Trabajo Fin de Master. Universidad de Barcelona, 2019.

[9] M. Salguero García. *Hopf Galois theory of separable field extensions*. Trabajo fin de grado, Universidad de Barcelona, 2016.

[10] C. Greither and B. Pareigis. *Hopf Galois theory for separable field extensions. J. Algebra*, 106(1):239–258, 1987.

[11] A. P. Gutiérrez. *Álgebras de Hopf y Extensiones de Galois*. Tesis doctoral, Universidad de los Andes, Colombia, 2006.

[12] D. Jimenez. Capítulo 3 producto tensorial. Apuntes de clase. Universidad de Valparaíso, Chile.

[13] S. Lang. *Algebra*. Springer-Verlag New York Inc, 2002, 3rd edition.

[14] M. Siles Molina. *Introducción a la teoría de módulos*. Escuela Pre-CIMPA 2015, 2014.

[15] S. Montgomery. *Hopf algebras and their actions on rings*, volume 82 of *CBMS Regional Conference Series in Mathematics*. 1993.

[16] A.Rio y M.Vela T.Crespo. *From Galois to Hopf Galois: Theory and Practice. Trends in number theory*. 29–46, Contemp. Math., 649, Amer. Math. Soc., Providence, Rl, 2015.

[17] R. G. Underwood. *Fundamentals of Hopf algebras*. Universitext. Springer, Cham, 2015.