UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

De Galois a Galois-Hopf

Autor/es

Alejandro Bergasa Alonso

Director/es

JOSÉ MARÍA PÉREZ IZQUIERDO

Facultad

Facultad de Ciencia y Tecnología

Titulación

Grado en Matemáticas

Departamento

MATEMÁTICAS Y COMPUTACIÓN

Curso académico

2021-22

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

UNIVERSIDAD DE LA RIOJA

Facultad de Ciencia y Tecnología

TRABAJO FIN DE GRADO

Grado en Matemáticas

De Galois a Galois-Hopf

Realizado por:

Alejandro Bergasa Alonso

Tutelado por:

José María Pérez Izquierdo

Logroño, Julio, 2022

Resumen

En este trabajo estudiaremos cómo la teoría de Galois puede ser generalizada a anillos que no son cuerpos. Esto requerirá redefinir la forma en que entendemos las extensiones de anillos, así como introducir nuevas restricciones que limitarán el alcance del nuevo teorema fundamental. El primer capítulo generalizará la teoría de Galois a extensiones de anillos conmutativos unitarios y establecerá una biyección entre los subgrupos de su grupo de Galois y algunas de sus subextensiones. El segundo capítulo introduce la teoría de Galois-Hopf, que generaliza la teoría de Galois a anillos unitarios arbitrarios sustituyendo la acción del grupo de Galois sobre la extensión por la coacción de dos álgebras de Hopf diferentes. El nuevo teorema fundamental establecerá una biyección entre algunas de las subextensiones de la extensión y ciertas subestructuras asociadas a una de las álgebras de Hopf. Estudiaremos en ambos casos cómo funciona la nueva teoría para extensiones de Galois clásicas y cómo se relaciona con la usual.

Abstract

We will discuss how Galois theory can be generalized to rings that are not fields. This will require redefining the way we understand ring extensions, as well as introducing new restrictions that will limit the scope of the new fundamental theorem. Chapter 1 will generalize Galois theory to unitary commutative ring extensions and will establish a bijection between the subgroups of their Galois groups and some of their subextensions. Chapter 2 introduces Hopf-Galois theory, which generalizes Galois theory to arbitrary unitary rings, replacing the Galois group action on the extension by the coaction of two different Hopf algebras. The new fundamental theorem will establish a bijection between some of the extension's subextensions and certain substructures associated to one of the Hopf algebras. In both cases we will study how the new theory behaves for classical Galois extensions and the way it is related to the usual one.

Índice general

Índice general III

Introducción 1

1. Teoría de Galois para anillos conmutativos 3

1.1. Extensiones de Galois de anillos conmutativos . . . 3

1.1.1. Homomorfismos fuertemente distintos . . . 3

1.1.2. Separabilidad . . . 3

1.1.3. Algunas álgebras y aplicaciones importantes . . . 5

1.1.4. Extensiones de Galois . . . 6

1.2. El teorema fundamental generalizado . . . 12

1.2.1. Subálgebras fuertes . . . 12

1.2.2. El teorema fundamental . . . 12

1.3. Ejemplos . . . 15

1.3.1. Extensión de anillos conmutativos a partir de una extensión de cuerpos . . . 15

1.3.2. Estudio de las extensiones de Galois $F \times \cdots \times F/F$ . . . 18

2. Teoría de Galois-Hopf 25

2.1. H-Extensiones de anillos . . . 25

2.1.1. Álgebras de Hopf . . . 25

2.1.2. Comódulos y comódulo álgebras . . . 27

2.1.3. H-Extensiones de Galois . . . 27

2.1.4. Estructura de ${}_A\mathcal{M}^H$ y $\mathcal{M}_A^H$ . . . 28

2.2. Extensiones fielmente planas . . . 29

2.3. (L, H)-Extensiones bi-Galois . . . 33

2.4. El álgebra de Hopf $L(A, H)$ . . . 33

2.4.1. Estructura de álgebra de Hopf de $L(A, H)$ . . . 33

2.4.2. A/R es una $(L(A, H), H)$-extensión bi-Galois . . . 39

2.5. El teorema fundamental de la teoría de Galois-Hopf . . . 40

2.5.1. Los conjuntos Quot(L) y Sub(A) 40
2.5.2. La conexión de Galois 41
2.5.3. Elementos admisibles y la correspondencia de Galois-Hopf 43
2.6. Ejemplos 44

Apéndice I. Módulos **52**

Apéndice II. Producto tensorial **54**

Apéndice III. Álgebras sobre anillos conmutativos **55**

Apéndice IV. Dual de un álgebra de Hopf **56**

Introducción

Las referencias históricas del siguiente apartado pueden encontrarse en [3], [10], [14].

Évariste Galois fue un matemático francés nacido el 31 de mayo de 1811. A pesar de su temprano fallecimiento en 1832, su trabajo sentó las bases de la teoría que a día de hoy lleva su nombre. La teoría de Galois conecta la teoría de cuerpos con la teoría de grupos. ¿Pero es posible ampliar esta teoría a estructuras más generales que los cuerpos? ¿Puede encontrarse un resultado similar al teorema fundamental de la teoría de Galois para, por ejemplo, extensiones de anillos conmutativos unitarios? En 1960, M. Auslander y O. Goldman introdujeron la noción de extensión de Galois de un anillo conmutativo, y la utilizaron para generalizar la teoría de extensiones de Galois a anillos conmutativos unitarios. En el capítulo 1 estudiaremos esta generalización, y comprobaremos que el nuevo teorema fundamental es equivalente al usual cuando nos restringimos a extensiones de Galois clásicas. Corresponde con el teorema 1.16 y su enunciado es el siguiente:

Figura 1: Évariste Galois.

Teorema. *Sea S una extensión de Galois de R con grupo de Galois G. Existe una correspondencia biyectiva entre los subgrupos de G y las R-subálgebras [G-fuertes] de S. Si T es una R-subálgebra separable [G-fuerte] de S, entonces el subgrupo correspondiente es*

$$\mathrm{Fix}(T) = \{\sigma \in G \mid \sigma(t) = t, \quad \textit{para todo } t \in T\}.$$

Esta correspondencia preserva la acción de G de la forma: si $\sigma \in G$ y T es una R-subálgebra separable [G-fuerte] de S, entonces $\mathrm{Fix}(\sigma(T)) = \sigma T \sigma^{-1}$. Un subgrupo H de G es normal si y solo si S^H es estable por el producto de elementos de G, en cuyo caso S^H es una extensión de Galois de R con grupo de Galois G/H.

¿Puede generalizarse más? ¿Puede desarrollarse una teoría de Galois para extensiones de anillos no necesariamente conmutativos? Una respuesta es la teoría de Galois-Hopf, que combina la teoría de Galois con una estructura algebraica llamada *álgebra de Hopf*, nacida en la década de 1950. En 1965 C. U. Chase, D. K. Harrison y A. Rosenberg [3] definieron el concepto de *extensión de Galois-Hopf* con el objetivo de generalizar la teoría de Galois clásica de grupos de automorfismos de cuerpos a grupos que actúan sobre anillos conmutativos. En 1969 S.U. Chase y M. E. Sweedler [4] extendieron estas ideas a coacciones de álgebras de Hopf sobre R-álgebras conmutativas, donde R es un anillo conmutativo unitario. Estudiaremos esto en el capítulo 2, donde veremos que la gran diferencia que esta teoría introduce es que las extensiones adecuadas para el teorema fundamental no están «controladas» por solo un álgebra de Hopf, sino que lo

están por dos. Las extensiones de Galois se convierten aquí en extensiones bi-Galois, contando con una estructura de extensión de Galois a derecha con un álgebra de Hopf H y a izquierda con otro álgebra de Hopf L. El teorema fundamental establecerá una biyección entre algunas subextensiones de la extensión de Galois a derecha y algunas subestructuras de L. Observaremos cómo un grupo G y un anillo conmutativo unitario R inducen de manera natural dos álgebras de Hopf: el álgebra grupo $R[G]$ y su dual $R[G]^*$. Estudiaremos cómo las extensiones de la teoría de Galois clásica pueden ser trasladadas a la teoría de Galois-Hopf mediante el dual del álgebra grupo. Por último, comprobaremos cómo el teorema fundamental de la teoría de Galois-Hopf no equivale al usual para extensiones clásicas, sino que solo permite establecer una biyección entre las subextensiones y subgrupos normales. Corresponde al teorema 2.42 de la memoria y su enunciado es el siguiente:

Teorema. *Sean H y L dos R-álgebras de Hopf con antípodas biyectivas. Sea A/R una (L,H)-extensión bi-Galois fielmente plana. Las aplicaciones $\mathcal{F}$ y $\mathcal{G}$ de la proposición 2.39 inducen biyecciones (mutuamente inversas) entre los coideales admisibles $I \in \mathrm{Quot}(L)$ y las subálgebras admisibles $B \in \mathrm{Sub}(A)$.*

Capítulo 1

Teoría de Galois para anillos conmutativos

1.1. Extensiones de Galois de anillos conmutativos

En esta sección ampliaremos la definición de extensiones de Galois a anillos conmutativos arbitrarios (unitarios) siguiendo la teoría desarrollada por [3]. El objetivo será obtener una generalización del teorema fundamental de la teoría de Galois apto para este nuevo tipo de extensiones. L

En lo que sigue se supondrá que todos los anillos, módulos y homomorfismos entre anillos son unitarios. La notación habitual será S, R para los anillos conmutativos de la extensión S/R. El símbolo «$\otimes$» se utilizará como abreviatura de «$\otimes_R$» (producto tensorial sobre el anillo R). Si G es un subgrupo finito de automorfismos del anillo S, denotamos por S^G o $\mathrm{Fix}(G)$ al subanillo de S formado por los elementos que quedan fijados por todo $\sigma \in G$.

1.1.1. Homomorfismos fuertemente distintos

Comenzamos introduciendo una noción necesaria para poder generalizar los resultados a anillos conmutativos arbitrarios.

Definición 1.1 (Homomorfismos fuertemente distintos)**.** Sean $f, g : S \to T$ homomorfismos de anillos conmutativos. f y g se dicen **fuertemente distintos** si, para todo idempotente no nulo $e \in T$, existe $s \in S$ tal que $f(s)e \neq g(s)e$.

Es claro que si 0 y 1 son los únicos idempotentes de T, entonces «fuertemente distintos» equivale a «distintos».

1.1.2. Separabilidad

Generalizar la teoría a anillos conmutativos también nos exige redefinir el significado de lo que llamábamos *separabilidad* en la teoría de Galois clásica.

Nota 1.2. Sea A un álgebra. A^{op} es el álgebra A pero con el producto opuesto ($a \cdot b := ba$). Definimos el álgebra $A^{\mathrm{e}} := A \otimes A^{\mathrm{op}}$ y notamos que A es A^{e}-módulo con la acción dada por $a' \otimes b' \cdot a := a'ab'$. Un ejemplo de la utilidad de A^{e} es que los ideales biláteros de A son los

A^{e}-submódulos para esta acción. Para que se dé esta estructura es necesario usar A^{op} en lugar de A, ya que $a' \otimes b' \cdot (a'' \otimes b'' \cdot a) = a'a''ab''b' = (a' \cdot a'')a(b' \cdot b'') = (a' \otimes b' \cdot a'' \otimes b'') \cdot a$.

Definición 1.3 (Separable)**.** Sea S una R-álgebra conmutativa. Diremos que S es **separable** si es un S^{e}-módulo proyectivo (definición 2.56).

Nota 1.4. Si trabajamos con anillos conmutativos, S^{op} y S coinciden. Por ello nos referiremos a S^{e} como $S \otimes S$ durante el resto del capítulo.

Proposición 1.5. *Sea S una R-álgebra. S es separable si y solo si existe $\sum x_i \otimes y_i \in S \otimes_R S$ tal que $\sum x_i y_i = 1$ y $\sum sx_i \otimes y_i = \sum x_i \otimes y_i s$ para todo $s \in S$.*

Demostración. Probamos ambas implicaciones por separado:

- Suponemos que S es separable. Notamos que $S \otimes S$ es S^{e}-módulo con la acción $a' \otimes b' \cdot a \otimes b := a'a \otimes bb'$. La aplicación $\pi : S \otimes S \to S$ dada por $\pi(a \otimes b) = ab$ es S^{e}-homomorfismo sobreyectivo. Como S es proyectivo, existe $f : S \to S \otimes_R S$ tal que $\pi f = id_S$. Sea $f(1) = \sum x_i \otimes y_i$, notamos que $\sum x_i y_i = \pi\left(\sum x_i \otimes y_i\right) = \pi(f(1)) = 1$. Además, dado $s \in S$,
$$f(s) = \begin{cases} f(s \otimes 1 \cdot 1) = s \otimes 1 \cdot f(1) = \sum sx_i \otimes y_i \\ f(1 \otimes s \cdot 1) = 1 \otimes s \cdot f(1) = \sum x_i \otimes y_i s \end{cases}$$
- Suponemos que existe tal elemento $\sum x_i \otimes y_i \in S \otimes S$. Es claro que la aplicación $f : S \to S \otimes S$ dada por $f(s) = \sum sx_i \otimes y_i$ es homomorfismo de S^{e}-módulos. Como $\pi f = id_S$, concluimos que S es un retracto (definición (2.58)) de $S \otimes S$. Notamos que $S^{\mathrm{e}}(1 \otimes 1) = \{\sum a_i \otimes b_i \cdot 1 \otimes 1 \mid a_i, b_i \in S\} = \{\sum a_i \otimes b_i \mid a_i, b_i \in S\} = S \otimes S$. Por otro lado, $\sum a_i \otimes b_i \cdot 1 \otimes 1 = 0$, que implica que $\sum a_i \otimes b_i = 0$. Concluimos entonces que $\{1 \otimes 1\}$ es S^{e}-base de $S \otimes S$, luego $S \otimes S$ es S^{e}-módulo libre. Esto implica que $S \otimes S$ es S^{e}-módulo proyectivo. Se sigue que S es S^{e}-módulo proyectivo ya que S es retracto de $S \otimes S$.

□

Lema 1.6. *Sean S una R-álgebra conmutativa y separable, y $f : S \to R$ un homomorfismo de R-álgebras. Existe un único idempotente e en S tal que $f(e) = 1$ y $se = f(s)e$, para todo $s \in S$. Es más, si $f_1, \ldots, f_n$ son homomorfismos de R-álgebras de S a R fuertemente distintos dos a dos, entonces los correspondientes idempotentes $e_1, \ldots, e_n$ son ortogonales dos a dos y $f_i(e_j) = \delta_{i,j}$.*

Demostración. Por la proposición 1.5, la separabilidad de S es equivalente a la existencia de elementos $x_i, y_i \in S$ con $i = 1, \ldots, m$ tales que:

$$\text{(a)} \sum_{i=1}^{m} x_i y_i = 1, \qquad \text{(b)} \sum_{i=1}^{m} sx_i \otimes y_i = \sum_{i=1}^{m} x_i \otimes y_i s, \quad \text{para todo } s \in S.$$

Sea $e = \sum_{i=1}^{m} f(x_i)y_i$, $f(e) = f\left(\sum f(x_i)y_i\right) = \sum f(x_i)f(y_i) = f\left(\sum x_i y_i\right) = f(1_S) = 1_R$. Esto implica que $f(e) = 1$. Si aplicamos $f \otimes 1$ a la igualdad en (b) se concluye que, para $s \in S$, $f(s)\left(\sum f(x_i) \otimes y_i\right) = \sum f(s)f(x_i) \otimes y_i = \sum f(x_i) \otimes y_i s = \left(\sum f(x_i) \otimes y_i\right) s$. De aquí obtenemos que, si $\pi(a \otimes b) = ab$,

$$f(s)e = f(s)\pi\left(\sum f(x_i) \otimes y_i\right) = \pi\left(\sum f(x_i) \otimes y_i\right) s = es = se, \tag{1.1}$$

y se sigue que $f(s)e = se$ para todo $s \in S$. Si tomamos $s = e$ en la igualdad (1.1) se tiene que $e = 1e = f(e)e = ee = e^2$, luego e es un idempotente. Sea e' otro idempotente que cumple $f(e') = 1$ y la igualdad (1.1). Entonces $e' = f(e)e' = ee' = e'e = f(e')e = e$ implica que este idempotente e es único. Para la segunda parte del lema, notamos que cada $f_i(e_j)$ es idempotente de R ya que $(f_i(e_j))^2 = f_i(e_j)f_i(e_j) = f_i(e_j^2) = f_i(e_j)$, y se tiene así que $f_i(s)f_i(e_j) = f_i(se_j) = f_i(f_j(s)e_j) = f_j(s)f_i(e_j)$. Como f_i y f_j son fuertemente distintos (para $i \neq j$) existe $s \in S$ tal que $f_i(s)e \neq f_j(s)e$ para todo $e \in R$ idempotente no nulo. Concluimos que $f_i(e_j) = 0$ para $i \neq j$. Como $f_i(e_i) = 1$ entonces $f_i(e_j) = \delta_{i,j}$. Por último, para $i \neq j$ se tiene que $e_ie_j = f_j(e_i)e_j = 0 \cdot e_j = 0$, luego los $e_1, \ldots, e_n$ son ortogonales dos a dos. □

1.1.3. Algunas álgebras y aplicaciones importantes

En lo que resta de capítulo supondremos de forma general que S es un anillo conmutativo y G un subgrupo finito de $\mathrm{Aut}(S)$. Como ya se ha mencionado, al subanillo de S formado por los elementos fijados por todo $\sigma \in G$ lo denotaremos por $R = S^G$.

Definición de D

Consideraremos el **producto cruzado trivial de S con G**, que denotaremos por D. D es un S-módulo libre (definición 2.55) con base u_σ ($\sigma \in G$) (escribimos u_σ en lugar de σ a pesar de ser «lo mismo» para diferenciar si nos referimos a un elemento de G o de D). Es decir,

$$\boxed{D = \bigoplus_{\sigma \in G} Su_\sigma}$$

con la acción de S en D dada por

$$\begin{array}{rcl} S \times D & \longrightarrow & D \\ (s, \sum_i s_i u_{\sigma_i}) & \longmapsto & \sum_i (ss_i)u_{\sigma_i} \end{array} . \tag{1.2}$$

Definimos el producto en D mediante

$$(su_\sigma)(tu_\tau) \;=\; s\sigma(t)u_{\sigma\tau}.$$

Notamos que esta construcción es similar al álgebra grupo $S[G]$ pero con la diferencia de que los elementos de S ya no se mueven libremente por la expresión, sino que hay una «penalización» por «pasar a través» de un elemento de G (que aplica la acción de G en S es decir, $u_\sigma s = \sigma(s)u_\sigma$ en D). Veamos que con esta multiplicación D tiene estructura de R-álgebra. La operación es bilineal porque para cualesquiera $r \in R$ y $d, d' \in D$ se cumple que $r(dd') = d(rd') = (rd)d'$, ya que $R = S^G$. El resto de condiciones de la bilinealidad son ciertas por definición. Esta multiplicación es asociativa, pues dados $s, t, w \in S$, $\sigma, \tau, \omega \in G$:

$$\begin{aligned} (su_\sigma tu_\tau)wu_\omega &= (s\sigma(t)u_{\sigma\tau})wu_\omega = s\sigma(t)\sigma(\tau(w))u_{\sigma\tau\omega} = s\sigma(t\tau(w))u_{\sigma\tau\omega} \\ &= (su_\sigma)(t\tau(w)u_{\tau\omega}) = su_\sigma(tu_\tau wu_\omega). \end{aligned}$$

Por último, $u_1 = 1_D$ es el elemento identidad, pues dado $su_\sigma \in D$, $u_1(su_\sigma) = 1(s)u_{1\sigma} = su_\sigma = s\sigma(1)u_{\sigma 1} = (su_\sigma)u_1$, luego D es una R-álgebra con la multiplicación propuesta.

Definición de j

Consideramos la aplicación

$$\boxed{\begin{array}{rccl} j: & D & \longrightarrow & \mathrm{Hom}_R(S,S) \\ & su_\sigma & \longmapsto & j(su_\sigma)(x) = s\sigma(x) \end{array}}$$

para $s, x \in S$, $\sigma \in G$. Es fácil ver que se trata de un homomorfismo de R-álgebras, así como un homomorfismo de S-módulos, ya que dados $r \in R$, $s, t, x \in S$, $\sigma, \tau \in G$,

$$\begin{aligned} j((su_\sigma)(tu_\tau))(x) &= j(s\sigma(t)u_{\sigma\tau})(x) = s\sigma(t)\sigma(\tau(x)) = s\sigma(t\tau(x)) \\ &= j(su_\sigma)(t\tau(x)) = j(su_\sigma) \circ j(tu_\tau)(x), \end{aligned}$$

$$j(rsu_\sigma)(x) = j((rs)u_\sigma)(x) = (rs)\sigma(x) = rs\sigma(x) = rj(su_\sigma)(x).$$

Definición de E

Consideramos la S-álgebra E formada por todas las aplicaciones de G a S con las operaciones suma y producto punto a punto. Utilizaremos la notación $v_\sigma(\tau) = \delta_{\sigma,\tau}$, con la que resulta evidente que

$$\boxed{E = \bigoplus_{\sigma \in G} S v_\sigma}$$

Adicionalmente notamos como para $\sigma, \tau, \rho \in G$ con $\sigma \neq \tau$ se tiene que $(v_\sigma \cdot v_\tau)(\rho) = \delta_{\sigma,\rho} \cdot \delta_{\tau,\rho} = 0$, luego $v_\sigma v_\tau = 0$. Además $v_\sigma^2(\rho) = \delta_{\sigma,\rho}^2 = \delta_{\sigma,\rho} = v_\sigma(\rho)$ y

$$\sum_{\sigma \in G} v_\sigma(\rho) \;=\; \sum_{\sigma \in G} \delta_{\sigma,\rho} \;=\; \delta_{\rho,\rho} + \sum_{\sigma \in G \setminus \{\rho\}} \delta_{\sigma,\rho} \;=\; 1,$$

con lo que la familia $\{v_\sigma\}_{\sigma \in G}$ es una base de E formada por idempotentes ortogonales dos a dos, tales que la suma de todos es igual a 1.

Definición de h

Como $S \otimes S$ puede ser vista como S-álgebra a través del primer factor se tiene que

$$\boxed{\begin{array}{rccl} h: & S \otimes S & \longrightarrow & E \\ & s \otimes t & \longmapsto & h(s \otimes t)(\sigma) = s\sigma(t) \end{array}}$$

es un homomorfismo de S-álgebras, ya que es aditiva y para $s, s', t, t', x \in S$, $\sigma \in G$ cumple que $h((s \otimes t)(s' \otimes t))(\sigma) = h(ss' \otimes tt')(\sigma) = ss'\sigma(tt') = s\sigma(t)s'\sigma(t') = h(s \otimes t)(\sigma) \cdot h(s' \otimes t')(\sigma)$ y $h(xs \otimes t)(\sigma) = h((xs) \otimes t)(\sigma) = (xs)\sigma(t) = xs\sigma(t) = xh(s \otimes t)(\sigma)$.

1.1.4. Extensiones de Galois

Previo a definir lo que es una extensión de Galois, estudiemos la equivalencia de las distintas condiciones del teorema siguiente, cuya utilidad veremos más adelante. Las hipótesis que aparecen [entre corchetes] son automáticamente ciertas si los únicos idempotentes de S son 0 y 1 y en tal caso pueden omitirse.

Teorema 1.7. *Sea S un anillo conmutativo, G un grupo finito de automorfismos de S, y $R = S^G$. Equivalen:*

(a) S es una R-álgebra separable [y los elementos de G son fuertemente distintos dos a dos].

(b) Existen elementos $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ tales que $\sum_{i=1}^n x_i \sigma(y_i) = \delta_{1,\sigma}$ para todo $\sigma \in G$.

(c) S es un R-módulo proyectivo finitamente generado y j es isomorfismo.

(d) Sea M un D-módulo a izquierda, que se puede ver también como G-módulo a izquierda mediante $\sigma(m) := u_\sigma(m)$. Entonces la aplicación $\omega : S \otimes M^G \to M$ dada por $\omega(s \otimes m) = sm$ es isomorfismo de S-módulos.

(e) $h : S \otimes S \to E$ es isomorfismo de S-álgebras.

(f) Dado $\sigma \in G$ distinto de 1 y un ideal maximal P de S, existe $s = s(P, \sigma) \in S$ tal que $s - \sigma(s) \notin P$.

Demostración. Probaremos las siguientes implicaciones:

- **(a) implica (b):** S es una R-álgebra separable, luego existe $e = \sum_i x_i \otimes y_i \in S \otimes S$ tal que $\sum_i x_i y_i = 1$ y $se = es$ para todo $s \in S$. Consideramos $e' = \sum_i (1 \otimes x_i) \otimes_{S \otimes 1} (1 \otimes y_i)$. Notamos que $\sum_i (1 \otimes x_i)(1 \otimes y_i) = \sum_i 1 \otimes (x_i y_i) = 1 \otimes 1 = 1_{S \otimes S}$. Además, como $\otimes_{S \otimes 1}$ es equilibrado respecto de $S \otimes 1$, para $s \otimes 1 \in S \otimes 1$ se tiene que

$$(s \otimes 1)e' = \sum_i (s \otimes x_i) \otimes_{S \otimes 1} (1 \otimes y_i) = \sum_i (1 \otimes x_i) \otimes_{S \otimes 1} (s \otimes y_i) = e'(s \otimes 1),$$

de donde se sigue que $S \otimes S$ es un $S \otimes 1$-álgebra separable. Notamos ahora que la aplicación $F : S \to S \otimes 1$ dada por $F(s) = s \otimes 1$ verifica que, para $s, s' \in S$,

$$\begin{cases} F(s + s') = (s + s') \otimes 1 = s \otimes 1 + s' \otimes 1 = F(s) + F(s'), \\ F(ss') = (ss') \otimes 1 = (ss') \otimes (1 \cdot 1) = (s \otimes 1)(s' \otimes 1) = F(s)F(s'), \\ F(1) = 1 \otimes 1 = 1_{S \otimes S}. \end{cases}$$

Así F es un homomorfismo de anillos y por tanto $S \otimes S$ es una S-álgebra separable. Definimos para cada $\sigma \in G$ la aplicación $f_\sigma : S \otimes S \to S$ dada por $s \otimes t \mapsto s\sigma(t)$. Para $\sigma \in G$; $r, s, s', t, t' \in S$ se verifica que

$$\begin{aligned} &f_\sigma((s \otimes t)(s' \otimes t')) = f_\sigma((ss') \otimes (tt')) = ss'\sigma(tt') = f_\sigma(s \otimes t) f_\sigma(s' \otimes t'), \\ &f_\sigma(rs \otimes t) = f_\sigma((rs) \otimes t) = (rs)\sigma(t) = r(s\sigma(t)) = r f_\sigma(s \otimes t), \end{aligned}$$

y como cada f_σ es aditiva por definición, concluimos que son homomorfismos de S-álgebras. Además, como los elementos de G son fuertemente distintos dos a dos, así lo es también cada f_σ. Aplicando el lema 1.6, existe un idempotente $e \in S \otimes S$ tal que $f_\sigma(e) = \delta_{1,\sigma}$ para cualquier $\sigma \in G$. Entonces los $x_1, \ldots, x_n, y_1, \ldots, y_n$ son justo los que forman este idempotente $e = \sum_{i=1}^n x_i \otimes y_i$, ya que:

$$\sum_{i=1}^n x_i \sigma(y_i) = f_\sigma \left(\sum_{i=1}^n x_i \otimes y_i \right) = f_\sigma(e) = \delta_{1,\sigma}.$$

- **(b) implica (c):** Definimos la traza de $s \in S$ como $\mathrm{tr}(s) = \sum_{\sigma \in G} \sigma(s)$. Dado $\tau \in G$,

$$\tau(\mathrm{tr}(s)) = \tau\left(\sum_{\sigma \in G} \sigma(s)\right) = \sum_{\sigma \in G} \tau(\sigma(s)) = \sum_{\sigma \in G} \sigma(s) = \mathrm{tr}(s),$$

luego $\mathrm{tr}(s)$ queda fijo por cualquier elemento de G y en consecuencia $\mathrm{tr}(S) \subseteq R$. Sean $\varphi_1, \ldots, \varphi_n$ las funciones en S dadas por $\varphi_i(s) = \mathrm{tr}(sy_i)$. Para $s, s' \in S$, $r \in R$,

$$\mathrm{tr}(s + s') = \sum_{\sigma \in G} \sigma(s + s') = \sum_{\sigma \in G} \sigma(s) + \sum_{\sigma \in G} \sigma(s') = \mathrm{tr}(s) + \mathrm{tr}(s')$$
$$\mathrm{tr}(rs) = \sum_{\sigma \in G} \sigma(rs) = \sum_{\sigma \in G} \sigma(r)\sigma(s) = r \sum_{\sigma \in G} \sigma(s) = r \cdot \mathrm{tr}(s)$$

luego $\mathrm{tr}(\cdot) \in \mathrm{Hom}_R(S, R)$, y así $\varphi_i \in \mathrm{Hom}_R(S, R)$ para cada $i = 1, \ldots, n$. Se sigue que

$$\sum_{i=1}^{n} \varphi_i(s)x_i = \sum_{i=1}^{n} \left(\sum_{\sigma \in G} \sigma(sy_i)x_i\right) = \sum_{\sigma \in G} \sigma(s) \left(\sum_{i=1}^{n} x_i \sigma(y_i)\right) = \sum_{\sigma \in G} \sigma(s)\delta_{1,\sigma} = s \cdot 1 = s,$$

es decir, $s = \sum_i \varphi_i(s)x_i$ para todo $s \in S$. Usemos esto para probar que S es R-módulo proyectivo finitamente generado:

- Sea $\Psi : F \to S$ un homomorfismo de un R-módulo libre de base $\{e_\alpha\}$ en S, y sea $S_\alpha = \Psi(e_\alpha)$. Por [2, VII, 3.1] sabemos que para que S sea proyectivo es necesario y suficiente que exista un homomorfismo $\varphi : S \to F$ tal que $\Psi\varphi = id_S$. Si escribimos $\varphi(s) = \sum_\alpha (\varphi_\alpha(s))e_\alpha$ obtenemos homomorfismos $\varphi_\alpha : S \to R$ tales que para todo $s \in S$, $\varphi_\alpha(s) = 0$ para todo α excepto una cantidad finita de ellos. La condición $\Psi\varphi = id_S$ es equivalente a

$$\Psi\left(\sum_\alpha \varphi_\alpha(s)e_\alpha\right) = \sum_\alpha \varphi_\alpha(s)s_\alpha = s = \Psi(\varphi(s)), \quad \text{para todo } s \in S.$$

Como $s = \sum_i \varphi_i(s)x_i$ para todo $s \in S$ y dado que la familia de índices es finita, podemos aplicar este resultado en nuestro caso, probando que S es un R-módulo proyectivo finitamente generado. Probemos ahora que $j : D \to \mathrm{Hom}_R(S, S)$ es isomorfismo:

- **Sobreyectividad**: Dado un elemento $u \in \mathrm{Hom}_R(S, S)$,

$$j\left(\sum_{\sigma \in G} \sum_{i=1}^{n} u(x_i)\sigma(y_i)u_\sigma\right)(x) = \sum_\sigma \sum_i j\left(u(x_i)\sigma(y_i)u_\sigma\right)(x) = \sum_\sigma \sum_i u(x_i)\sigma(y_i)\sigma(x)$$
$$= \sum_i u(x_i)\,\mathrm{tr}(xy_i) = u\left(\sum_i x_i\varphi_i(x)\right) = u(x),$$

  luego todo elemento de $\mathrm{Hom}_R(S, S)$ tiene preimagen por j.
- **Inyectividad**: Dado un elemento $\tau \in G$,

$$\tau^{-1}\left(\sum_i \tau(x_i)\sigma(y_i)\right) = \sum_i x_i\tau^{-1}(\sigma(y_i)) = \delta_{1,\tau^{-1}\circ\sigma} = \delta_{\sigma,\tau}.$$

  Como τ es homomorfismo de anillos, $\tau(1_S) = 1_S$ y $\tau(0_S) = 0_S$, luego $\tau(\delta_{\sigma,\tau}) = \delta_{\sigma,\tau}$ y se sigue que $\sum_{i=1}^{n} \tau(x_i)\sigma(y_i) = \delta_{\sigma,\tau}$. Dado $v = \sum_\tau s_\tau u_\tau \in D$,

$$\sum_\sigma \sum_i \left(j(v)(x_i)\right)\sigma(y_i)u_\sigma = \sum_{\sigma,\tau,i} s_\tau\tau(x_i)\sigma(y_i)u_\sigma = \sum_\tau \left(s_\tau \sum_\sigma \left(u_\sigma \sum_i \tau(x_i)\sigma(y_i)\right)\right)$$
$$= \sum_\tau \left(s_\tau \sum_\sigma u_\sigma\delta_{\sigma,\tau}\right) = \sum_\tau s_\tau u_\tau = v,$$

luego $v \neq w$ implica que $j(v) \neq j(w)$.

- **(c) implica (d):** Como S es un R-módulo proyectivo finitamente generado, repetimos el mismo argumento de [(b) implica (c)] y concluimos que para $i = 1, \ldots, n$ existen $x_i \in S$, $\varphi_i \in \mathrm{Hom}_R(S, R)$ tales que $s = \sum_{i=1}^{n} \varphi_i(s)x_i$, para todo $s \in S$. Como j es isomorfismo, cada φ_i tiene preimagen por j (ya que $\mathrm{Hom}_R(S, R) \subseteq \mathrm{Hom}_R(S, S)$). Es decir, existe $d_i \in D$ tal que $j(d_i) = \varphi_i$ para cada $i = 1, \ldots, n$. Notamos que

$$j\left(\sum_{i=1}^{n} x_i d_i\right)(s) = \sum_i x_i j(d_i)(s) = \sum_i x_i \varphi_i(s) = s,$$

luego $j(\sum_i x_i d_i)(s) = (s)$, y como j es isomorfismo y $j(1_D) = id_S$ se tiene que $\sum_i x_i d_i = 1_D$. Además, como $\varphi_i(s) \in R$ para todo $s \in S$, $j(u_\sigma d_i)(s) = j(u_\sigma)j(d_i)(s) = \sigma\varphi_i(s) = \sigma(\varphi_i(s)) = \varphi_i(s) = j(d_i)(s)$, y se sigue que $u_\sigma d_i = d_i$. En consecuencia $d_i m \in M^G$ para todo $m \in M$, $i = 1, \ldots, n$, ya que (como M es un D-módulo) $\sigma(d_i m) = u_\sigma(d_i m) = (u_\sigma d_i)(m) = d_i m$. También podemos considerar M como un S-módulo porque $S \subseteq D$. De este modo vemos que para $s \in S$, $d \in D$, $m_0 \in M^G$:

$$\begin{aligned} d(sm_0) &= \left(\sum_{\sigma \in G} s_\sigma u_\sigma\right)(sm_0) = \sum_\sigma (s_\sigma u_\sigma(sm_0)) = \sum_\sigma (s_\sigma u_\sigma(s) m_0) \\ &= \left(\sum_\sigma (s_\sigma u_\sigma)(s)\right) m_0 = (j(d)(s))\, m_0. \end{aligned}$$

Definimos la aplicación $\gamma : M \to S \otimes M^G$ dada por $m \mapsto \sum_i x_i \otimes d_i m$. Notamos que γ está bien definida ya que antes probamos que $d_i m \in M^G$. Dado $m \in M$,

$$\omega(\gamma(m)) = \omega\left(\sum_i x_i \otimes d_i m\right) = \sum_i x_i d_i m = 1_D m = m,$$

y concluimos que $\omega\gamma = id_M$. Sean $s \in S$, $m_0 \in M^G$,

$$\begin{aligned} \gamma(\omega(s \otimes m_0)) = \gamma(sm_0) &= \sum_{i=1}^{n} x_i \otimes d_i(sm_0) = \sum_i x_i \otimes \varphi_i(s) m_0 \\ &= \left(\sum_i x_i \varphi_i(s)\right) \otimes m_0 = s \otimes m_0, \end{aligned}$$

luego $\gamma\omega = id_{S \otimes M^G}$. Como ω es aditiva y para cualesquiera $s, s' \in S$, $m_0 \in M^G$ cumple que $\omega(s'(s \otimes m_0)) = \omega((s's) \otimes m_0) = (s's)m_0 = s'(sm_0) = s'\omega(s \otimes m_0)$, tenemos que ω es un homomorfismo de S-módulos. Como existe $\gamma : M \to S \otimes M^G$ tal que $\omega\gamma = id = \gamma\omega$ se sigue que ω es además biyección, luego ω es un isomorfismo de S-módulos.

- **(d) implica (e):** Consideramos la acción de G en E dada por $\sigma v(\tau) = \sigma(v(\sigma^{-1}\tau))$. Si $s \in S$ y $\tau \in G$ se tiene que $\sigma(sv)(\tau) = \sigma(sv(\sigma^{-1}\tau)) = \sigma(s)\sigma(v)$, así que podemos ver E como un D-módulo mediante la fórmula

$$(su_\sigma)(v) \;=\; s\sigma v \tag{1.3}$$

Que v pertenezca a E^G significa que para todo $\sigma, \tau \in G$, $\sigma v(\tau) = \sigma(v(\sigma^{-1}\tau)) = v(\tau)$. Dicho de otra forma, que $\sigma(v(\tau)) = v(\sigma\tau)$, para todo $\sigma, \tau \in G$. Así es claro que E^G está formado por los G-homomorfismos de G a S. Notamos que E^G es un R-módulo, combinando la fórmula (1.3) con que $\sigma(r) = r$ para cualesquiera $r \in R$, $\sigma \in G$. Así la aplicación $\theta : S \to E^G$ dada por $\theta(s)(\sigma) = \sigma(s)$ es claramente un homomorfismo de R-módulos. Veamos que además es isomorfismo:

- **Sobreyectividad**: Sea $f : G \to S \in E^G$. Si consideramos $s = f(1_G)$, $\theta(s)(\sigma) = \sigma(s) = \sigma(f(1)) = \sigma(f(\sigma^{-1}\sigma)) = (\sigma f)(\sigma) = f(\sigma)$, luego $\theta(s) = f$ y queda probado que θ es sobreyectiva.
- **Inyectividad**: Como $G \leq \mathrm{Aut}(S)$, $s \neq t$ implica $\sigma(s) \neq \sigma(t)$ para cualquier $\sigma \in G$. En consecuencia si $s \neq t$ entonces $\theta(s) \neq \theta(t)$, luego θ es inyectiva.

Queda probado que $\theta : S \to E^G$ es un isomorfismo de R-módulos. Se sigue que la composición $\omega(1 \otimes \theta) : S \otimes S \to E$ es un isomorfismo de S-módulos. Dados $s, t \in S$, $\sigma \in G$, notamos que $\omega\left((1 \otimes \theta)(s \otimes t)\right)(\sigma) = \omega\left(s \otimes \theta(t)\right)(\sigma) = s\sigma(t) = h(s \otimes t)$, luego h es un isomorfismo de S-álgebras.

- **(e) implica (a):** Sea $v_1(\sigma) = \delta_{1,\sigma} \in E$. $v_1^2(\sigma) = \delta_{1,\sigma}$, implica que v_1 es idempotente de E, luego Ev_1 es un E-módulo proyectivo. Notamos que $Ev_1 = Sv_1$, luego Sv_1 es también E-módulo proyectivo. Como $h : S \otimes S \to E$ es isomorfismo se sigue que Sv_1 es un $S \otimes S$-módulo proyectivo. Dados $s \in S$, $\sigma \in G$,

$$\begin{cases} h(s \otimes 1)v_1(\sigma) = s\sigma(1)\delta_{1,\sigma} = s\delta_{1,\sigma} = \begin{cases} s, & \text{si } \sigma = 1 \\ 0, & \text{si } \sigma \neq 1 \end{cases} \\ \\ h(1 \otimes s)v_1(\sigma) = 1 \cdot \sigma(s)\delta_{1,\sigma} = \sigma(s)\delta_{1,\sigma} = \begin{cases} \sigma(s) = s, & \text{si } \sigma = 1 \\ 0, & \text{si } \sigma \neq 1 \end{cases} \end{cases}$$

luego $h(1 \otimes s)v_1 = h(s \otimes 1)v_1$ y así $Sv_1 \cong S$ como $S \otimes S$-módulos. Queda así probado que S es un $S \otimes S$-módulo proyectivo, es decir, una R-álgebra separable. Como h es un isomorfismo podemos tomar $h^{-1} = \sum_{i=1}^n x_i \otimes y_i$. Observamos que

$$h\left(\sum_{i=1}^n x_i \otimes y_i\right)(\sigma) = x_i\sigma(y_i) = v_1 = \delta_{1,\sigma}, \quad \text{para todo } \sigma \in G.$$

Estos x_i, y_i verifican la propiedad del inciso (b). Sea e un idempotente de S tal que $\sigma(s)e = \tau(s)e$ para ciertos $\sigma, \tau \in G$ diferentes y para todo $s \in S$, observamos que $e = \sum x_i y_i e = \sum x_i \tau^{-1}\sigma(y_i)e = 0 \cdot e = 0$. Concluimos así que los elementos de G son fuertemente distintos.

- **(b) implica (f):** Supongamos que para algunos $1 \neq \sigma \in G$ e ideal maximal P de S no exista $s \in S$ tal que $s - \sigma(s) \notin P$. Esto equivale a $S - \sigma(S) = (1 - \sigma)S \subseteq P$. En particular $(1 - \sigma)y_i \in P$ para cada i. Como P es ideal se tiene que además

$$\sum_{i=1}^n x_i(1 - \sigma)y_i = \sum_{i=1}^n x_i(y_i - \sigma(y_i)) \in P.$$

Sin embargo, $\sum_i x_i(y_i - \sigma(y_i)) = \sum_i x_i y_i - \sum_i x_i\sigma(y_i) = 1 \in P$, lo que implica que $P = S$. Esto es absurdo ya que P era maximal. Queda así probado que existe $s \in S$ tal que $s - \sigma(s) \notin P$.

- **(f) implica (a):** Sea $1 \neq \sigma \in G$. Por hipótesis existe $s \in S$ tal que $s - \sigma(s) \notin P$ para cada ideal maximal P de S. Esto implica que el ideal $I \subseteq S$ generado por los elementos de la forma $s - \sigma(s)$ no está contenido en ningún ideal maximal (ya que en un anillo conmutativo unitario todo ideal propio está contenido en algún ideal maximal). De esto concluimos que I no puede ser otro que el propio S. Entonces $1 \in I$ y por lo tanto

existen $a_1, \ldots, a_r, b_1, \ldots, b_r \in S$ tales que $\sum_{j=1}^{r} a_j(b_j - \sigma(b_j)) = 1$. Definimos además $a_{r+1} = -\sum_{j=1}^{r} a_j\sigma(b_j)$ y $b_{r+1} = 1$. Notamos que

$$\sum_{j=1}^{r+1} a_j b_j = \sum_{j=1}^{r+1} a_j(b_j - \sigma(b_j)) = 1,$$
$$\sum_{j=1}^{r+1} a_j\sigma(b_j) = \sum_{j=1}^{r} a_j(\sigma(b_j) - \sigma(b_j)) = \sum_{j=1}^{r} a_j \cdot 0 = 0.$$

Consideramos las distintas familias $\{a_{i,\sigma}\}$, $\{b_{i,\sigma}\}$ definidas como arriba para cada $\sigma \in G$ no trivial. Los elementos $x_1, \ldots, x_n, y_1, \ldots, y_n$ que cumplen (b) son el resultado por multiplicar respectivamente los a_j, b_j construidos para cada $\sigma \in G$ no trivial.

□

La utilidad de estas equivalencias se ve en la definición de extensión de Galois para anillos conmutativos que damos a continuación.

Definición 1.8 (Extensión de Galois)**.** Sea G un grupo finito de automorfismos de un anillo conmutativo S, y sea $R = S^G$. Diremos que S es una **extensión de Galois** de R con grupo de Galois G si se verifica cualquiera (luego todas) de las propiedades del teorema 1.7.

Nota 1.9. Para el caso particular en que S es un cuerpo, el único ideal maximal es $\{0\}$. Como $1 \neq \sigma$ existe $s \in S$ tal que $s \neq \sigma(s)$. Esto equivale a que $s - \sigma(s) \notin \{0\}$ y así la condición (f) del teorema 1.7 se cumple automáticamente. Así la definición de extensión de Galois coincide con la usual. Es más, (a) y (c) indican que S es una extensión separable finita de R de dimensión igual al orden del grupo de Galois.

Lema 1.10. *Sea S una extensión de Galois de R con grupo de Galois G. Entonces existe $c \in S$ tal que $\mathrm{tr}(c) = 1$, y R es un R-módulo sumando directo de S.*

Demostración. Ya hemos visto en la demostración del teorema 1.7 que $\mathrm{tr}(\cdot) \in \mathrm{Hom}_R(S, R)$, y se sigue que $\mathrm{tr}(S)$ es un ideal de R. Sean elementos $x_1, \ldots, x_n, y_1, \ldots, y_n \in S$ tales que verifican la propiedad (b) del teorema 1.7,

$$\sum_{i=1}^{n} x_i \,\mathrm{tr}(y_i) = \sum_{i=1}^{n} x_i \sum_{\sigma\in G} \sigma(y_i) = \sum_{i=1}^{n} \left(\sum_{\sigma\in G} x_i\sigma(y_i) \right) = \sum_{\sigma\in G} \left(\sum_{i=1}^{n} x_i\sigma(y_i) \right) = \sum_{\sigma\in G} \delta_{1,\sigma} = 1,$$

Con esto concluimos que el ideal de S generado por $\mathrm{tr}(S)$ es el mismo S. La propiedad (c) del teorema 1.7 nos dice que S es un R-módulo finitamente generado. Aplicamos [9, lema 8.4] (lema de Nakayama) y se tiene que $\mathrm{tr}(S) = R$, lo que establece la existencia de $c \in S$ tal que $\mathrm{tr}(c) = 1$. Queda así claro que R es un R-módulo sumando directo de S, con complemento el núcleo de la aplicación $s \mapsto \mathrm{tr}(cs)$ (en otras palabras, si denotamos φ a la aplicación $s \mapsto \mathrm{tr}(cs)$, entonces $S = R \oplus \ker\varphi$). □

Lema 1.11. *Sea S una extensión de Galois de R con grupo de Galois G. Sea A cualquier R-álgebra conmutativa. G actúa en $A \otimes S$ por la fórmula $\sigma(a \otimes s) = a \otimes \sigma(s)$ para $s \in S$, $\sigma \in G$, $a \in A$ y $A \otimes S$ es extensión de Galois de A con grupo de Galois G.*

Demostración. Como por el lema 1.10 se tiene que R es sumando directo de S, $A \otimes_R S$ es una extensión de $A \otimes_R R \cong A$, identificando $A \otimes 1$ y A por medio de su isomorfismo $(a \otimes 1 \mapsto a)$. Sean los $x_1, \ldots, x_n, y_1, \ldots, y_n$ que satisfacen la propiedad (b) del teorema 1.7,

$$\begin{aligned}\sum_{i=1}^{n}(1 \otimes x_i)(1 \otimes \sigma(y_i)) &= \sum_{i=1}^{n}(1 \cdot 1) \otimes (x_i\sigma(y_i)) = \sum_{i=1}^{n} 1 \otimes (x_i\sigma(y_i)) \\ &= 1 \otimes \Big(\sum x_i\sigma(y_i)\Big) = 1 \otimes \delta_{1,\sigma} \approx \delta_{1,\sigma},\end{aligned}$$

ya que $1 \otimes 0 = 0_{A\otimes S}$ y $1 \otimes 1 = 1_{A\otimes S}$. Es decir, los términos $1 \otimes x_i$, $1 \otimes y_i$ satisfacen la misma condición (b) del teorema 1.7 pero en $A \otimes S$. Probemos que $(A \otimes S)^G = A$ (por doble contenido):

- Dado $u \in (A \otimes S)^G$, sea $c \in S$ tal que $\mathrm{tr}(c) = 1$. Tenemos que $u = u \cdot 1_A \otimes 1_S = u \cdot (id_A \otimes \mathrm{tr})(1_A \otimes c) = (id_A \otimes \mathrm{tr})(u \cdot 1_A \otimes c) \in A \otimes \mathrm{tr}(S) = A \otimes R$. Se sigue que $u \in A \otimes R$ y así $(A \otimes S)^G \subseteq A \otimes R$.
- Sea $u = \sum a_i \otimes r_i \in A \otimes R$, dado cualquier $\sigma \in G$ $\sigma(u) = \sum a_i \otimes \sigma(r_i) = \sum a_i \otimes r_i = u$, luego $u \in (A \otimes S)^G$ y así $(A \otimes S)^G \supseteq A$.

Queda así probado que $(A \otimes S)^G = A \otimes R \approx A$, lo que completa la prueba. □

1.2. El teorema fundamental generalizado

El objetivo de esta sección es alcanzar el teorema fundamental de la teoría de Galois generalizado a anillos conmutativos, que relaciona los subgrupos de G con R-subálgebras de S.

1.2.1. Subálgebras fuertes

La noción de *subálgebra fuerte* es el «precio a pagar» por esta generalización. Más adelante veremos que la correspondencia de Galois no incluirá todas las subálgebras de la extensión, sino tan solo las fuertes.

Definición 1.12 (Subálgebra fuerte)**.** Sea S una extensión de Galois de R con grupo de Galois G, y sea T un subanillo de S. T se dice **G-fuerte** si las restricciones a T de dos elementos cualesquiera de G son o bien iguales o bien fuertemente distintas.

Nota 1.13. Si los únicos idempotentes de S son 0 y 1, toda subálgebra es fuerte. Los teoremas de esta sección tienen [entre corchetes] las hipótesis que pueden ser omitidas en este caso.

1.2.2. El teorema fundamental

Dividiremos el contenido del teorema fundamental en dos subteoremas (1.14 y 1.15) que demostramos por separado. El teorema fundamental será una combinación de sus resultados.

Teorema 1.14. *Sean S una extensión de Galois de R con grupo de Galois G, H un subgrupo de G y $T = S^H$. Entonces T es una R-álgebra separable y G-fuerte, S es una extensión de Galois de T con grupo de Galois H, y H es el conjunto de todos los elementos de G que fijan todos los puntos de T. Si H es un subgrupo normal de G, T es además extensión de Galois de R con grupo de Galois G/H.*

Demostración. Probamos cada afirmación por separado:

1. S **es una extensión de Galois de** T **con grupo de Galois** H: Sean $x_i, y_i \in S$ como en (b) del teorema 1.7. Como $H \leq G$, es claro que $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1,\sigma}$ para todo $\sigma \in H$. Entonces por el teorema 1.7 S es extensión de Galois de T con grupo de Galois H.

2. T **es una** R**-álgebra separable**: Por el apartado (c) del teorema 1.7, S es un T-módulo proyectivo finitamente generado. Se sigue que $S \otimes S$ es $T \otimes T$-módulo proyectivo [2]. Pero por el apartado (a) del teorema 1.7 S es una R-álgebra separable, es decir, que es un $S \otimes S$-módulo proyectivo. Así concluimos que S es $T \otimes T$-módulo proyectivo. Aplicando el lema 1.10, T es un T-módulo sumando directo de S, luego T es además $T \otimes T$-módulo sumando directo de S. Así T es un $T \otimes T$-módulo proyectivo (R-álgebra separable).

3. H **es el conjunto de elementos de** G **que fijan cada** $t \in T$: Sea H' el conjunto de elementos de G que fija todo $t \in T$. Es claro que H' es un subgrupo de G tal que $H \subseteq H'$, y $S^{H'} = S^H = T$. Sean n, n' los órdenes de H, H' respectivamente. Tenemos que S es extensión de Galois de T con grupo asociado H, pero también con H'. Como $E = \bigoplus_\sigma S v_\sigma$ y h es isomorfismo (apartado (e) del teorema 1.7), entonces $S \otimes_T S$ es S-módulo libre, de rango n, y también de rango n'. Veamos que cualesquiera dos bases de un R-módulo libre a izquierda M con R conmutativo comparten cardinal:

   - Sean $\{e_i\}_{i \in I}$ una base de M y A un ideal de R. Notamos que AM está generado por productos rx con $r \in A$, $x \in M$, cuyas coordenadas están en A. Por otro lado, si $x_i \in A$ para todo $i \in I$ entonces $\sum_i x_i e_i \in AM$. De esto se sigue que $x = \sum_i x_i e_i \in AM$ si y solo si $x_i \in A$ para todo $i \in I$. Como A es ideal de R, M/AM es un R/A-módulo con la multiplicación $(r + A)(x + AM) = rx + AM$. Notamos que:
     - Todo elemento de M/AM es combinación lineal de elementos $e_i + AM$ con $I \in I$.
     - Si $\sum_i (r_i + A)(e_i + AM) = 0$, entonces $\sum_i r_i e_i \in AM$. Por lo visto antes esto equivale a que $r_i \in A$ para cada i, luego $(r_i + A) = 0$ para todo $i \in I$.

     Queda así claro que $\{e_i + AM\}_{i \in I}$ es base de M/AM. Si tomamos el caso particular de A maximal, R/A es cuerpo. Así M/AM es un espacio vectorial sobre R/A, luego todas sus bases comparten cardinal (el de I). Lo mismo se sigue para M sobre R.

   Visto esto queda probado que $n = n'$. Como $H \subseteq H'$, concluimos que $H = H'$.

4. T **es** G**-fuerte**: El lema 1.10 asegura la existencia de $c \in S$ tal que $\mathrm{tr}(c) = 1$ con la traza $\mathrm{tr}(s) = \sum_{\rho \in H} \rho(s)$. Sean $x_i, y_i \in S$ como en (b) del teorema 1.7 para S y G. Consideramos

$$x_i' = \sum_{\rho \in H} \rho(x_i c), \quad y_i' = \sum_{\rho \in H} \rho(y_i), \quad \text{con } i = 1, \ldots, n. \tag{1.4}$$

   Como la traza de un elemento de S respecto de un grupo G está en S^G, tenemos que $x_i', y_i' \in S^H = T$ para cada i. Dado $\sigma \in G$,

$$\begin{aligned} \sum_{i=1}^{n} x_i' \sigma(y_i') &= \sum_{i=1}^{n} \left(\sum_{\rho \in H} \rho(x_i c) \cdot \sigma \left(\sum_{\tau \in H} \tau(y_i) \right) \right) = \sum_{\rho \in H} \sum_{\tau \in H} \sum_{i=1}^{n} \rho(c) \rho(x_i \cdot \rho^{-1} \sigma \tau(y_i)) \\ &= \sum_{\rho \in H} \rho(c) \rho \left(\sum_{\tau \in H} \sum_{i=1}^{n} x_i \rho^{-1} \sigma \tau(y_i) \right) = \sum_{\rho \in H} \rho(c) \rho \left(\sum_{\tau \in H} \delta_{1, \rho^{-1} \sigma \tau} \right). \end{aligned}$$

Si $\sigma \in H$, existe $\tau \in H$ tal que $\tau = \sigma^{-1}\rho$. Así $\rho\sigma\tau = 1$ y $\sum_{i=1}^{n} x_i'\sigma(y_i') = \mathrm{tr}(c) = 1$. Por otro lado, si $\sigma \notin H$ se tiene que $\delta_{1,\rho^{-1}\sigma\tau} = 0$, $\forall \tau \in H$. Queda así probado que

$$\sum_{i=1}^{n} x_i'\sigma(y_i') = \begin{cases} 1, & \text{si } \sigma \in H \\ 0, & \text{si } \sigma \notin H \end{cases}$$

Sean $\sigma, \tau \in G$ tales que $\sigma|_T \neq \tau|_T$. Se sigue que $\tau\sigma^{-1} \notin H$ y que $\tau\sigma^{-1}|_T \neq id_T$. Dado un idempotente $e \in S$ con $\sigma(t)e = \tau(t)e$ para todo $t \in T$,

$$e = \sum_{i=1}^{n} x_i'y_i' \cdot e = \sum_{i=1}^{n} x_i'\tau^{-1}\sigma(y_i') \cdot e = 0 \cdot e = 0,$$

luego τ y σ son fuertemente distintas y queda probado que $T = S^H$ es G-fuerte.

5. **Si $H \trianglelefteq G$, T es extensión de Galois de R con grupo G/H**: Supongamos que $H \trianglelefteq G$. Entonces G/H actúa sobre $T = S^H$ mediante $\sigma H(t) = \sigma(t)$ (entendemos $\sigma(t)$ como clase de equivalencia), ya que $\rho(t) = t$ para todo $\rho \in H$. Así $T^{G/H} = S^G = R$ (hipótesis del teorema 1.7). Los $x_i', y_i' \in T$ definidos en (1.4) verifican la condición (b) del teorema 1.7 para T (como R-álgebra) con grupo asociado G/H. Si φ es la acción de G/H en T, $\ker\varphi = \{\sigma H \in G/H \mid \sigma H(t) = t,\ \forall t \in T\} = 1H$, luego la acción es fiel. Así T es extensión de Galois de R con grupo de Galois G/H.

□

Teorema 1.15. *Sea S extensión de Galois de R con grupo de Galois G, y sea T cualquier R-subálgebra separable de S [que sea G-fuerte]. Sea H el subgrupo de G de todos los elementos que fijan todo punto de T. Entonces $T = S^H$.*

Demostración. Por la definición de H es trivial que $T \subseteq S^H$, por lo que basta con probar el contenido $S^H \subseteq T$. Tomando $A = S$ en el lema 1.11, $S \otimes S$ es una extensión de Galois de S con grupo de Galois G, donde S y G operan sobre el primer y segundo factor de $S \otimes S$ respectivamente. Como por el teorema 1.7 h es isomorfismo, h induce una acción de G en E dada por $(\sigma v)(\tau) = v(\tau\sigma)$. Esto nos permite ver E como extensión de Galois de S con grupo asociado G. Por el apartado (c) del teorema 1.7, S es R-módulo proyectivo. Podemos tratar de identificar $S \otimes T$ en la imagen por h de $S \otimes S$. Veamos que $E^H \subseteq h(S \otimes T)$. Consideremos al grupo G de la forma siguiente:

$$G = \bigcup_{i=1}^{r} \sigma_i H.$$

E^H estará formado por las funciones $f : G \to S$ constantes por cada $\sigma_i H$, es decir, tales que $(\sigma_i\rho_1)f = (\sigma_i\rho_2)f$, para todo $\rho_1, \rho_2 \in H$, $i = 1, \ldots, r$. Definimos la familia de homomorfismos $\{f_i : E \to S\}$ con $f_i(v) = v(\sigma_i)$. Dada la definición de E como S-álgebra (suma y multiplicación punto a punto) es claro que las f_i son además homomorfismos de S-álgebras. Sean $i \neq j$, como H es el grupo de los $\sigma \in G$ que fijan todo punto de T, se tiene que $\sigma_i|_T \neq \sigma_j|_T$. Sea $e \in S$ un idempotente distinto de cero. Como T es G-fuerte, existe $t \in T$ tal que $\sigma_i(t)e \neq \sigma_j(t)e$, o lo que es lo mismo, $f_i(h(1 \otimes t))e \neq f_j(h(1 \otimes t))e$. Concluimos así que las $f_1, \ldots, f_r$ son fuertemente distintas dos a dos como homomorfismos de $S \otimes R$ a S. Tenemos que T es R-separable y que $S \otimes S$ es S-separable (apartado (a) del teorema 1.7 para la extensión de Galois $S \otimes S/S$). Esto implica que $S \otimes T$ es S-separable. Como h es isomorfismo, así lo es $h(S \otimes T)$. Podemos aplicar el lema 1.6 para escoger idempotentes ortogonales dos a dos $w_1, \ldots, w_r \in h(S \otimes T)$ tales que

$$\text{(I)} \quad f_i(x)w_i = xw_i, \quad \text{para todo } x \in h(S \otimes T)$$
$$\text{(II)} \quad w_j(\sigma_i) = f_i(w_j) = \delta_{i,j}, \quad \text{para todo } i, j \leq r$$

Dada $f \in E^H$, existe $s_i \in S$ tal que $f(\sigma_i\rho) = f(\sigma_i) = s_i$ para todo $\rho \in H$, $i \leq r$. Como $f = \sum_{i=1}^{r} s_i w_i$, queda probado que los $w_1, \ldots, w_r$ generan todo E^H. Como E^H es de dimensión r y los w_i son r elementos ortogonales dos a dos, concluimos que son la familia $\{w_1, \ldots, w_r\}$ es base de E^H. Como $w_i \in h(S \otimes T)$ para cada i, se sigue que $E^H \subseteq h(S \otimes T)$. h es isomorfismo así que podemos usar h^{-1} y se obtiene $(S \otimes S)^H \subseteq S \otimes T$. Aplicando $\mathrm{tr} \otimes 1$ a ambos lados de $S \otimes S^H \subseteq (S \otimes S)^H$:

$$(\mathrm{tr} \otimes 1)\left(S \otimes S^H\right) \subseteq (\mathrm{tr} \otimes 1)(S \otimes T) \text{ implica que } S^H \otimes S^H \subseteq S^H \otimes T.$$

Esto implica que $S^H \subseteq T$ y queda así probado que $S^H = T$. □

Combinando los resultados de los teoremas 1.14 y 1.15 podemos enunciar una generalización del teorema fundamental de la teoría de Galois para anillos conmutativos. Las [hipótesis entre corchetes] pueden ser omitidas si los únicos idempotentes de S son 1 y 0 al igual que antes.

Teorema 1.16 (Teorema fundamental de la teoría de Galois generalizado)**.** *Sea S una extensión de Galois de R con grupo de Galois G. Entonces:*

1. *Existe una correspondencia biyectiva entre los subgrupos de G y las R-subálgebras [G-fuertes] de S. Si T es una R-subálgebra separable [G-fuerte] de S, entonces el subgrupo correspondiente es*

$$\mathrm{Fix}(T) = \{\sigma \in G \mid \sigma(t) = t, \quad \textit{para todo } t \in T\}.$$

   Además, si $\sigma \in G$ y T es una R-subálgebra separable [G-fuerte] de S, entonces $\mathrm{Fix}(\sigma(T)) = \sigma T \sigma^{-1}$.

2. *Un subgrupo H de G es normal si y solo si S^H es estable por el producto de elementos de G, en cuyo caso S^H es una extensión de Galois de R con grupo de Galois G/H.*

1.3. Ejemplos

A continuación veremos algunos ejemplos que ilustran las peculiaridades de esta generalización (nuevas nociones de «fuertemente distintas», «G-fuertes», la posibilidad de tener varios grupos de Galois diferentes para una misma extensión de Galois, etc.) Estos ejemplos seguramente son bien conocidos, pero no hemos encontrado ninguna referencia adecuada.

1.3.1. Extensión de anillos conmutativos a partir de una extensión de cuerpos

Realizaremos algunas observaciones antes de desarrollar el ejemplo. El objetivo es obtener una extensión de Galois de anillos de la forma $F \times \cdots \times F/F$ a partir de una extensión de Galois de cuerpos F/K de grado finito.

Proposición 1.17. *Sea F/K una extensión de cuerpos, la aplicación*

$$\begin{array}{rccc} \varphi: & F \otimes_K K[x] & \longrightarrow & F[x] \\ & \sum \lambda_i \otimes p_i(x) & \longmapsto & \sum \lambda_i p_i(x) \end{array}$$

es un isomorfismo de K-álgebras y de F-álgebras.

Demostración. La aplicación $F \times K[x] \to F[x]$ dada por $(\lambda, p(x)) \mapsto \lambda p(x)$ es K-bilineal, luego induce una aplicación K-lineal que es precisamente φ. Es sencillo ver que se trata de un homomorfismo de K-álgebras (y de F-álgebras). Además:

- Dado $f(x) = \sum \lambda_i x^i \in F[x]$ cualquiera, $f(x) = \varphi\left(\sum \lambda_i \otimes x^i\right)$. Así φ es sobreyectiva.
- Como $\otimes_K$ es equilibrado para elementos de K, todo elemento de $F \otimes_K K[x]$ se puede escribir de la forma $\sum \lambda_i \otimes x^i$. Si $\sum \lambda_i \otimes x^i \in \ker\varphi$, entonces $\sum \lambda_i x^i = 0$. Esto implica que $\lambda_i = 0$ para cada i y así $\sum \lambda_i \otimes x^i = \sum 0 \otimes x^i = 0$. Luego $\ker\varphi = \{0\}$ y φ es inyectiva.

□

Proposición 1.18. *Sea F/K una extensión de cuerpos. Dado $q(x) \in K[x]$, la aplicación*

$$\begin{array}{rccc} \overline{\varphi}: & F \otimes_K K[x]/\langle q(x)\rangle & \longrightarrow & F[x]/\langle q(x)\rangle \\ & \sum \lambda_i \otimes \overline{p_i(x)} & \longmapsto & \sum \overline{\lambda_i p_i(x)} \end{array}$$

es un isomorfismo de F-álgebras.

Demostración. La aplicación $F \times K[x]/\langle q(x)\rangle \to F[x]/\langle q(x)\rangle$ dada por $(\lambda, \overline{p(x)}) \mapsto \overline{\lambda p(x)}$ es K-bilineal, luego induce una aplicación lineal que es precisamente $\overline{\varphi}$. Es inmediato comprobar que se trata de un homomorfismo de F-álgebras. La sobreyectividad se prueba igual que en la demostración anterior. Dado $\sum \lambda_i \otimes \overline{x^i} \in \ker\overline{\varphi}$,

$$\overline{\sum \lambda_i x^i} = \overline{0} \text{ implica que } \sum \lambda_i x^i = q(x)p(x) \text{ para algún } p(x) \in F[x].$$

Se tiene entonces que $\sum \lambda_i \otimes x^i = c_0 \otimes \overline{q(x)} + \cdots + c_n \otimes \overline{q(x)x^n} = 0$ y $\overline{\varphi}$ es inyectiva. □

Recordatorio 1.19 (Teorema Chino de los Restos)**.** *Sean R un anillo e $I_1, \ldots, I_k$ ideales de R comaximales dos a dos ($I_i + I_j = R$ para $i \neq j$), y sea $I = \bigcap_i I_i$. Entonces se tiene el isomorfismo:*

$$\begin{array}{rccc} \varphi: & R/I & \longrightarrow & (R/I_1) \times \cdots \times (R/I_k) \\ & x + I & \longmapsto & (x + I_1, \ldots, x + I_k) \end{array}$$

Además, si R es conmutativo, se tiene que $I = \bigcap_i I_i = I_1 I_2 \cdots I_k$.

Corolario 1.20. *Si F/K es una extensión de cuerpos y $q(x) \in K[x]$ tiene todas sus raíces en F, con $q(x) = (x - \lambda_1)^{e_1} \cdots (x - \lambda_n)^{e_n}$, entonces*

$$F \otimes_K K[x]/\langle q(x)\rangle \cong F[x]/\langle q(x)\rangle \cong F[x]/\langle (x-\lambda_1)^{e_1}\rangle \times \cdots \times F[x]/\langle (x-\lambda_n)^{e_n}\rangle$$

como F-álgebras. Si la extensión es de Galois de grado finito, por el teorema de elemento primitivo $F = K(a)$ para cierto $a \in F$. Así, $F \cong K[x]/\langle m_a^K(x)\rangle$. Además $m_a^K(x)$ tiene todas sus raíces $a = a_1, \ldots, a_n$ en F y son simples. En tal caso,

$$F \otimes_K F \cong F \otimes_K K[x]/\langle m_a^K(x)\rangle \cong F[x]/\langle x - a_1\rangle \times \cdots \times F[x]/\langle x - a_n\rangle \cong F \times \cdots \times F.$$

Observación 1.21 (Teorema 1.7 en el caso clásico). Veamos cómo nuestra nueva definición de extensión de Galois equivale a la clásica para cuerpos. Sea F/K una extensión de cuerpos de grado finito tal que $F \otimes_K F \cong F \times \cdots \times F$. Vemos que:

- Dado $a \in F$ no separable, entonces $m_a^K(x)$ es igual a $(x-a)^e p(x)$ en $F[x]$ con $e \geq 2$, $\mathrm{mcd}((x-a)^e, p(x)) = 1$. Esto implica que, por lo visto antes,

$$F \otimes_K K(a) \cong F \otimes_K K[x]/\langle m_a^K(x)\rangle \cong F[x]/\langle (x-a)^e\rangle \times F[x]/\langle p(x)\rangle.$$

  Notamos que $(\overline{x-a}, \overline{0})^e = 0$, luego hay un nilpotente distinto de 0 en $F \otimes_K K(a)$. Esto es absurdo, ya que $F \otimes_K K(a)$ es F-subálgebra de $F \otimes_K F \cong F \times \cdots \times F$, que no posee nilpotentes no nulos. Con esto queda probado que F/K es **separable**.

- Dado $a_1 \in F$, sea $m_{a_1}^K(x) = (x-a_1)\cdots(x-a_r)p(x)$, con $p(x)$ irreducible en $F[x]$. En este caso,

$$F \otimes_K K(a_1) \;\cong\; F \times \cdots \times F \times F[x]/\langle p(x)\rangle,$$

  donde $F[x]/\langle p(x)\rangle$ es cuerpo extensión de F. Como $F \otimes_K F \cong F \times \cdots \times F$ no posee F-subálgebras que sean cuerpos de extensión de F de grado mayor o igual que 2, $p(x)$ es necesariamente constante. Se sigue que la extensión es **normal**.

Lo que acabamos de probar es que:

La extensión finita de cuerpos F/K es de Galois	si y solo si	$F \otimes_K F \cong F \times \cdots \times F$ como $F-$álgebras

¿Cómo se relaciona esto con el teorema 1.7? El álgebra E que aparece en el apartado (e) es en este caso:

$$E = \{f : G \to F\} = \bigoplus_{\sigma \in G} F v_\sigma \cong F \times \cdots \times F, \quad \text{con} \quad v_\sigma(\tau) = \delta_{\sigma,\tau}$$

Lo que este apartado nos dice es que h es un isomorfismo (es decir, $F \otimes_K F \cong E$) si y solo si la extensión es de Galois, que es justo lo que hemos demostrado antes. Así queda comprobado que, para cuerpos, la definición generalizada de extensión de Galois coincide con la clásica.

Ejemplo 1.22 (**La extensión de Galois** $F \otimes_K F/F$)**.** Sea $\mathrm{Aut}_K(F)$ el grupo de automorfismos de la extensión de Galois F/K. Vemos que cada $\sigma \in \mathrm{Aut}_K(F)$ induce un $id_F \otimes \sigma \in \mathrm{Aut}_K(F \otimes_K F)$. Para $a, a', b \in F$, $(id_F \otimes \sigma)(a' \cdot a \otimes b) = a'a \otimes \sigma(b) = a'(id_F \otimes \sigma)(a \otimes b)$, luego $id_F \otimes \sigma$ es un isomorfismo F-lineal. De hecho, es automorfismo de F-álgebras. Es claro que

$$\begin{array}{rccc} \psi: & \mathrm{Aut}_K(F) & \longrightarrow & \mathrm{Aut}_K(F \otimes_K F) \\ & \sigma & \longmapsto & id_F \otimes \sigma \end{array}$$

es un homomorfismo de grupos. $\ker\psi$ está formado por los σ tales que $id_F \otimes \sigma = id_{F \otimes_K F}$. Si $(id_F \otimes \sigma)(1 \otimes a) = 1 \otimes a$, entonces $\sigma(a) = a$ para todo $a \in F$ y concluimos que $\sigma = id_F$. Se sigue que ψ es inyectiva, y es posible identificar $\mathrm{Aut}_K(F)$ con

$$G := \{id_F \otimes \sigma \mid \sigma \in \mathrm{Aut}_K(F)\}. \tag{1.5}$$

Es inmediato que $F \cong F \otimes_K K \subseteq (F \otimes_K F)^G$. Por otro lado, dado $\sum a_i \otimes b_i \in (F \otimes_K F)^G$ (podemos asumir sin pérdida de generalidad que los $a_1, \ldots, a_n$ son K-independientes), se tiene que

$$\sum_{i=1}^n a_i \otimes b_i = \sum_{i=1}^n a_i \otimes \sigma(b_i), \quad \text{para todo } \sigma \in \mathrm{Aut}_K(F).$$

Se sigue de la independencia de $\{a_i\}_{i=1}^n$ que $b_i = \sigma(b_i)$ para todo $\sigma \in \mathrm{Aut}_K(F)$. Queda probado que si F/K es extensión de Galois finita, entonces $F \cong F \otimes_K K = (F \otimes_K F)^G$, para el G

definido en 1.5. Tomamos los $x_i, y_i \in F$ que cumplen el apartado (b) del teorema 1.7 para la extensión F/K, y vemos que

$$\sum_{i=1}^{n}(1\otimes x_i)(id_F\otimes\sigma)(1\otimes y_i) = 1\otimes\sum_{i=1}^{n}x_i\sigma(y_i) = \delta_{id_{F\otimes_K F},id_F\otimes\sigma}, \quad \text{para todo } id_F\otimes\sigma\in G.$$

Entonces por el teorema 1.7 concluimos que $F\otimes_K F/F$ es de Galois.

1.3.2. Estudio de las extensiones de Galois $F\times\cdots\times F/F$

Los siguientes ejemplos están dedicados al estudio en detalle de estas extensiones de Galois, analizando cómo son sus subálgebras y los posibles grupos de Galois asociados, así como los detalles de la correspondencia de Galois.

Ejemplo 1.23. Sea F un cuerpo. Dado $n\in\mathbb{N}$, consideremos el anillo conmutativo

$$S_n = Fe_1\oplus Fe_2\oplus\cdots\oplus Fe_n,$$

donde para cada $i=1,\dots,n$ $e_i=(0,\dots,0,1,0,\dots,0)$, con el 1 en la i-ésima posición y el resto ceros (notemos que los e_i son idempotentes de S_n ortogonales dos a dos). Comencemos realizando un estudio de los idempotentes, subálgebras y automorfismos del anillo S_n. Por comodidad, en lo sucesivo denotaremos S_n por S y R_n por R.

Idempotentes de S

Sea un subconjunto de índices $I\subseteq\{1,\dots,n\}$, definimos los elementos:

$$e_I \;=\; \sum_{i\in I}e_i, \quad (e_\emptyset := 0_S).$$

Como la familia $\{e_i\}_{i=1}^n$ está formada por idempotentes ortogonales dos a dos, se sigue que cada e_I es también idempotente de S. Se ve fácilmente que además, dados $I,J\subseteq\{1,\dots,n\}$, entonces $e_I\cdot e_J = e_{I\cap J}$. Sea $e\in S$ un idempotente. Entonces existen $\lambda_1,\dots,\lambda_n\in F$ tales que $e=\sum_i\lambda_i e_i$. Como e es idempotente, $\sum_i\lambda_i e_i = e = e^2 = \sum_i\lambda_i^2 e_i$, luego $\lambda_i=\lambda_i^2$ para todo $i\in\{1,\dots,n\}$. Es decir, cada λ_i es idempotente de F, y como F es cuerpo sus únicos idempotentes son 0 y 1, luego cada λ_i es 0 o 1. En consecuencia existe $I\subseteq\{1,\dots,n\}$ tal que $e=e_I$. Queda así probado que el conjunto de idempotentes de S es exactamente $\{e_I \mid I\subseteq\{1,\dots,n\}\}$.

F-subálgebras de S

Sea T una F-subálgebra de S no nula. Sea un elemento $t\in T$ distinto de cero. Entonces existen $I_1,\dots,I_r\subseteq\{1,\dots,n\}$ no vacíos y disjuntos dos a dos tales que $t = \lambda_1 e_{I_1}+\cdots+\lambda_r e_{I_r}$, con $\lambda_1,\dots,\lambda_r\in F$ distintos y no nulos. Para cada $i\in\{1,\dots,n\}$, $t^i = \lambda_1^i e_{I_1}+\cdots+\lambda_r^i e_{I_r}\in T$, dando lugar al siguiente sistema matricial:

$$\begin{pmatrix}\lambda_1 & \cdots & \lambda_r\\ \lambda_1^2 & \cdots & \lambda_r^2\\ \vdots & \ddots & \vdots\\ \lambda_1^r & \cdots & \lambda_r^r\end{pmatrix}\begin{pmatrix}e_{I_1}\\ e_{I_2}\\ \vdots\\ e_{I_r}\end{pmatrix} = \begin{pmatrix}t\\ t^2\\ \vdots\\ t^r\end{pmatrix}$$

Como los $\lambda_1,\dots,\lambda_r$ son distintos y no nulos, la matriz $(\lambda_j^i)_{i,j}$ es de *Vandermonde* y, por tanto, invertible. Se sigue que $e_{I_1},\dots,e_{I_r}\in T$, luego T está generado como F-espacio vectorial por estos idempotentes. Así concluimos que toda F-subálgebra no nula T de S será de la forma $T = Fe_{I_1}\oplus\cdots\oplus Fe_{I_r}$, con $I_1,\dots,I_r\subseteq\{1,\dots,n\}$ no vacíos y disjuntos dos a dos.

F-automorfismos de S

Dado $\sigma \in \mathrm{Aut}_F(S)$, y $\mathrm{Aut}_F(S) := \{\sigma : S \to S \mid \sigma \text{ automorfismo de } F\text{-álgebras}\}$, como los $\{e_i\}$ son ortogonales dos a dos tenemos que

$$\sigma(e_i)\sigma(e_j) \;=\; \sigma(e_i e_j) \;=\; \begin{cases} \sigma(e_i), & i = j \\ 0, & i \neq j \end{cases} .$$

Es decir, la familia $\{\sigma(e_i)\}$ está formada por idempotentes ortogonales dos a dos. En consecuencia, existen $I_1, \ldots, I_n \subseteq \{1, \ldots, n\}$ no vacíos disjuntos dos a dos tales que cada $\sigma(e_i) = e_{I_i}$. Como $I_1, \ldots, I_n$ son n subconjuntos de $\{1, \ldots, n\}$ disjuntos y no vacíos, cada I_i tiene cardinal 1, es decir, que $\sigma(e_i) = e_{i'}$ para cierta permutación $i \mapsto i'$ de $\{1, \ldots, n\}$. Abusando de notación denotaremos esta permutación con el mismo σ, es decir, $\sigma(e_i) \;=\; e_{\sigma(i)}$ para todo $i \in \{1, \ldots, n\}$. Tenemos así definida una aplicación

$$\begin{array}{rccc} \varphi\colon & \mathrm{Aut}_F(S) & \longrightarrow & \mathrm{Sym}(n) \\ & \sigma & \longmapsto & \sigma \end{array}$$

donde $\mathrm{Sym}(n)$ denota el grupo simétrico de grado n. Como $\sigma\tau(e_i) = e_{\sigma\tau(i)}$, se tiene que φ es homomorfismo de grupos, y además inyectivo. Dado cualquier $\sigma \in \mathrm{Sym}(n)$, es posible definir el isomorfismo F-lineal sobre los elementos de la base dado por $\sigma(e_i) \;=\; e_{\sigma(i)}$. Además σ es homomorfismo de anillos ya que

$$\sigma(e_i)\sigma(e_j) = e_{\sigma(i)}e_{\sigma(j)} = \left\{ \begin{array}{ll} e_{\sigma(i)}, & i = j \\ 0, & i \neq j \end{array} \right\} = \sigma(e_i e_j),$$

luego φ es sobreyectiva y, por lo tanto, es un isomorfismo de grupos; es decir, $\mathrm{Aut}_F(S) \cong \mathrm{Sym}(n)$ como grupos.

Subgrupos de $\mathrm{Aut}_F(S)$ que sirven como grupo de Galois de S/R:

Veamos que los subgrupos de $\mathrm{Aut}_F(S)$ que sirven como grupo de Galois de la extensión S/R quedan caracterizados por las dos siguientes propiedades:

1. $|G| = n$.
2. Si $\sigma \in G$, $\sigma \neq id$, entonces $\sigma(i) \neq i$ para todo $i \in \{1, \ldots, n\}$.

En primer lugar, supongamos que la extensión S/R es de Galois con grupo de Galois asociado $G \leq \mathrm{Aut}_F(S)$. Sea $I \subseteq \{1, \ldots, n\}$ el conjunto de imágenes de 1 por las permutaciones asociadas a los distintos elementos de G. Dado $\sigma \in G$, $\sigma(e_I) = e_{\sigma(I)} = e_I$, ya que $\sigma(I) = I$ para todo $\sigma \in G$, luego $e_I \in S^G = R$. Como e_I tiene coeficiente 1 en e_1, no queda otra posibilidad aparte de $e_I = e_1 + \cdots + e_n$. Concluimos así que existe $\sigma \in G$ tal que $\sigma(1) = i$ para cada $i \in \{1, \ldots, n\}$. Con esto queda probado que $|G| \geq n$. Sea $\sigma \in G$, con $\sigma \neq id$. Si existiera algún $i \in \{1, \ldots, n\}$ tal que $\sigma(i) = i$, como los elementos de G son fuertemente distintos (apartado (a), teorema 1.7), se tendría que existe e_j tal que $\sigma(e_j)e_i \;\neq\; e_j e_i$. Como $\sigma(i) = i$, entonces $\sigma(e_i) = e_{\sigma(i)} = e_i$ y se sigue que $\sigma(e_j e_i) \neq e_j e_i$. Distinguimos entonces dos posibilidades:

- Si $i \neq j$, $e_j e_i = 0$ por ser ortogonales y $\sigma(e_j e_i) = \sigma(0) = 0 = e_j e_i$, absurdo.
- Si $i = j$, entonces $\sigma(e_i e_i) = \sigma(e_i) = e_i = e_i e_i$, absurdo.

De este modo queda probado que para cualquier elemento $\sigma \neq id$ de G no existe $i \in \{1, \dots, n\}$ tal que $\sigma(i) = i$. Terminemos ahora de ver que $|G| = n$. Ya sabemos que $|G| \geq n$, así que supongamos que $|G| > n$. En tal caso existen $\sigma, \tau \in G$, $\sigma \neq \tau$ tales que $\sigma(1) = \tau(1)$. Entonces $\tau^{-1}\sigma(1) = 1$, pero $\tau^{-1}\sigma \neq id$. Esto contradice lo que acabamos de demostrar, luego $|G| = n$. Queda así probado que todo grupo de Galois de la extensión de Galois S/R verifica las propiedades (1) y (2) propuestas.

Veamos el recírpoco, es decir, que todo subgrupo de $\mathrm{Aut}_F(S)$ que cumpla estas propiedades será un grupo de Galois de la extensión S/R. Asumamos que cierto subgrupo G de $\mathrm{Aut}_F(S)$ cumple las propiedades (1) y (2). Deducimos inmediatamente que $\{\sigma(1) \mid \sigma \in G\} = \{1, \dots, n\}$. Dado $s \in S^G$, $s = \lambda_1 e_1 + \cdots + \lambda_n e_n$ para ciertos $\lambda_i \in F$. Sea $\sigma \in G$ tal que $\sigma(1) = i$, $\sigma(s) = s$ implica $\lambda_i = \lambda_1$. Repitiendo esto para cada posible imagen del elemento 1 se concluye que existe $\lambda \in F$ tal que $\lambda_i = \lambda$ para cada i, es decir, que $s \in R$ y $S^G = R$ (hipótesis del teorema 1.7). Sean $x_i := e_i$, $y_i := e_i$, con $i = 1, \dots, n$. Dado $\sigma \in G$, notamos que

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \sum_{i=1}^{n} e_i e_{\sigma(i)} = \begin{cases} 0, & \sigma \neq id \\ 1_S, & \sigma = id \end{cases},$$

luego estos elementos $\{x_i, y_i\}$ cumplen la propiedad (b) del teorema 1.7 y, por lo tanto, la extensión es de Galois con grupo de Galois G.

Así hemos probado que las propiedades (1) y (2) son una caracterización de los subgrupos de $\mathrm{Aut}_F(S)$ que sirven como grupo de Galois de la extensión de Galois S/R. Una implicación de este resultado es que una misma de extensión de Galois puede tener varios grupos de Galois diferentes no isomorfos entre sí (de hecho, esto es lo natural).

Correspondencia de Galois

A continuación veremos cómo dado un subgrupo H de G, la aplicación $H \mapsto \mathrm{Fix}(H)$ proporciona una biyección entre los subgrupos de G y las subálgebras G-fuertes de S. Para esto estudiaremos por separado cómo son las álgebras $\mathrm{Fix}(H)$ y las subálgebras G-fuertes, además de cómo la aplicación propuesta las relaciona uno a uno.

1. **Estudio de** $\mathrm{Fix}(H)$**:**

   Sea un subgrupo $H \leq G$. Consideremos la descomposición en órbitas de $\{1, \dots, n\}$ bajo la acción de H, que denotamos $\{1, \dots, n\} = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_m$. Es claro que para cada órbita $\mathcal{O}_i$ el idempotente $e_{\mathcal{O}_i}$ pertenece a $\mathrm{Fix}(H)$, de donde concluimos que

   $$Fe_{\mathcal{O}_1} \oplus \cdots \oplus Fe_{\mathcal{O}_m} \subseteq \mathrm{Fix}(H).$$

   Sea $s = \sum_i \lambda_i e_i \in \mathrm{Fix}(H)$ para ciertos $\lambda_i \in F$. Entonces $\sum_i \lambda_i e_i = s = \sigma(s) = \sum_i \lambda_i e_{\sigma(i)}$ para todo $\sigma \in H$. Esto implica que $\lambda_i = \lambda_{\sigma(i)}$ para todo $\sigma \in H$, de donde se sigue que $\lambda_i = \lambda_j$ implica $\mathrm{Orb}(i) = \mathrm{Orb}(j)$. Queda así probado que $s \in Fe_{\mathcal{O}_1} \oplus \cdots \oplus Fe_{\mathcal{O}_m}$, con lo que finalmente

   $$\mathrm{Fix}(H) \;=\; Fe_{\mathcal{O}_1} \oplus \cdots \oplus Fe_{\mathcal{O}_m}$$

2. $\mathrm{Fix}(H)$ **es** G**-fuerte:**

   Veamos que la aplicación $H \mapsto \mathrm{Fix}(H)$ manda todo subgrupo a una subálgebra G-fuerte de S. Sean $\sigma, \tau \in G$ tales que $\sigma|_{\mathrm{Fix}(H)} \neq \tau|_{\mathrm{Fix}(H)}$ y $e \in S$ un idempotente no nulo. Entonces e es igual a e_I para cierto $I \subseteq \{1, \dots, n\}$ no vacío. Sea $j \in \tau^{-1}(I)$, consideremos su órbita

bajo la acción de H $\mathrm{Orb}(j) = \mathcal{O}$. Notamos que $j \in \tau^{-1}(I) \cap \mathcal{O}$, luego $\tau(j) \in I \cap \tau(\mathcal{O})$. Supongamos que $\sigma(e_{\mathcal{O}})e = \tau(e_{\mathcal{O}})e$. Entonces

$$e_{\sigma(\mathcal{O})}e_I = e_{\tau(\mathcal{O})}e_I \text{ , que implica } e_{\sigma(\mathcal{O})\cap I} = e_{\tau(\mathcal{O})\cap I},$$

luego $\sigma(\mathcal{O}) \cap I = \tau(\mathcal{O}) \cap I$. Como $\tau(j) \in I \cap \tau(\mathcal{O})$, existe $j' \in \mathcal{O}$ tal que $\tau(j) = \sigma(j')$. Además, como $j' \in \mathcal{O}$, existe $\rho \in H$ tal que $j' = \rho(j)$, lo que implica que $\tau(j) = \sigma\rho(j)$. Se sigue entonces que $\tau^{-1}\sigma\rho(j) = j$, por lo que según la caracterización de los grupos de Galois, $\tau^{-1}\sigma\rho = id$, o lo que es lo mismo, $\tau = \sigma\rho$. No obstante, como $\rho \in H$,

$$\tau|_{\mathrm{Fix}(H)} = \sigma\rho|_{\mathrm{Fix}(H)} = \sigma|_{\mathrm{Fix}(H)}.$$

Absurdo, luego las restricciones a $\mathrm{Fix}(H)$ de elementos de G son fuertemente distintas dos a dos, y en consecuencia que $\mathrm{Fix}(H)$ es G-fuerte.

3. $\mathrm{Fix}(\cdot)$ **es inyectiva con los subgrupos de** G**:**

   Ya hemos probado antes que para $H \leq G$, $\mathrm{Fix}(H) = Fe_{\mathcal{O}_1} \oplus \cdots \oplus Fe_{\mathcal{O}_m}$, donde los $\mathcal{O}_i$ son las órbitas que deja H en $\{1, \ldots, n\}$. Notamos que el único conjunto de $m = \dim(\mathrm{Fix}(H))$ idempotentes ortogonales dos a dos es $\{e_{\mathcal{O}_1}, \ldots, e_{\mathcal{O}_m}\}$. Si $\mathrm{Fix}(H) = \mathrm{Fix}(H')$, las órbitas de H' en su acción en $\{1, \ldots, n\}$ coinciden con las de H. Sea $\sigma \in H$, como $\sigma(1) \in \mathrm{Orb}(1)$, existe un $\sigma' \in H'$ tal que $\sigma'(1) = \sigma(1)$. Entonces $\sigma^{-1}\sigma'(1) = 1$, es decir, $\sigma^{-1}\sigma' = id$ y así $\sigma = \sigma' \in H'$. Al aplicar esto a cada elemento de H se obtiene que $H \subseteq H'$. De forma análoga se sigue que $H' \subseteq H$, luego $H = H'$. Queda así probado que $H \neq H'$ implica que $\mathrm{Fix}(H) \neq \mathrm{Fix}(H')$.

4. **Subálgebras** G**-fuertes de** S **que contienen a** R**:**

   Sea T una subálgebra de S. Por lo ya visto sabemos que $T = Fe_{I_1} \oplus \cdots \oplus Fe_{I_r}$ para ciertos $I_1, \ldots, I_r \subseteq \{1, \ldots, n\}$ no vacíos y disjuntos dos a dos. Como $R \subseteq T$, necesariamente $\bigcup_j I_j = \{1, \ldots, n\}$. Consideremos $H := \mathrm{Fix}(T)$. Como $\sigma(e_{I_j}) = e_{I_j}$ para todo $\sigma \in H$, entonces $\sigma(I_j) = I_j$ para todo $\sigma \in H$. Se sigue que cada I_i es unión de órbitas bajo H. Supongamos que existe I_i tal que es unión de más de una H-órbita, y sean $\mathcal{O}'$, $\mathcal{O}''$ dos H-órbitas distintas contenidas en este I_i. Consideremos $j \in \mathcal{O}'$. Como $\{\sigma(j) \mid \sigma \in G\} = \{1, \ldots, n\}$, existe $\sigma \in G$ tal que $\sigma(j) \in \mathcal{O}''$. Como $\sigma(j) \in \mathcal{O}'' \neq \mathcal{O}'$, necesariamente $\sigma \notin H$, luego $\sigma|_T \neq id|_T$. Esto implica que existe $t \in T$ tal que $\sigma(t)e_{\sigma(j)} \neq te_{\sigma(j)}$. Se sigue que existe I_k tal que $\sigma(e_{I_k})e_{\sigma(j)} \neq e_{I_k}e_{\sigma(j)}$, pero como I_k es unión de H-órbitas:

   - Si $k \neq i$, entonces $I_k \cap I_i = \emptyset$, que implica $I_k \cap \mathcal{O}' = I_k \cap \mathcal{O}'' = \emptyset$. Se sigue que $j, \sigma(j) \notin I_k$, luego $\sigma(e_{I_k})e_{\sigma(j)} = \sigma(e_{I_k}e_j) = 0 = e_{I_k}e_{\sigma(j)}$, absurdo. Concluimos que la única posibilidad es $k = i$.
   - Si $k = i$, entonces $j, \sigma(j) \in I_k$. Esto implica que $\sigma(e_{I_k})e_{\sigma(j)} = \sigma(e_{I_k}e_j) = \sigma(e_j) = e_{\sigma(j)} = e_{I_k}e_{\sigma(j)}$, otro absurdo.

   Concluimos que ningún I_j puede ser unión de más de una H-órbita. Como los I_j son no vacíos y disjuntos dos a dos, concluimos que cada I_j es exactamente una H-órbita diferente. Como además $\bigcup_j I_j = \{1, \ldots, n\}$, resulta finalmente que $I_1, \ldots, I_r$ son todas las H-órbitas, y así $T = \mathrm{Fix}(H)$.

Hemos visto así que $H \mapsto \mathrm{Fix}(H)$ está bien definida como aplicación de los subgrupos de G a las subálgebras G-fuertes de S que contienen a R (puntos 1 y 2), que es inyectiva (punto 3) y que es sobreyectiva (punto 4). Queda entonces probado que proporciona la correspondencia biyectiva de la que nos habla el teorema fundamental generalizado (teorema 1.16).

Ejemplo 1.24 (Caso particular $n = 4$)**.** Consideremos la extensión del ejemplo 1.23 para $n = 4$,

$$S = Fe_1 \oplus Fe_2 \oplus Fe_3 \oplus Fe_4,\ R = F(e_1 + e_2 + e_3 + e_4),$$

(por comodidad renombramos $S_4 = S$, $R_4 = R$) con el grupo de Galois $G = \langle\sigma\rangle$, donde σ es la permutación (1234) (que cumple la caracterización de los grupos de Galois de S/R probada en el ejemplo 1.23). Como σ es un 4-ciclo, notamos que $G \cong \mathbb{Z}/4\mathbb{Z}$. Por otro lado, consideremos el grupo $H = \langle\tau_1, \tau_2\rangle < \mathrm{Aut}(S)$, con $\tau_1 = (12)(34)$ y $\tau_2 = (13)(24)$. Observamos que $\tau_1\tau_2 = (14)(23) = \tau_2\tau_1$, luego todo elemento de H tiene orden 2 y $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Calculamos S^H: dado un elemento $s = ae_1 + be_2 + ce_3 + de_4 \in S$,

$$\left\{\begin{array}{rcll} 1(s) & = & ae_1 + be_2 + ce_3 + de_4 & = & (a,b,c,d) \\ \tau_1(s) & = & be_1 + ae_2 + de_3 + ce_4 & = & (b,a,d,c) \\ \tau_2(s) & = & ce_1 + de_2 + ae_3 + be_4 & = & (c,d,a,b) \\ \tau_1\tau_2(s) & = & de_1 + ce_2 + be_3 + ae_4 & = & (d,c,b,a) \end{array}\right.$$

Notamos que $s = \tau(s)$ para todo $\tau \in H$ equivale a que $a = b = c = d$. Es decir, $s \in R$, luego $S^H = S^G = R$. Si $x_i = y_i = e_i$ para $i = 1, \ldots, 4$, dado $\tau \in H$ se tiene que

$$\sum_{i=1}^{4} x_i\tau(y_i) = \sum_{i=1}^{4} e_i\tau(e_i) = \left\{\begin{array}{ll} 1, & \text{si } \tau = 1 \\ 0, & \text{si } \tau \neq 1 \end{array}\right.$$

luego se verifica la propiedad (b) del teorema 1.3 y concluimos que S es extensión de Galois de R con grupo de Galois H. También se podría haber visto que H cumple la caracterización de los grupos de Galois de S/R probada en el ejemplo 1.23. Acabamos de ver así que la extensión de Galois S/R lo es tanto para el grupo G como para el grupo H. Sin embargo, observamos que

$$G \cong \mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong H,$$

ejemplo de que una extensión puede tener asociados distintos grupos de Galois no isomorfos.

A continuación veremos cómo solo las subálgebras *fuertes* participan en la correspondencia. Si usamos como grupo de Galois $G = \langle\sigma\rangle = \langle(1234)\rangle$, $\langle\sigma^2\rangle$ es el único subgrupo no trivial de G. Sin embargo S tiene más de una R-subálgebra diferente. Lo que sucede es que, a excepción de una única subálgebra T que hallaremos ahora, ninguna más (no trivial) es G-fuerte. Como $\sigma = (1234)$, entonces $\sigma^2 = (13)(24)$, $\sigma^3 = (1432)$ y $\sigma^4 = id = 1$. Veamos que la subálgebra $T = F(e_1 + e_3) \oplus F(e_2 + e_4)$ es G-fuerte y que $\mathrm{Fix}(T) = \langle\sigma^2\rangle$. Sea $t \in T$, existen $a, b \in F$ tales que $t = a(e_1 + e_3) + b(e_2 + e_4) = (a,b,a,b)$. La imagen de t por cada elemento de G es:

$$\left\{\begin{array}{rcll} 1(t) & = & \sigma^2(t) & = & (a,b,a,b) \\ \sigma(t) & = & \sigma^3(t) & = & (b,a,b,a) \end{array}\right.$$

Resulta que $1|_T = \sigma^2|_T$ y $\sigma|_T = \sigma^3|_T$, luego para probar que T es G-fuerte basta con ver que $1|_T$ y $\sigma|_T$ son fuertemente distintas como aplicaciones de T a S. Los idempotentes de S son los elementos de la forma $e = (\lambda_1, \lambda_2, \lambda_3, \lambda_4)$, donde cada λ_i es 1 ó 0. Sea $t \in T$,

$$1(t)e = \sigma(t)e \ \text{ equivale a que } \ a\lambda_i = b\lambda_i, \ \text{ para todo } a, b \in F, \ i = 1, \ldots, 4.$$

Esto implica que $\lambda_i = 0$ para cada i, es decir, que $e = 0$. Así queda probado que $1|_T$ y $\sigma|_T$ son fuertemente distintas, y concluimos que T es G-fuerte. Observamos ahora que, según la fórmula dada en el teorema fundamental 1.16, $\mathrm{Fix}(T) = \{\tau \in G \mid \tau(t) = t, \text{ para todo } t \in T\}$. Como σ^2 es el único elemento de G cuya restricción a T coincide con $1|_T$, $\mathrm{Fix}(T) = \langle\sigma^2\rangle$. Es claro que las restricciones de los elementos de $G = \langle\sigma\rangle$ a R son todas iguales, luego R es G-fuerte y $\mathrm{Fix}(R) = G$. Como la extensión es de Galois, por el apartado (a) del teorema 1.7 sabemos que todos los elementos de G son fuertemente distintos dos a dos, luego S también es G-fuerte y $\mathrm{Fix}(S)$ es el grupo trivial. Podemos representar nuestra correspondencia con el diagrama de la Figura 1.1.

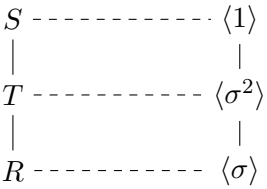


Figura 1.1: Diagrama de la correspondencia entre las R-subálgebras G-fuertes de S y los subgrupos del grupo de Galois G

Este ejemplo es particularmente ilustrativo, ya que el subgrupo $\langle\sigma\rangle$ es normal. Según el teorema fundamental, no solo S/T es extensión de Galois con grupo de Galois $\langle\sigma^2\rangle$, sino que además T/R es extensión de Galois con grupo de Galois $G/\langle\sigma^2\rangle$. Es sencillo comprobar que $T^{G/\langle\sigma^2\rangle} = R$, y tomando $x_1 = y_1 = e_1 + e_3$, $x_2 = y_2 = e_2 + e_3$ vemos que:

$$x_1\bar{1}(y_1) + x_2\bar{1}(y_2) = (e_1 + e_3)^2 + (e_2 + e_4)^2 = e_1 + e_3 + e_2 + e_4 = 1_T$$
$$x_1\bar{\sigma}(y_1) + x_2\bar{\sigma}(y_2) = 2(e_1 + e_3)(e_2 + e_4) = 2 \cdot 0_T = 0_T$$

luego se cumple la propiedad (b) del teorema 1.7 y concluimos que la extensión T/R es de Galois, con grupo de Galois $G/\langle\sigma^2\rangle$.

Veamos ahora qué sucede con el resto de subálgebras. Comprobaremos que efectivamente no son G-fuertes, luego no participan en la correspondencia con los subgrupos de G. Sea $U = Fe_1 \oplus F(e_2 + e_3 + e_4)$ (resultado equivalente para las demás subálgebras generadas por $\{(1,1,1,1), e_i\}$ para algún i). En este caso, dado un elemento $u = (a, b, b, b) \in U$,

$$\begin{cases} 1(u) &= (a,b,b,b) \\ \sigma(u) &= (b,a,b,b) \end{cases}$$

Es claro que $1|_U \neq \sigma|_U$, pero para el idempotente $e_3 = (0,0,1,0)$ de S se tiene que $1(u)e_3 = (0,0,b,0) = \sigma(u)e_3$. Es decir, no son fuertemente distintas y en consecuencia U no es G-fuerte. Probemos ahora con $V = F(e_1 + e_2) \oplus F(e_3 + e_4)$ (análogo para $F(e_1 + e_4) \oplus F(e_2 + e_3)$). En este caso los elementos son de la forma $v = (a, a, b, b)$ para valores $a, b \in F$, y se tiene que

$$\begin{cases} 1(v) &= (a,a,b,b) \\ \sigma(v) &= (b,a,a,b) \end{cases}$$

Notamos que $1|_V \neq \sigma|_V$, pero $1(v)e_4 = \sigma(v)e_4$ para todo $v \in V$, luego V no es G-fuerte. Por último, para $W = F(e_1) \oplus F(e_2) \oplus F(e_3 + e_4)$ (análogo para los demás generados por $\{(1,1,1,1), e_i, e_j\}$), los elementos son de la forma $w = (a, b, c, c)$ para valores $a, b, c \in F$, y así

$$\begin{cases} 1(w) &= (a,b,c,c) \\ \sigma(w) &= (c,a,b,c) \end{cases}$$

Vemos que $1|_W \neq \sigma|_W$, pero $1(w)e_4 = c = \sigma(w)e_4$ para todo $w \in W$, luego W no es G-fuerte. Con esto queda visto que todas las demás subálgebras de S/R no son G-fuertes.

A continuación, realicemos el estudio de la correspondencia de Galois pero esta utilizando $H = \langle\tau_1 = (12)(34), \tau_2 = (13)(24)\rangle$ como grupo de Galois de S/R. Como $\tau_2 = \sigma^2$, una de las subálgebras H-fuertes es la misma T encontrada antes para G, que denotaremos $T_2 = F(e_1 + e_3) \oplus F(e_2 + e_4)$. Su subgrupo correspondiente es $\mathrm{Fix}(T_2) = \langle\tau_2\rangle$. Sea $T_1 = F(e_1 + e_2) \oplus F(e_3 + e_4)$. Para $t = (a, a, b, b) \in T_1$,

$$\begin{cases} 1(t) &= \tau_1(t) &= (a,a,b,b) \\ \tau_2(t) &= \tau_3(t) &= (b,b,a,a) \end{cases}$$

Vemos que $1|_{T_1} = \tau_1|_{T_1}$, $\tau_2|_{T_1} = \tau_3|_{T_1}$. Siguiendo un argumento análogo al utilizado antes con T y el grupo G, se comprueba que $1|_{T_1}$ y $\tau_2|_{T_1}$ son fuertemente distintas, luego T_1 es H-fuerte. De hecho, con la fórmula del teorema fundamental se obtiene que $\mathrm{Fix}(T_1) = \langle\tau_1\rangle$. Para la subálgebra $T_3 = F(e_1 + e_4) \oplus F(e_2 + e_3)$, un proceso completamente análogo indica que T_3 también es H-fuerte, y que $\mathrm{Fix}(T_3) = \langle\tau_3\rangle$. El grupo H solo posee tres subgrupos no triviales: $\langle\tau_1\rangle$, $\langle\tau_2\rangle$ y $\langle\tau_3\rangle$; y ya hemos encontrado sus tres subálgebras correspondientes (T_1, T_2 y T_3 respectivamente). Se sigue que ninguna de las demás subálgebras de la extensión S/R es H-fuerte (el proceso es análogo al utilizado cuando el grupo de Galois era G). La Figura 1.2 muestra un diagrama de la correspondencia hallada:

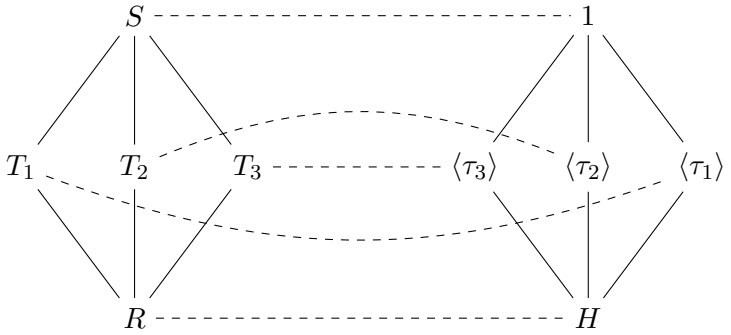


Figura 1.2: Diagrama de la correspondencia entre las R-subálgebras H-fuertes de S y los subgrupos del grupo de Galois H

De esta manera hemos visto cómo S es una extensión de Galois de T_1 con grupo de Galois $\langle\tau_1\rangle$ (y análogo para T_2 y T_3). Como además los tres subgrupos son normales, tenemos también que T_1 es extensión de Galois de R con grupo de Galois $H/\langle\tau_1\rangle$ (análogo para T_2 y T_3).

Capítulo 2

Teoría de Galois-Hopf

En este segundo capítulo estudiaremos la teoría de Galois basada en álgebras de Hopf, que permite generalizar la teoría de Galois a extensiones de anillos unitarios (no necesariamente conmutativos). La teoría de este capítulo se basa principalmente en [10] y [13]. En lo que sigue, se considerará de nuevo R como un anillo conmutativo unitario, que nos servirá como conjunto de escalares.

2.1. H-Extensiones de anillos

El primer paso es definir lo que entendemos por extensión de anillos, que ahora utilizará un álgebra de Hopf. Definir el concepto de álgebra de Hopf requiere introducir nuevas estructuras algebraicas.

2.1.1. Álgebras de Hopf

La siguiente estructura corresponde al dual del álgebra, que se sigue de la de dual de un módulo (definición 2.61).

Definición 2.1 (Coálgebra)**.** Una **coálgebra** sobre un anillo conmutativo R (o R-coálgebra) es un R-módulo C junto con dos aplicaciones R-lineales $\Delta : C \to C \otimes C$ (comultiplicación) y $\varepsilon : C \to R$ (counidad) tales que:

1. $(id_C \otimes \Delta) \circ \Delta = (\Delta \otimes id_C) \circ \Delta$
2. $(id_C \otimes \varepsilon) \circ \Delta = id_C = (\varepsilon \otimes id_C) \circ \Delta$

Definición 2.2 (Biálgebra)**.** Sea R un anillo conmutativo y B un R-módulo. $(B, m, \eta, \Delta, \varepsilon)$ es una **biálgebra** sobre R (o R-biálgebra) si se verifica que:

1. (B, m, η) es un álgebra ($m : B \otimes B \to B$ es la multiplicación y $\eta : R \to B$ es la unidad).
2. (B, Δ, ε) es un coálgebra ($\Delta : B \to B \otimes B$ es la comultiplicación y $\varepsilon : B \to R$ es la counidad).
3. Δ y ε son homomorfismos de álgebras.

Definición 2.3 (Álgebra de Hopf)**.** Un **álgebra de Hopf** H sobre un anillo conmutativo R (o R-álgebra de Hopf) es una biálgebra sobre R junto con una aplicación R-lineal $S : H \to H$ (llamada antípoda) tal que se verifican las siguientes identidades:

$$m \circ (S \otimes id_H) \circ \Delta \quad = \quad m \circ (id_H \otimes S) \circ \Delta \quad = \quad \varepsilon \circ \eta$$

La notación habitual para las álgebras de Hopf que intervienen en la teoría de Galois-Hopf utiliza las letras H y L. En lo que sigue, se considerarán H y L como álgebras de Hopf sobre el anillo conmutativo R. A continuación veremos uno de los ejemplos más naturales de álgebras de Hopf: el álgebra grupo. Será su dual el álgebra de Hopf que utilizaremos más adelante para trasladar las extensiones de cuerpos clásicas a la teoría de Galois-Hopf.

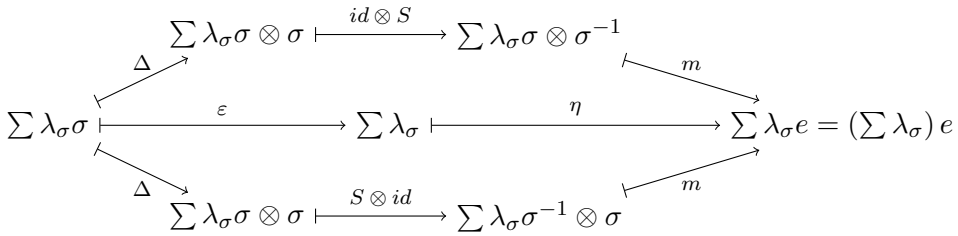
Ejemplo 2.4 (El álgebra grupo)**.** Sean R un anillo conmutativo unitario y G un grupo. El álgebra grupo, denotada $R[G]$, es un R-módulo libre con base $\{\sigma \in G\}$. Notamos que todo elemento de $R[G]$ es de la forma $\sum_{\sigma\in G} \lambda_\sigma \sigma$, donde cada $\lambda_\sigma \in R$. Su estructura de álgebra está dada por la multiplicación de los elementos de la base mediante el producto del grupo G. Veamos a continuación que las aplicaciones (expresadas en términos homogéneos)

$$\Delta(\sigma) = \sigma \otimes \sigma, \quad \varepsilon(\sigma) = 1_R,$$

dotan a $R[G]$ de estructura de coálgebra. Notamos que, para $\sum_{\sigma\in G} \lambda_\sigma \sigma \in R[G]$,

$$\begin{aligned}
(id \otimes \Delta)\left(\Delta\left(\sum \lambda_\sigma \sigma\right)\right) &= (id \otimes \Delta)\left(\sum \lambda_\sigma(\sigma \otimes \sigma)\right) = \sum \lambda_\sigma(\sigma \otimes \sigma \otimes \sigma) \\
&= (\Delta \otimes id)\left(\sum \lambda_\sigma(\sigma \otimes \sigma)\right) = (\Delta \otimes id)\left(\Delta\left(\sum \lambda_\sigma \sigma\right)\right), \\
(id \otimes \varepsilon)\left(\Delta\left(\sum \lambda_\sigma \sigma\right)\right) &= (id \otimes \varepsilon)\left(\sum \lambda_\sigma(\sigma \otimes \sigma)\right) = \sum \lambda_\sigma(\sigma \otimes 1) \cong \sum \lambda_\sigma \sigma \\
&\cong \sum \lambda_\sigma(1 \otimes \sigma) = (\varepsilon \otimes id)\left(\Delta\left(\sum \lambda_\sigma \sigma\right)\right),
\end{aligned}$$

luego en efecto $(R[G], \Delta, \varepsilon)$ es una R-coálgebra. Es trivial que Δ y ε son homomorfismos de álgebras, luego $R[G]$ es además una biálgebra. Veamos ahora que la aplicación $S(\sigma) = \sigma^{-1}$ es una antípoda de $R[G]$ mediante el siguiente diagrama:



Así queda probado que $R[G]$ es un álgebra de Hopf. Cuando G es un grupo finito, el dual de $R[G]$ (que denotamos $R[G]^*$) es también un álgebra de Hopf (proposición 2.73). Notamos que $\{\sigma^* \mid \sigma \in G\}$ es una base de $R[G]^*$, donde cada σ^* denota el dual de cada $\sigma \in G$ (es decir, $\sigma^*(\tau) = \delta_{\sigma,\tau}$, para todo $\sigma, \tau \in G$). Se sigue que el producto en $R[G]^*$ está dado por multiplicar los elementos de la base mediante $\sigma^*\tau^* = \delta_{\sigma,\tau}\tau^*$. Sin entrar en los detalles de la obtención de cada una de sus aplicaciones y unidad como álgebra de Hopf, nos basta con saber que estas son (expresadas en términos homogéneos):

$$\Delta'(\sigma^*) = \sum_{\tau\in G} \tau^* \otimes (\tau^{-1}\sigma)^*, \quad \varepsilon'(\sigma^*) = \delta_{\sigma,e}, \quad S'(\sigma^*) = (\sigma^{-1})^*, \quad 1_{R[G]^*} = \sum_{\sigma\in G} \sigma^*.$$

2.1.2. Comódulos y comódulo álgebras

Definición 2.5 (Comódulo)**.** Sea (C, Δ, ε) una R-coálgebra. Un C**-comódulo** a derecha es un R-módulo A junto con una aplicación R-lineal

$$\begin{array}{rccc} \delta\colon & A & \longrightarrow & A \otimes C \\ & a & \longmapsto & \sum a_{(0)} \otimes a_{(1)} \end{array}$$

tal que $(A \otimes \Delta) \circ \delta = (\delta \otimes C) \circ \delta$. Si además $(A \otimes \varepsilon) \circ \delta = id_A$, el comódulo se dice **counital**.

La definición de comódulo a izquierda cambia δ por $\delta' : A \to C \otimes A$. Para los comódulos a izquierda usaremos la notación $\delta'(a) = a_{(-1)} \otimes a_{(0)}$.

Notación. Aunque lo correcto es escribir $\delta(a) = \sum a_{(0)} \otimes a_{(1)}$, omitimos el sumatorio por comodidad. Además, abusaremos de notación escribiendo X en lugar de id_X, sobre todo cuando id_X aparezca como factor de un producto tensorial de aplicaciones.

Definición 2.6 (Homomorfismo de comódulos a derecha)**.** Sea C una R-coálgebra. Sean M y N dos C-comódulos a derecha, cuya estructura está dada por δ_M y δ_N respectivamente. Una aplicación R-lineal $f : M \to N$ se dice **homomorfismo de C-comódulos** a derecha si $\delta_N \circ f = (f \otimes C) \circ \delta_M$.

Definición 2.7 (Comódulo álgebra)**.** Un H**-comódulo álgebra** a derecha A es un álgebra y un H-comódulo counital a derecha tal que:

1. $(ab)_{(0)} \otimes (ab)_{(1)} = a_{(0)}b_{(0)} \otimes a_{(1)}b_{(1)}$
2. $\delta_r(1_A) = 1_A \otimes 1_H$

Llamamos conjunto de **coinvariantes** de A al conjunto $A^{\mathrm{co}H} := \left\{ a \in A \mid a_{(0)} \otimes a_{(1)} = a \otimes 1 \right\}$ (para los comódulos álgebra a izquierda lo denotamos ${}^{\mathrm{co}H}A$).

2.1.3. H-Extensiones de Galois

A continuación definiremos las extensiones de anillos utilizando la estructura de comódulo álgebra. Las siguientes definiciones serán solo «a derecha», pero su versión a izquierda es análoga.

Definición 2.8 (H-Extensión)**.** Sean A, B dos R-álgebras, donde B es una subálgebra unitaria de A. Diremos que A/B es una H**-extensión** a derecha si A es una H-comódulo álgebra a derecha tal que $A^{\mathrm{co}H} = B$.

Definición 2.9 (H-Extensión de Galois)**.** Sea A un H-comódulo álgebra a derecha, donde su estructura de comódulo está dada por $\delta : A \to A \otimes H$. Diremos que la H**-extensión** $A/A^{\mathbf{co}H}$ **es de Galois** a derecha si la aplicación

$$\boxed{\begin{array}{rccc} \kappa_r\colon & A \otimes_{A^{\mathrm{co}H}} A & \longrightarrow & A \otimes_R H \\ & a \otimes' b & \longmapsto & (a \otimes 1)\delta(b) = ab_{(0)} \otimes b_{(1)} \end{array}}$$

es biyectiva. A esta aplicación κ_r la llamaremos *aplicación de Galois* de la extensión.

En secciones posteriores utilizaremos también una aplicación (definida cuando la H-extensión es de Galois, por ser biyectiva) que denotaremos γ y definimos como sigue (entendiendo que omitimos el sumatorio en i):

$$\boxed{\begin{array}{rccc} \gamma\colon & H & \longrightarrow & A \otimes A \\ & h & \longmapsto & l_i(h) \otimes r_i(h) := \kappa_r^{-1}(1 \otimes h) \end{array}}$$

2.1.4. Estructura de ${}_A\mathcal{M}^H$ y $\mathcal{M}_A^H$

A continuación estudiaremos ciertas estructuras de $A \otimes A$ y $A \otimes H$ (para H un álgebra de Hopf y A un H-comódulo álgebra a derecha), que será necesario conocer para la demostración de algunos resultados posteriores. Estas proposiciones se han tomado de [15, 196-231]. En particular, definimos las categorías ${}_A\mathcal{M}^H$ y $\mathcal{M}_A^H$ de la forma siguiente:

- Objetos de ${}_A\mathcal{M}^H$: A-módulos a izquierda M que son además H-comódulos a derecha (mediante δ), y tales que $\delta(ax) = a_{(0)}x_{(0)} \otimes a_{(1)}x_{(1)}$.
- Objetos de $\mathcal{M}_A^H$: A-módulos a derecha M que son además H-comódulos a derecha (mediante δ), y tales que $\delta(xa) = x_{(0)}a_{(0)} \otimes x_{(1)}a_{(1)}$.

En lo que sigue, abusaremos de notación escribiendo tan solo $M \in \mathcal{M}_A^H$ en lugar de $M \in \mathrm{Obj}(\mathcal{M}_A^H)$. En general, el producto tensorial de dos H-comódulos a derecha M, N es también H-comódulo a derecha mediante la **coacción codiagonal** $\delta(x \otimes y) = x_{(0)} \otimes y_{(0)} \otimes x_{(1)}y_{(1)}$. Sin embargo, la demostración de algunas identidades de más adelante requerirá una estructura diferente, que presentamos en la siguiente proposición.

Proposición 2.10 (Estructuras auxiliares de $A \otimes A$ y $A \otimes H$)**.** *Sean H un álgebra de Hopf y A un H-comódulo álgebra a derecha. Entonces:*

1. $A \otimes A \in_A \mathcal{M}^H$ *mediante* $a(b \otimes c) := (ab) \otimes c$, $\delta(b \otimes c) := b_{(0)} \otimes c \otimes b_{(1)}$.
2. $A \otimes H \in_A \mathcal{M}^H$ *mediante* $a(b \otimes h) := (ab) \otimes h$, $\delta(b \otimes h) := b_{(0)} \otimes h_{(2)} \otimes b_{(1)}S(h_{(1)})$.
3. $A \otimes A \in \mathcal{M}_A^H$ *mediante* $(b \otimes c)a := b \otimes (ca)$, $\delta(b \otimes c) := b \otimes c_{(0)} \otimes c_{(1)}$.
4. $A \otimes H \in \mathcal{M}_A^H$ *mediante* $(b \otimes h)a := ba_{(0)} \otimes h_{(1)}a_{(1)}$, $\delta(b \otimes h) := b \otimes h_{(0)} \otimes h_{(1)}$.

Proposición 2.11. *La aplicación κ_r es un morfismo en ${}_A\mathcal{M}^H$ y $\mathcal{M}_A^H$.*

Demostración. Veamos en primer lugar que κ_r es un morfismo en ${}_A\mathcal{M}^H$. Notamos que, para $a, b, c \in A$, $\kappa_r(a(b \otimes c)) = \kappa_r((ab) \otimes c) = abc_{(0)} \otimes c_{(1)} = a \cdot (bc_{(0)}) \otimes c_{(1)} = a \cdot \kappa_r(b \otimes c)$. Por otro lado, $\delta(\kappa_r(b \otimes c)) = \delta(bc_{(0)} \otimes c_{(1)}) = b_{(0)}c_{(0)(0)} \otimes c_{(1)(2)} \otimes b_{(1)}c_{(0)(1)}S(c_{(1)(1)}) = b_{(0)}c_{(0)} \otimes c_{(3)} \otimes b_{(1)}c_{(1)}S(c_{(2)})$. Usando que $h_{(1)}S(h_{(2)}) = \varepsilon(h)1$ obtenemos que esta última expresión es igual a $b_{(0)}c_{(0)} \otimes c_{(1)} \otimes b_{(1)}$. Como $(\kappa_r \otimes H)\delta(b \otimes c) = (\kappa_r \otimes H)(b_{(0)} \otimes c \otimes b_{(1)}) = b_{(0)}c_{(0)} \otimes c_{(1)} \otimes b_{(1)}$, se sigue que $\delta\kappa_r = (\kappa_r \otimes H)\delta$. Veamos ahora que κ_r es un morfismo en $\mathcal{M}_A^H$. Dados $a, b, c \in A$, $\kappa_r((b \otimes c)a) = \kappa_r(b \otimes (ca)) = bc_{(0)}a_{(0)} \otimes c_{(1)}a_{(1)} = bc_{(0)} \otimes c_{(1)} \cdot a = \kappa_r(b \otimes c) \cdot a$. Por otro lado, $\delta(\kappa_r(b \otimes c)) = \delta(bc_{(0)} \otimes c_{(1)}) = bc_{(0)} \otimes c_{(1)} \otimes c_{(2)} = (\kappa_r \otimes H)(b \otimes c_{(0)} \otimes c_{(1)}) = (\kappa_r \otimes H)\delta(b \otimes c)$. □

Cerramos esta sección con algunas propiedades útiles de $\gamma(h) = l_i(h) \otimes r_i(h)$.

Proposición 2.12. *Si κ_r es biyectiva, entonces γ está definida y cumple las siguientes relaciones:*

- (R1) $l_i(h)r_i(h) = \varepsilon(h)1_A$
- (R2) $l_i(h) \otimes r_i(h)_{(0)} \otimes r_i(h)_{(1)} = l_i(h_{(1)}) \otimes r_i(h_{(1)}) \otimes h_{(2)}$
- (R3) $l_i(h)_{(0)} \otimes r_i(h) \otimes l_i(h)_{(1)} = l_i(h_{(2)}) \otimes r_i(h_{(2)}) \otimes S(h_{(1)})$
- (R4) $l_i(gh) \otimes r_i(gh) = l_i(h)l_j(g) \otimes r_j(g)r_i(h)$

- (R5) $a_{(0)}l_i(a_{(1)}) \otimes r_i(a_{(1)}) = 1_A \otimes a$

Demostración. Probamos cada relación por separado:

- **(R1)** Notamos que $\kappa_r\left(l_i(h) \otimes r_i(h)\right) = 1 \otimes h$, luego $l_i(h)r_i(h)_{(0)} \otimes r_i(h)_{(1)} = 1 \otimes h$. Aplicando $A \otimes \varepsilon$ a ambos lados de la igualdad obtenemos (R1).
- **(R2)** κ_r es por el teorema 2.11 un morfismo en $\mathcal{M}_A^H$, luego su inversa también lo es. Se sigue entonces que $l_i(h) \otimes r_i(h)_{(0)} \otimes r_i(h)_{(1)} = \delta(l_i(h) \otimes r_i(h)) = \delta(\kappa_r^{-1}(1 \otimes h)) = (\kappa_r^{-1} \otimes H)\delta(1 \otimes h) = (\kappa_r^{-1} \otimes H)(1 \otimes h_{(1)} \otimes h_{(2)}) = l_i(h_{(1)}) \otimes r_i(h_{(1)}) \otimes h_{(2)}$.
- **(R3)** κ_r es por el teorema 2.11 un morfismo en ${}_A\mathcal{M}^H$, luego su inversa también lo es. De aquí se sigue que $l_i(h)_{(0)} \otimes r_i(h) \otimes l_i(h)_{(1)} = \delta(\kappa_r^{-1}(1 \otimes h)) = (\kappa_r^{-1} \otimes H)\delta(1 \otimes h) = (\kappa_r^{-1} \otimes H)(1 \otimes h_{(2)} \otimes S(h_{(1)})) = l_i(h_{(2)}) \otimes r_i(h_{(2)}) \otimes S(h_{(1)})$.
- **(R4)** Observamos que, como $l_j(g)r_j(g)_{(0)} \otimes r_j(g)_{(1)} = 1 \otimes g$, la relación se obtiene de aplicar κ_r^{-1} a ambos extremos de la siguiente igualdad: $\kappa_r\left(l_i(h)l_j(g) \otimes r_j(g)r_i(h)\right) = l_i(h)l_j(g)r_j(g)_{(0)}r_i(h)_{(0)} \otimes r_j(g)_{(1)}r_i(h)_{(1)} = l_i(h)1r_i(h)_{(0)} \otimes gr_i(h)_{(1)} = l_i(h)r_i(h)_{(0)} \otimes gr_i(h)_{(1)} = 1 \otimes gh$.
- **(R5)** Utilizando de nuevo que $l_j(g)r_j(g)_{(0)} \otimes r_j(g)_{(1)} = 1 \otimes g$ y aplicando κ_r^{-1} a ambos extremos de la siguiente expresión se sigue la relación: $\kappa_r\left(a_{(0)}l_i(a_{(1)}) \otimes r_i(a_{(1)})\right) = a_{(0)}l_i(a_{(1)})r_i(a_{(1)})_{(0)} \otimes r_i(a_{(1)})_{(1)} = a_{(0)} \otimes a_{(1)} = \kappa_r(1 \otimes a)$.

□

2.2. Extensiones fielmente planas

Al igual que en la teoría de Galois clásica y en nuestro capítulo 1, no cualquier extensión es adecuada para el teorema fundamental. Es ahí donde entraba el concepto de extensión separable, que la teoría de Galois-Hopf sustituye por el de extensión fielmente plana. A continuación introducimos la definición y propiedades de este tipo de extensiones.

Definición 2.13 (Sucesión exacta)**.** Una sucesión de R-módulos

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_n$$

es **exacta** si $\ker f_{i+1} = \operatorname{Im} f_i$, para cada $i = 1, \ldots, n-1$.

Sea $F : \mathcal{M}_R \to \mathcal{M}_R$ un functor. El resultado de aplicar F a una sucesión de R-módulos exacta es

$$F(M_0) \xrightarrow{F(f_1)} F(M_1) \xrightarrow{F(f_2)} \cdots \xrightarrow{F(f_n)} F(M_n),$$

que no es exacta en general. Esto nos lleva a la siguiente definición.

Definición 2.14 (Functor exacto)**.** Sea $F : \mathcal{M}_R \to \mathcal{M}_R$ un functor, y sean $\mathcal{S}$ una sucesión de R-módulos y $F(\mathcal{S})$ su imagen por F. Diremos que F es:

- **Exacto** si siempre que $\mathcal{S}$ es exacta, también lo es $F(\mathcal{S})$.
- **Fielmente exacto** si $\mathcal{S}$ es exacta si y solo si lo es $F(\mathcal{S})$.

Definición 2.15 (Módulo plano)**.** Sea A un R-módulo, y sea $F_A : \mathcal{M}_R \to \mathcal{M}_R$ el functor dado por $F_A(M) = M \otimes_R A$. Diremos que A es:

- **Plano** si F_A es exacto.
- **Fielmente plano** si F_A es fielmente exacto.

Adicionalmente, diremos que la extensión A/R es (fielmente) plana si A es un R-módulo (fielmente) plano.

Proposición 2.16. *Si A es un R-módulo plano y $f : M \to N$ es un homomorfismo, entonces* $\ker(f \otimes A) = (\ker f) \otimes A$.

Demostración. La sucesión $\ker f \xrightarrow{\iota} M \xrightarrow{f} N$ es trivialmente exacta. Como el módulo A es plano, $(\ker f) \otimes A \xrightarrow{\iota \otimes A} M \otimes A \xrightarrow{f \otimes A} N \otimes A$ también es exacta, luego $\ker(f \otimes A) = \iota(\ker f \otimes A) = (\ker f) \otimes A$. □

Proposición 2.17. *Si A es un R-módulo fielmente plano, $N \leq M \in \mathcal{M}_R$ y $N \otimes A = M \otimes A$, entonces $N = M$.*

Demostración. La sucesión $N \xrightarrow{\iota} M \to 0$ induce la sucesión $N \otimes A \xrightarrow{\iota} M \otimes A \to 0 \otimes A = 0$, que es exacta por hipótesis. Como A es fielmente plano, la primera sucesión es también exacta, luego $\iota(N) = M$ y concluimos que $M = N$. □

Nos conviene tener en cuenta que dado un H-comódulo a derecha M, para la coacción codiagonal se verifica la siguiente relación:

(R6) $\quad x_i \otimes y_i \in (M \otimes N)^{\mathrm{co}H}$ si y solo si $x_i \otimes y_{i(0)} \otimes y_{i(1)} = x_{i(0)} \otimes y_i \otimes S(x_{i(1)})$.

En lo que resta de sección, supondremos que A/R es una H-extensión de Galois, con aplicación de Galois κ_r. Estudiaremos a continuación las propiedades que garantiza una extensión fielmente plana A/R.

Proposición 2.18. *Sea $M \in \mathcal{M}^H$ y A un H-comódulo álgebra plano. Entonces:*

$$M^{coH} \otimes A = \left\{ \sum x_i \otimes a_i \;\middle|\; \sum x_{i(0)} \otimes x_{i(1)} \otimes a_i = \sum x_i \otimes 1_H \otimes a_i \right\}.$$

Demostración. La sucesión $M^{\mathrm{co}H} \hookrightarrow M \xrightarrow{\delta - M \otimes 1_H} M \otimes H$ es trivialmente exacta. Como A es plano, la sucesión $M^{\mathrm{co}H} \otimes A \hookrightarrow M \otimes A \xrightarrow{\delta \otimes A - M \otimes 1_H \otimes A} M \otimes H \otimes A$ es también exacta, de donde se sigue el resultado. □

Teorema 2.19. *Si A es fielmente plano y $M \in \mathcal{M}_A^H$, entonces la siguiente aplicación es un R-isomorfismo:*

$$\begin{array}{rccc} \kappa_M : & M \otimes A & \longrightarrow & M \otimes H \\ & x \otimes a & \longmapsto & xa_{(0)} \otimes a_{(1)} \end{array}.$$

Demostración. Como A/R es una H-extensión de Galois, κ_r es biyectiva. Como $M \equiv M \otimes_A A$, se sigue que:

$$\begin{array}{ccccccc} M \otimes_R A & \equiv & M \otimes_A A \otimes_R A & \xleftrightarrow{M \otimes \kappa_r} & M \otimes_A A \otimes_R H & \equiv & M \otimes_R H \\ x \otimes a & \equiv & x \otimes 1 \otimes a & \longleftrightarrow & x \otimes a_{(0)} \otimes a_{(1)} & \equiv & xa_{(0)} \otimes a_{(1)} \end{array}.$$

□

Para el siguiente teorema (tomado de [7, 488-516]) consideraremos, aparte del recién definido $\kappa_M : M \otimes A \to M \otimes H$, los dos siguientes R-isomorfismos:

$$\begin{array}{rccc} \beta: & M\otimes H\otimes A & \longrightarrow & M\otimes H\otimes H \\ & x\otimes h\otimes a & \longmapsto & xa_{(0)}\otimes h\otimes a_{(1)} \end{array} \qquad \begin{array}{rccc} \kappa_H: & H\otimes H & \longrightarrow & H\otimes H \\ & h\otimes h' & \longmapsto & hh'_{(1)}\otimes h'_{(2)} \end{array}$$

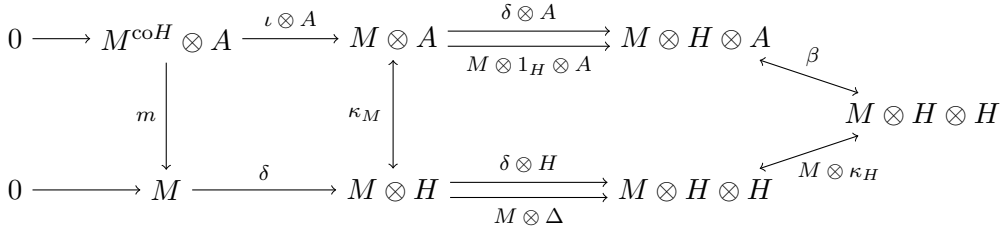
Notamos que la inversa de κ_H está dada por $h \otimes h' \mapsto hS(h'_{(1)}) \otimes h'_{(2)}$.

Teorema 2.20. *Sea A fielmente plano y $M \in \mathcal{M}_A^H$. Entonces la aplicación*

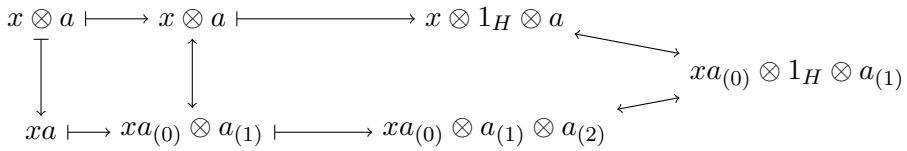
$$\begin{array}{ccc} M^{coH}\otimes A & \longrightarrow & M \\ x\otimes a & \longmapsto & xa \end{array}$$

es un isomorfismo en $\mathcal{M}_A^H$.

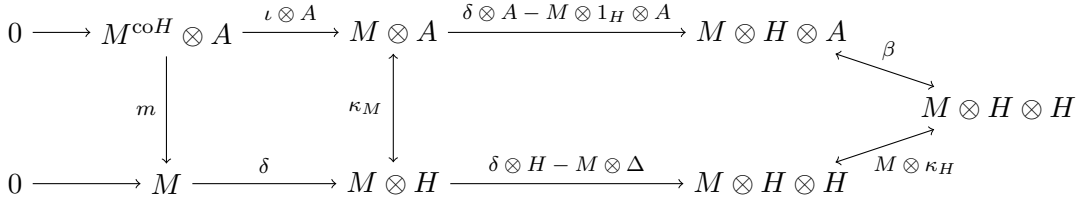
Demostración. Consideremos el siguiente diagrama, donde $m(x \otimes a) = xa$:



Notamos que el diagrama es conmutativo tanto si tomamos las flechas superiores como si tomamos las inferiores (en los lugares donde se presentan dos flechas):



Si tomamos la resta de la aplicación de arriba menos la de abajo (en los lugares donde hay dos flechas) obtenemos un diagrama que también es conmutativo:



Notamos que:

- **La fila inferior es exacta**: $x_i \otimes h_i \in \ker(\delta \otimes H - M \otimes \Delta)$ equivale a que $x_{i(0)} \otimes x_{i(1)} \otimes h_i = x_i \otimes h_{i(1)} \otimes h_{i(2)}$. Aplicando ε al tercer factor se sigue que $x_i \otimes h_i = \varepsilon(h_i)x_{i(0)} \otimes x_{i(1)} \in \operatorname{Im}\delta$. Así, $\operatorname{Im}\delta \subseteq \ker(\delta \otimes H - M \otimes \Delta) \subseteq \operatorname{Im}\delta$, luego es exacta en $M \otimes H$. La exactitud en M se debe a que si $\delta(x) = 0$ entonces $x_{(0)} \otimes x_{(1)} = 0 \otimes 0$, de donde se obtiene que $x = 0$ aplicando $M \otimes \varepsilon$.

- **La fila superior es exacta**: inmediato, ya que $0 \to M^{\mathrm{co}H} \xrightarrow{\iota} M \xrightarrow{\delta - M\otimes 1_H} M \otimes H$ es exacta y A es plano.

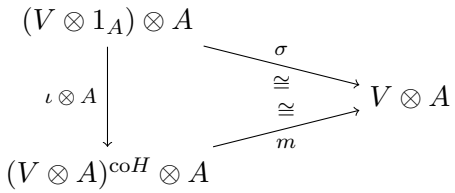
Ahora, utilizando que las filas son exactas y que dos de los caminos verticales (los que utilizan κ_M, β, $M \otimes \kappa_H$) son isomorfismos, podemos comprobar que $m(x_i \otimes a_i) = 0$ también lo es. En primer lugar, si $m(x_i \otimes a_i) = 0$, entonces $\kappa_M(\iota \otimes A)(x_i \otimes a_i) = \delta m(x_i \otimes a_i) = 0$. Como κ_M es un isomorfismo por el teorema 2.19, $\iota \otimes A(x_i \otimes a_i) = 0$, y como $\iota \otimes A$ es inyectiva concluimos que $x_i \otimes a_i = 0$. Por otro lado, dado $x \in M$ se tiene por la biyectividad de κ_M que $\delta(x) = \kappa_M(x_i \otimes a_i)$ para cierto $x_i \otimes a_i \in M \otimes A$. Como el diagrama conmuta y $\delta(x) \in \ker(\delta \otimes H - M \otimes \Delta)$,

$$x_i \otimes a_i \in \ker(\delta \otimes A - M \otimes 1_H \otimes A) = (\iota \otimes A)(M^{\mathrm{co}H} \otimes A) = M^{\mathrm{co}H} \otimes A.$$

Esto implica que $\delta m(x_i \otimes a_i) = \kappa_M(x_i \otimes a_i) = \delta(x)$. δ es inyectiva, luego $x = m(x_i \otimes a_i)$. Queda así probada la biyectividad de m. □

Teorema 2.21. *Si A es fielmente plano y $V \in \mathcal{M}_R$, entonces $(V \otimes_R A)^{coH} = V \otimes 1_A$.*

Demostración. Tomando $M := (V \otimes_R A)$ en el isomorfismo del teorema 2.20 se sigue que la aplicación $m : (V \otimes A)^{\mathrm{co}H} \otimes A \to V \otimes A$ dada por $m(v' \otimes a' \otimes b) = v' \otimes a'b$ es un isomorfismo. Tomando el isomorfismo $\sigma : (V \otimes 1_A) \otimes A \to V \otimes A$ dado por $\sigma(v \otimes 1_A \otimes b) = v \otimes b$,



luego $(\iota \otimes A) : (V \otimes 1_A) \otimes A \to (V \otimes A)^{\mathrm{co}H} \otimes A$ es también un isomorfismo. En particular, $\iota \otimes A$ es epimorfismo, así que $V \otimes 1_A \otimes A \xrightarrow{\iota \otimes A} (V \otimes A)^{\mathrm{co}H} \otimes A \to 0$ es exacta. Como A es fielmente plano, se sigue que $V \otimes 1_A \xrightarrow{\iota} (V \otimes A)^{\mathrm{co}H} \to 0$ es exacta. Como ι es epimorfismo, concluimos que $(V \otimes A)^{\mathrm{co}H} = V \otimes 1_A$. □

Corolario 2.22. *Si A es fielmente plano, las aplicaciones*

$$\begin{array}{rccc} \varphi: & \mathcal{M}_A^H & \longrightarrow & \mathcal{M}_R \\ & M & \longmapsto & M^{coH} \end{array} \qquad \begin{array}{rccc} \psi: & \mathcal{M}_R & \longrightarrow & \mathcal{M}_A^H \\ & V & \longmapsto & V \otimes A \end{array}$$

cumplen que:

1. $\psi\varphi(M) = \psi(M^{coH}) = M^{coH} \otimes A \cong M$.
2. $\varphi\psi(V) = \varphi(V \otimes A) = (V \otimes A)^{coH} = V \otimes 1_A \cong V$.

Por último, veamos dos observaciones interesantes acerca de las extensiones fielmente planas.

Observación 2.23. Si A/R es una H-extensión de Galois fielmente plana entonces $A \otimes A \cong A \otimes H \cong H \otimes A$. Como A es fielmente plano se sigue fácilmente que $A \otimes A$ y $H \otimes A$ también lo son. Así, que una sucesión $M_0 \otimes H \xrightarrow{f_1 \otimes H} \cdots \xrightarrow{f_n \otimes H} M_n \otimes H$ sea exacta equivale a que $M_0 \otimes H \otimes A \xrightarrow{f_1 \otimes H \otimes A} \cdots \xrightarrow{f_n \otimes H \otimes A} M_n \otimes H \otimes A$ lo sea. Como $H \otimes A$ es también fielmente plano, equivale a que $M_0 \xrightarrow{f_1} \cdots \xrightarrow{f_n} M_n$ sea exacta. Queda así probado que H/R es fielmente plano si A lo es.

Observación 2.24. Si A/R es fielmente plana, $M, N \in \mathcal{M}_A^H$ y $f : M \to N$ es un homomorfismo en $\mathcal{M}_A^H$,

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ \wr\| & & \wr\| \\ M^{\mathrm{co}H} \otimes A & \xrightarrow[f|_{M^{\mathrm{co}H}}]{} & N^{\mathrm{co}H} \otimes A \end{array}$$

luego f es epimorfismo si y solo si $f|_{M^{\mathrm{co}H}}$ lo es.

2.3. (L, H)-Extensiones bi-Galois

Definición 2.25 ((L, H)-bicomódulo)**.** Un (L, H)**-bicomódulo** A es un L-comódulo a izquierda (mediante $\delta_l : A \to L \otimes A$) y H-comódulo a derecha (mediante $\delta_r : A \to A \otimes H$) tal que $(L \otimes \delta_r) \circ \delta_l = (\delta_l \otimes H) \circ \delta_r$.

Definición 2.26 ((L, H)-Extensión bi-Galois)**.** A/R es una (L, H)**-extensión bi-Galois** si A es un (L, H)-bicomódulo tal que A/R es una L-extensión de Galois a izquierda y una H-extensión de Galois a derecha.

2.4. El álgebra de Hopf $L(A, H)$

En lo que sigue, supondremos que A/R es una H-extensión de Galois fielmente plana. Denotaremos por δ a la aplicación que da a A su estructura de H-comódulo y por κ_r a su correspondiente aplicación de Galois. En esta sección veremos cómo para toda H-extensión de Galois existe, salvo isomorfismo, una única álgebra de Hopf adicional L que controla la extensión por la izquierda, necesaria para el teorema fundamental. En particular, vamos a ver cómo este álgebra de Hopf es

$$\boxed{L(A, H) := (A \otimes A)^{\mathrm{co}H}}$$

Denotaremos los elementos de $L(A, H)$ de la forma $a' \otimes a''$, entendiendo que hemos omitido el sumatorio. De la defínción de $L(A, H)$ obtenemos directamente la siguiente propiedad:

$$\text{(R7)} \quad a'_{(0)} \otimes a''_{(0)} \otimes a'_{(1)} a''_{(1)} = a' \otimes a'' \otimes 1.$$

A continuación, repasaremos punto por punto cada uno de los resultados necesarios para ver que esta $L(A, H)$ es, salvo isomorfismo, la única álgebra de Hopf tal que A/R es una (L, H)-extensión bi-Galois. Los razonamientos de esta sección se basan en [11, 3797-3825] y [13, 53-70].

2.4.1. Estructura de álgebra de Hopf de $L(A, H)$

Estructura de álgebra de $L(A, H)$

Proposición 2.27. *$L(A, H)$ es una subálgebra de $A \otimes A^{op}$.*

Demostración. Observamos que, para $a' \otimes a'', b' \otimes b'' \in L(A, H)$,

$$\delta(a' \otimes a'' \cdot b' \otimes b'') = \delta(a'b' \otimes b''a'') = a'_{(0)} b'_{(0)} \otimes b''_{(0)} a''_{(0)} \otimes a'_{(1)} b'_{(1)} b''_{(1)} a''_{(1)}.$$

Utilizando la identidad (R7) se sigue entonces que $\delta(a' \otimes a'' \cdot b' \otimes b'') = a'_{(0)} b' \otimes b'' a''_{(0)} \otimes a'_{(1)} a''_{(1)} = a'b' \otimes b''a'' \otimes 1$. Así, $a'b' \otimes b''a'' \in L(A, H)$, luego $L(A, H)$ es cerrado por el producto de $A \otimes A^{\mathrm{op}}$. $\square$

Estructura de biálgebra de $L(A,H)$

Para dar de forma ordenada estructura de coálgebra (y posteriormente de biálgebra) a $L(A,H)$ son necesarios algunos resultados previos. Para abreviar, L denotará $L(A,H)$.

Lema 2.28. *Sea $V \in \mathcal{M}_R$ y $A \otimes A$ considerado en $\mathcal{M}_A^H$ mediante la coacción codiagonal. Las siguientes dos aplicaciones son biyecciones:*

$$\begin{array}{rccl} T: & \mathcal{M}^H(A, V\otimes A) & \longrightarrow & \mathcal{M}_A^H(A\otimes A, V\otimes A) \\ & \phi & \longmapsto & T(\phi): a\otimes b \mapsto \phi(a)b \end{array}$$

$$\begin{array}{rccl} B: & \mathcal{M}_A^H(A\otimes A, V\otimes A) & \longrightarrow & \mathcal{M}_R((A\otimes A)^{coH}, V) \\ & g & \longmapsto & B(g) \ \ tal\ que \ \ g(a'\otimes a'') = B(g)(a'\otimes a'')\otimes 1 \end{array}$$

Demostración. Lo demostramos por pasos:

- **Veamos que T está bien definida y es biyectiva**:

  Dado $\phi \in \mathcal{M}^H(A, V\otimes A)$, se comprueba fácilmente que $T(\phi)(a\otimes b\cdot c) = T(\phi)(a\otimes (bc)) = \phi(a)bc = T(\phi)(a\otimes b)\cdot c$. Por otro lado, usando que $\delta\phi = (\phi\otimes H)\delta$ se sigue que $T(\phi)\in \mathcal{M}_A^H(A\otimes A, V\otimes A)$ ya que

  $$\begin{aligned}(T(\phi)\otimes H)\delta(a\otimes b) &= (T(\phi)\otimes H)(a_{(0)}\otimes b_{(0)}\otimes a_{(1)}b_{(1)}) = \phi(a_{(0)})b_{(0)}\otimes a_{(1)}b_{(1)} \\ &= \phi(a)_{(0)}b_{(0)}\otimes \phi(a)_{(1)}b_{(1)} = \delta(\phi(a)b) = \delta\circ T(\phi)(a\otimes b)\end{aligned}$$

  Ahora definimos (abusando de notación, pues aún no hemos probado la existencia de T^{-1}) la aplicación $T^{-1}(\varphi)(a) = \varphi(a\otimes 1)$, para $\varphi\in\mathcal{M}_A^H(A\otimes A, V\otimes A)$. Como $\delta\varphi = (\varphi\otimes H)\delta$, entonces $\delta(T^{-1}(\varphi)(a)) = \delta(\varphi(a\otimes 1)) = (\varphi\otimes H)\delta(a\otimes 1) = (\varphi\otimes H)(a_{(0)}\otimes 1\otimes a_{(1)}) = \varphi(a_{(0)}\otimes 1)\otimes a_{(1)} = (T^{-1}(\varphi)\otimes H)\delta(a)$, luego $T^{-1}(\varphi)\in\mathcal{M}^H(A, V\otimes A)$. Además,

  $$\begin{cases} T(T^{-1}(\varphi))(a\otimes b) = T^{-1}(\varphi)(a)b = \varphi(a\otimes 1)b = \varphi(a\otimes b), \text{ luego } T(T^{-1}(\varphi)) = \varphi \\ \\ T^{-1}(T(\phi))(a) = T(\phi)(a\otimes 1) = \phi(a)1 = \phi(a), \text{ luego } T^{-1}(T(\phi)) = \phi \end{cases}$$

  Queda así probado que T está bien definida y es biyectiva.

- **Veamos que $B(g)\in\mathcal{M}_R((A\otimes A)^{\mathbf{co}H}, V)$**:

  Si $g\in\mathcal{M}_A^H(A\otimes A, V\otimes A)$, entonces $g((A\otimes A)^{\mathrm{co}H}) \subseteq (V\otimes A)^{\mathrm{co}H} = V\otimes 1$. Se sigue que, para $a'\otimes a''\in (A\otimes A)^{\mathrm{co}H}$, $g(a'\otimes a'') = B(g)(a'\otimes a'')\otimes 1_A$ para cierta aplicación $B(g)\in\mathcal{M}_R((A\otimes A)^{\mathrm{co}H}, V)$, que es la que consideramos. Para probar la biyectividad, dada $g_c\in\mathcal{M}_R((A\otimes A)^{\mathrm{co}H}, V)$ definimos sobre $A\otimes A = (A\otimes A)^{\mathrm{co}H}A \cong (A\otimes A)^{\mathrm{co}H}\otimes A$ (teorema 2.20 con $M = A\otimes A$) a $B^{-1}(g_c)(a'\otimes a''\cdot b) := g_c(a'\otimes a'')\otimes b$. Vemos que:

  - $B^{-1}(g_c)\in\mathcal{M}_A^H(A\otimes A, V\otimes A)$: Por un lado, $B^{-1}(g_c)(a'\otimes a''bc) = g_c(a'\otimes a'')\otimes bc = B^{-1}(g_c)(a'\otimes a''b)c$. Por otro lado, $\delta B^{-1}(g_c)(a'\otimes a''b) = \delta(g_c(a'\otimes a'')\otimes b) = g_c(a'\otimes a'')\otimes b_{(0)}\otimes b_{(1)} = (B^{-1}(g_c)\otimes H)\delta(a'\otimes a''b)$.
  - $B(B^{-1}(g_c))(a'\otimes a'')\otimes 1_A = B^{-1}(g_c)(a'\otimes a'') = g_c(a'\otimes a'')\otimes 1_A$, luego $B(B^{-1}(g_c)) = g_c$.
  - $B^{-1}(B(g))(a'\otimes a''b) = B(g)(a'\otimes a'')\otimes b = (B(g)(a'\otimes a'')\otimes 1)b = g(a'\otimes a'')b = g(a'\otimes a''b)$, luego $B^{-1}(B(g)) = g$.

□

El siguiente resultado será útil en la construcción de la comultiplicación Δ de L y la demostración de la unicidad de L para (L,H)-extensiones bi-Galois A/R.

Teorema 2.29. *Sea A/R una H-extensión de Galois fielmente plana y $L := L(A,H)$. Existe una aplicación $\delta' \in \mathcal{M}^H(A, L\otimes A)$ definida por $\delta'(a) = a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(1)})$ que verifica la siguiente propiedad universal:*

- *Dadas $V \in \mathcal{M}_R$ y $\phi \in \mathcal{M}^H(A, V\otimes A)$, existe una única aplicación R-lineal $f : L \to V$ tal que $\phi = (f\otimes A)\delta'$. Además, esta aplicación cumple que $f(a'\otimes a'')\otimes 1_A = \phi(a')a''$.*

Demostración. Siguiendo la notación del lema 2.28,

$$\mathcal{M}^H(A, V\otimes A) \xrightarrow{T} \mathcal{M}_A^H(A\otimes A, V\otimes A) \xrightarrow{B} \mathcal{M}_R(L,V).$$

Para $V := L$, consideremos $\delta' := T^{-1}B^{-1}(id_L)$. Comprobamos utilizando la relación (R1) que $T^{-1}B^{-1}(id_L)(a) = B^{-1}(id_L)(a\otimes 1) = id_L(a_{(0)}\otimes l_i(a_{(1)}))\otimes r_i(a_{(1)}) = a_{(0)}\otimes l_i(a_{(1)})\otimes r_i(a_{(1)})$, luego la fórmula de δ' coincide con la propuesta en el enunciado. Veamos ahora que esta aplicación verifica la propiedad universal. Dados $V \in \mathcal{M}_R$ y $g \in \mathcal{M}_R(L,V)$, notamos que

$$T^{-1}B^{-1}(g)(a) = B^{-1}(g)(a\otimes 1) = g(a_{(0)}\otimes l_i(a_{(1)}))\otimes r_i(a_{(1)}) = (g\otimes A)\delta'(a).$$

Se sigue que $T^{-1}B^{-1}(g) = (g\otimes A)\delta'$, que implica que $g = BT((g\otimes A)\delta')$. Ahora, dado $\phi \in \mathcal{M}^H(A, V\otimes A)$, $\phi = T^{-1}B^{-1}(TB(\phi)) = (TB(\phi)\otimes A)\delta'$. Si definimos $f := TB(\phi)$ se tiene que existe $f \in \mathcal{M}_R(L,V)$ tal que $\phi = (f\otimes A)\delta'$. Además, si existe otra $g \in \mathcal{M}_R(L,V)$ tal que $\phi = (g\otimes A)\delta'$, necesariamente se tendrá que $g = BT((g\otimes A)\delta') = BT(\phi) = f$. Queda con esto probada la unicidad de f. Además, por la definición de T y B,

$$f(a'\otimes a'')\otimes 1 = BT(\phi)(a'\otimes a'')\otimes 1 = T(\phi)(a'\otimes a'') = \phi(a')a''.$$

□

La siguiente proposición (de la cual ya hemos demostrado una parte) servirá para garantizar que la comultiplicación Δ que construiremos para L es homomorfismo de álgebras.

Proposición 2.30. *Sea A/R H-extensión de Galois fielmente plana y $L := L(A,H)$.*

1. *L es subálgebra de $A\otimes A^{op}$ y $\delta' : A \to L\otimes A$ es homomorfismo de álgebras.*
2. *Si en la propiedad universal V es álgebra y ϕ es homomorfismo de álgebras, entonces la aplicación f tal que $\phi = (f\otimes A)\delta'$ es también un homomorfismo de álgebras.*

Demostración. En la proposición 2.27 hemos probado que $L \leq A\otimes A^{\mathrm{op}}$. Utilizando la relación (R4) y denotando en este caso por $\cdot$ al producto de $A\otimes A^{\mathrm{op}}$ comprobamos que δ' es homomorfismo de álgebras:

$$\begin{aligned}\delta'(ab) &= a_{(0)}b_{(0)}\otimes l_i(a_{(1)}b_{(1)})\otimes r_i(a_{(1)}b_{(1)}) \overset{(R4)}{=} a_{(0)}b_{(0)}\otimes l_i(b_{(1)})l_i(a_{(1)})\otimes r_i(a_{(1)})r_i(b_{(1)})\\ &= \Big((a_{(0)}\otimes l_i(a_{(1)}))\otimes r_i(a_{(1)})\Big)\cdot\Big((b_{(0)}\otimes l_i(b_{(1)}))\otimes r_i(b_{(1)})\Big) = \delta'(a)\delta'(b).\end{aligned}$$

Demostremos ahora el apartado 2. Si suponemos las hipótesis y denotamos $\phi(c) = \sum c_V\otimes c_A$, podemos usar que $f(a'\otimes a'')\otimes 1 = \phi(a')a''$ para ver que

$$\begin{aligned}f(a'b'\otimes b''a'')\otimes 1_A = \phi(a'b')b''a'' = \phi(a')\phi(b')b''a'' = \phi(a')f(b'\otimes b'')\otimes a'' =\\ = \sum a'_V f(b'\otimes b'')\otimes a'_A a'' = f(a'\otimes a'')f(b'\otimes b'')\otimes 1.\end{aligned}$$

Se sigue así que $f(a'b'\otimes b''a'') = f(a'\otimes a'')f(b'\otimes b'')$, completando la prueba. □

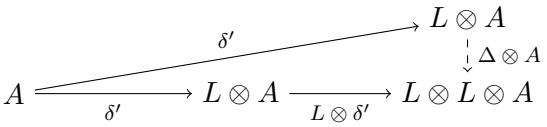
Tras estos resultados podemos finalmente dar a $L(A,H)$ estructura de biálgebra.

Teorema 2.31. *Sea A/R una H-extensión de Galois fielmente plana. Con el producto heredado de $A \otimes A^{op}$ y las aplicaciones Δ y ε dadas por*

$$\begin{aligned} \Delta(a' \otimes a'') &:= a'_{(0)} \otimes l_i(a'_{(1)}) \otimes r_i(a'_{(1)}) \otimes a'', \\ \varepsilon(a' \otimes a'') &:= a'a'' \in R1_A, \end{aligned}$$

$L(A,H)$ es una biálgebra.

Demostración. Comencemos probando que Δ es una comultiplicación para L. Para obtener con mayor facilidad las propiedades de Δ, la definiremos a partir de δ' y su propiedad universal. Como $\delta' \in \mathcal{M}^H(A, L \otimes A)$, por la propiedad universal existe una única $\Delta : L \to L \otimes L$ que hace conmutar al siguiente diagrama:

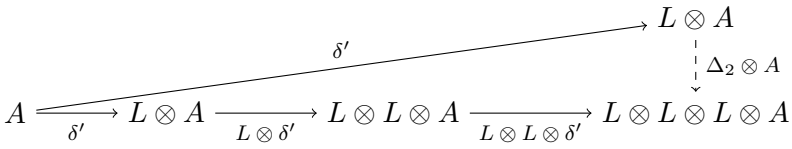


Por el teorema 2.29, $\Delta(a' \otimes a'') \otimes 1 = (L \otimes \delta')\delta'(a')a'' = (L \otimes \delta')(a'_{(0)} \otimes l_i(a'_{(1)}) \otimes r_i(a'_{(1)}))a''$. Aplicando $L \otimes A \otimes \kappa_r$ a ambos lados de esta expresión obtenemos

$$(L \otimes A \otimes \kappa_r)(\Delta(a' \otimes a'') \otimes 1) = \Delta(a' \otimes a'') \otimes 1_H \tag{2.1}$$

$$\begin{aligned} &(L \otimes A \otimes \kappa_r)\left((L \otimes \delta')(a'_{(0)} \otimes l_i(a'_{(1)}) \otimes r_i(a'_{(1)}))a''\right) \\ &\quad = a_{(0)} \otimes l_i(a'_{(1)}) \otimes (A \otimes \kappa_r)(\delta'(r_i(a'_{(1)}))a'') \\ &\quad = a_{(0)} \otimes l_i(a'_{(1)}) \otimes \left(r_i(a'_{(1)})_{(0)} \otimes a''_{(0)} \otimes r_i(a'_{(1)})_{(1)} a''_{(1)}\right) \end{aligned} \tag{2.2}$$

y aplicando ε al último factores de las expresiones (2.1) y (2.2) se sigue que esta Δ coincide con la definición dada en el teorema. Para probar que es coasociativa volvemos a utilizar la propiedad universal de δ', pero esta vez con el diagrama

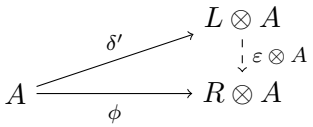


Obtendríamos así una única Δ_2 para la que el diagrama es conmutativo. Notamos que

$$\begin{aligned} (\Delta_2 \otimes A)\delta' &= (L \otimes L \otimes \delta')(L \otimes \delta')\delta' = (L \otimes L \otimes \delta')(\Delta \otimes A)\delta' \\ &= (\Delta \otimes \delta')\delta' = (\Delta \otimes L \otimes A)(L \otimes \delta')\delta' \\ &= (\Delta \otimes L \otimes A)(\Delta \otimes A)\delta' = ((\Delta \otimes L)\Delta \otimes A)\delta' \end{aligned} \tag{2.3}$$

$$\begin{aligned} (\Delta_2 \otimes A)\delta' &= (L \otimes L \otimes \delta')(L \otimes \delta')\delta' = (L \otimes (L \otimes \delta')\delta')\delta' \\ &= (L \otimes (\Delta \otimes A)\delta')\delta' = (L \otimes \Delta \otimes A)(L \otimes \delta')\delta' \\ &= (L \otimes \Delta \otimes A)(\Delta \otimes A)\delta' = ((L \otimes \Delta)\Delta \otimes A)\delta' \end{aligned} \tag{2.4}$$

Combinando los resultados de 2.3 y 2.4, concluimos que $(\Delta \otimes L)\Delta = (L \otimes \Delta)\Delta$, es decir, que Δ es coasociativa. Pasemos ahora a probar que ε es una counidad para L. De forma similar a lo hecho con Δ, definimos ε a través de la propiedad universal de δ'. Tomando $\phi(a) = 1 \otimes a$, aseguramos la existencia de un único homomorfismo de álgebras $\varepsilon : L \to R$ tal que el siguiente diagrama conmuta



Además $\varepsilon(a' \otimes a'') \otimes 1_A = \phi(a')a'' = 1 \otimes a'a''$, de donde multiplicando los factores se obtiene que la expresión de este ε es justo la del enunciado. Notamos ahora que, por la unicidad en la propiedad universal, $(L \otimes \varepsilon)\Delta$ es la identidad en L ya que

$$\begin{aligned}((L \otimes \varepsilon)\Delta \otimes A)\,\delta' &= (L \otimes \varepsilon \otimes A)(\Delta \otimes A)\delta' = (L \otimes \varepsilon \otimes A)(L \otimes \delta')\delta' \\ &= \left(L \otimes (\varepsilon \otimes A)\delta'\right)\delta' \;\equiv\; \delta'.\end{aligned}$$

Por último, dado $a' \otimes a'' \in L$ se tiene $(\varepsilon \otimes L)\Delta(a' \otimes a'') = a'_{(0)} l_i(a'_{(1)}) \otimes r_i(a'_{(1)}) \otimes a'' = 1 \otimes a' \otimes a'' \equiv a' \otimes a''$, luego $(\varepsilon \otimes L)\Delta = (L \otimes \varepsilon)\Delta = id_L$. Queda así probado que (L, Δ, ε) es una coálgebra. □

La antípoda de $L(A,H)$

Ya hemos probado que $L(A,H)$ tiene estructura de biálgebra, por lo que solo nos falta comprobar que admite una antípoda para tener su estructura de álgebra de Hopf. Esto no es sencillo, por lo que dividiremos la demostración en varias partes.

Teorema 2.32. *Sean A/R una H-extensión de Galois fielmente plana y $L := L(A,H)$. La aplicación $S : L \to L$ definida por $S(a' \otimes a'') := a''_{(0)} \otimes l_i(a''_{(1)}) a' r_i(a''_{(1)})$ cumple que $m_L(S \otimes L)\Delta = \varepsilon 1_L$, donde m_L denota el producto de L.*

Demostración. En primer lugar, comprobamos que $S(L) \subseteq L$. Dado $a' \otimes a'' \in L$ notamos que

$$\begin{aligned}\delta S(a' \otimes a'') &= \delta\left(a''_{(0)} \otimes l_i(a''_{(1)})\; a'\; r_i(a''_{(1)})\right) \\ &= a''_{(0)(0)} \otimes l_i(a''_{(1)})_{(0)}\; a'_{(0)}\; r_i(a''_{(1)})_{(0)} \otimes a''_{(0)(1)}\; l_i(a''_{(1)})_{(1)}\; a'_{(1)}\; r_i(a''_{(1)})_{(1)} \\ &= a''_{(0)} \otimes l_i(a''_{(1)})_{(0)}\; a'_{(0)}\; r_i(a''_{(2)})_{(0)} \otimes a''_{(1)}\; l_i(a''_{(2)})\; a'_{(1)}\; r_i(a''_{(2)})_{(1)} \\ &= a''_{(0)} \otimes l_i(a''_{(1)})\; a'_{(0)}\; r_i(a''_{(1)})_{(0)} \otimes a'_{(1)}\; r_i(a''_{(1)})_{(1)} \\ &\overset{\text{R2}}{=} a''_{(0)} \otimes l_i(a''_{(1)})\; a'_{(0)}\; r_i(a''_{(1)}) \otimes a'_{(1)}\; a''_{(2)} \\ &= a''_{(0)} \otimes l_i(a''_{(1)})\; a'\; r_i(a''_{(1)}) \otimes 1 \;=\; S(a' \otimes a'') \otimes 1\end{aligned}$$

Como $\delta S(a' \otimes a'') = S(a' \otimes a'') \otimes 1 \in L \otimes A$, se sigue que $S(a' \otimes a'') \in L$ y por tanto que $S(L) \subseteq L$. Veamos ahora que $m_L(S \otimes L)\Delta = \varepsilon 1_L$:

$$\begin{aligned}S(a'_{(0)} \otimes l_i(a'_{(1)})) \cdot r_i(a'_{(1)}) \otimes a'' &= \left(l_i(a'_{(1)})_{(0)} \otimes l_j\left(l_i(a'_{(1)})_{(1)}\right) a'_{(0)} r_j\left(l_i(a'_{(1)})_{(1)}\right)\right) \cdot r_i(a'_{(1)}) \otimes a'' \\ &= l_i(a'_{(1)})_{(0)} r_i(a'_{(1)}) \otimes a'' l_j\left(l_i(a'_{(1)})_{(1)}\right) a'_{(0)} r_j\left(l_i(a'_{(1)})_{(1)}\right) \\ &\overset{\text{R3}}{=} l_i(a'_{(1)(2)}) r_i(a'_{(1)(2)}) \otimes a'' l_j\left(S(a'_{(1)(1)})\right) a'_{(0)} r_j\left(S(a'_{(1)(1)})\right) \\ &= l_i(a'_{(2)}) r_i(a'_{(2)}) \otimes a'' l_j\left(S(a'_{(1)})\right) a'_{(0)} r_j\left(S(a'_{(1)})\right) \\ &\overset{\text{R1}}{=} 1 \otimes a'' l_j\left(S(a'_{(1)})\right) a'_{(0)} r_j\left(S(a'_{(1)})\right) \\ &\overset{\text{R6}}{=} 1 \otimes a''_{(0)} l_j(a''_{(1)}) a' r_j(a''_{(1)}) \\ &\overset{\text{R5}}{=} 1 \otimes a'a'' = \varepsilon(a' \otimes a'')1 \otimes 1\end{aligned}$$

□

Este teorema no nos permite aún dar a $L(A,H)$ estructura de álgebra de Hopf, ya que solo ha demostrado una de las condiciones necesarias de S para ser una antípoda. Para demostrar la otra con la mayor claridad posible, consideramos en $\mathrm{Hom}_R(L,L)$ el **producto convolución**:

$$f * g\ (a' \otimes a'') \ := \ f\left((a' \otimes a'')_{(1)}\right)\ g\left((a' \otimes a'')_{(2)}\right).$$

Como L es asociativa y coasociativa, $\mathrm{Hom}_R(L,L)$ es una R-álgebra con este producto. Notamos que el elemento neutro es la aplicación $\varepsilon 1_L : a' \otimes a'' \mapsto \varepsilon(a' \otimes a'')1_L$, ya que $\varepsilon 1_L * g(a' \otimes a'') = \varepsilon((a' \otimes a'')_{(1)})g((a' \otimes a'')_{(2)}) = g(a' \otimes a'')$ y $f * \varepsilon 1_L = f$. Con este producto podemos reescribir los axiomas de la antípoda como

$$S * id_L = \varepsilon 1_L \quad , \quad id_L * S = \varepsilon 1_L,$$

o dicho de otra manera, que S es el inverso de id_L para el producto convolución. En el teorema 2.32 solo hemos probado que $S * id_L = \varepsilon 1_L$. Se tiene entonces que para terminar de dar la estructura de álgebra de Hopf a S nos basta con probar que id_L es invertible para el producto convolución. Esto lo logramos con el siguiente teorema tomado de [12, 83-85].

Teorema 2.33. *Sea L una biálgebra y A/R una L-extensión de Galois a izquierda fielmente plana. En tal caso, L es un álgebra de Hopf.*

Demostración. Sea $M \in \mathcal{M}_A$. Veamos que la aplicación $\pi : \mathrm{Hom}_R(L,M) \to \mathrm{Hom}_R(A,M)$ dada por $f \mapsto f(a_{(-1)})a_{(0)}$ es inyectiva. Si $\pi(f) = \pi(g)$, entonces la aplicación

$$\begin{array}{ccccc} A \otimes A & \xrightarrow{\kappa_l} & L \otimes A & \longrightarrow & M \\ a \otimes b & \longmapsto & a_{(-1)} \otimes a_{(0)}b & \longmapsto & f(a_{(-1)})a_{(0)}b = \pi(f)(a)b \end{array}$$

coincide con la obtenida a partir de g. Como κ_l es biyectiva por ser la L-extensión A/R de Galois a izquierda, se sigue que $f(z)b = g(z)b$ para todo $z \in L$, $b \in A$. Concluimos entonces que $f = g$ y por tanto que π es inyectiva. Veamos ahora que si C es una coálgebra, L un álgebra y $f : C \to L$ una aplicación tal que $\tilde{f}(c) := f(c) \otimes 1_A \in L \otimes A$ es invertible para la convolución, entonces f también lo es. Consideramos los siguientes homomorfismos de álgebras:

$$\begin{array}{rccccc} \eta_1 : & L \otimes A & \longrightarrow & L \otimes A \otimes A & \qquad \eta_2 : & L \otimes A & \longrightarrow & L \otimes A \otimes A \\ & z \otimes a & \longmapsto & z \otimes a \otimes 1 & & z \otimes a & \longmapsto & z \otimes 1 \otimes a \end{array}$$

Ahora, si $\tilde{g} \in \mathrm{Hom}(C, L \otimes A)$ es la inversa de $\tilde{f}$, entonces es claro que $\eta_i\tilde{g}$ lo es de $\eta_i\tilde{f}$ para $i = 1,2$. Como $\eta_1\tilde{f} = \eta_2\tilde{f}$, necesariamente también $\eta_1\tilde{g} = \eta_2\tilde{g}$. Así, si $\tilde{g}(c) = \tilde{g}(c)_L \otimes \tilde{g}(c)_A$, tenemos que $\tilde{g}(c)_L \otimes \tilde{g}(c)_A \otimes 1_A = \tilde{g}(c)_L \otimes 1_A \otimes \tilde{g}(c)_A$. Como A/R es fielmente plana, concluimos que $\tilde{g}(c)_A \in R1$, y se sigue que $\tilde{g}(c) = g(c) \otimes 1_A$ para cierta $g : C \to L$. Notamos que $\varepsilon(c)1_L \otimes 1_A = \tilde{g}(c_{(1)})\tilde{f}(c_{(2)}) = g(c_{(1)})f(c_{(2)}) \otimes 1_A$, luego $g(c_{(1)})f(c_{(2)}) = \varepsilon(c)1_L$; e igualmente $f(c_{(1)})g(c_{(2)}) = \varepsilon(c)1_L$. Queda así probado que g es la inversa de f para el producto convolución. Tomamos ahora la aplicación $\eta_0 : L \to L \otimes A$, dada por $z \mapsto z \otimes 1_A$, y veamos que tiene inversa por el producto convolución. En tal caso, id_L también la tendría y así L sería un álgebra de Hopf, concluyendo la demostración. Consideramos $\tilde{S} : L \to L \otimes A$, dada por $\tilde{S}(z) := r_i(z)_{(-1)} \otimes l_i(z)r_i(z)_{(0)}$. Notamos que

$$\begin{aligned} \eta_0 * \tilde{S}(z) &= z_{(1)}r_i(z_{(2)})_{(-1)} \otimes l_i(z_{(2)})r_i(z_{(2)})_{(0)} = l_i(z)_{(-1)}r_i(z)_{(-1)} \otimes l_i(z)_{(0)}r_i(z)_{(0)} \\ &= (l_i(z)r_i(z))_{(-1)} \otimes (l_i(z)r_i(z))_{(0)} = \varepsilon(z)1_L \otimes 1_A \end{aligned}$$

Ahora utilizaremos la aplicación $\pi : \mathrm{Hom}(L, L \otimes A) \to \mathrm{Hom}(A, L \otimes A)$ definida al principio de esta demostración para ver que $\tilde{S} * \eta_0 = \varepsilon(z)1_L \otimes 1_A$. Definimos:

$$\begin{aligned} f(z) &:= \tilde{S} * \eta_0(z) = r_i(z_{(1)})_{(-1)}z_{(2)} \otimes l_i(z_{(1)})r_i(z_{(1)})_{(0)} \\ g(z) &:= \varepsilon(z)1_L \otimes 1_A \end{aligned}$$

Para estas aplicaciones, observamos que

$$\begin{aligned}\pi(f)(a) &= r_i(a_{(-1)(1)})_{(-1)}a_{(-1)(2)} \otimes l_i(a_{(-1)(1)})r_i(a_{(-1)(1)})a_{(0)} \\ &= r_i(a_{(-1)})_{(-1)}a_{(0)(-1)} \otimes l_i(a_{(-1)})r_i(a_{(-1)})_{(0)}a_{(0)(0)} \\ &= \Big(r_i(a_{(-1)})a_{(0)}\Big)_{(-1)} \otimes l_i(a_{(-1)}) \Big(r_i(a_{(-1)})a_{(0)}\Big)_{(0)} = 1 \otimes a \\ \pi(g)(a) &= \varepsilon(a_{(-1)})1_L \otimes a_{(0)} = 1 \otimes a\end{aligned}$$

Queda así probado que $\pi(f) = \pi(g)$, que implica $f = g$ por la inyectividad de π. Concluimos así que $\tilde{S} * \eta_0 = \varepsilon 1_L \otimes 1_A$, con lo que η_0 es invertible para el producto convolución, terminando la demostración. □

2.4.2. A/R es una $(L(A,H),H)$-extensión bi-Galois

Ya hemos comprobado que $L(A,H)$ es un álgebra de Hopf, por lo que ahora es posible definir extensiones $L(A,H)$-Galois. En esta subsección demostraremos que, salvo isomorfismo, $L := L(A,H)$ es la única álgebra de Hopf que verifica que A/R es una (L,H)-extensión bi-Galois. El teorema siguiente aparece en [11, 3797-3825].

Teorema 2.34. *Sea A/R una H-extensión de Galois fielmente plana. Se tiene:*

1. *A/R es una $(L(A,H),H)$-extensión bi-Galois.*
2. *Si B es otra biálgebra y $\phi : A \to B \otimes A$ convierte a A/R en una extensión B-H bi-Galois, entonces existe un único isomorfismo $f : L(A,H) \to B$ de biálgebras tal que $\phi = (f \otimes A)\delta'$.*

Demostración. Denotamos $L := L(A,H)$ para abreviar. La candidata para dar estructura de L-comódulo álgebra a A es $\delta' : A \to L \otimes A$. Demostraremos el teorema por partes:

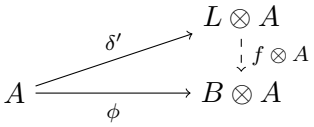
- **A es un L-comódulo álgebra**: La condición $(L \otimes \delta')\delta' = (\Delta \otimes A)\delta'$ es precisamente la que define a Δ a través de la propiedad universal de δ' (teorema 2.31). También se tiene $(\varepsilon \otimes A)\delta' \equiv \delta'$, por el mismo motivo. Se sigue así que A es un L-comódulo a izquierda. Como sabemos por la proposición 2.30 que δ' es un homomorfismo de álgebras, concluimos que A es además un L-comódulo álgebra a izquierda.
- **A es un (L,H)-bicomódulo**: Utilizando la relación (R2) se tiene que

$$\begin{aligned}(L \otimes \delta)\delta'(a) &= (L \otimes \delta)(a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(1)})) \\ &= (a_{(0)} \otimes l_i(a_{(1)})) \otimes r_i(a_{(1)(0)} \otimes r_i(a_{(1)(1)} \\ &\overset{(R2)}{=} a_{(0)} \otimes l_i(a_{(1)(1)}) \otimes r_i(a_{(1)(1)}) \otimes a_{(1)(2)} \\ &= a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(1)}) \otimes a_{(2)}\end{aligned}$$

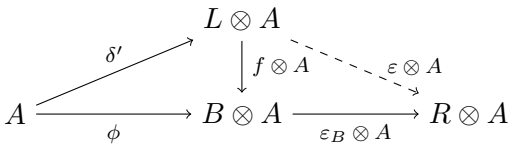
  Por otro lado, $(\delta' \otimes H)\delta(a) = (\delta' \otimes H)(a_{(0)} \otimes a_{(1)}) = a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(1)}) \otimes a_{(2)}$, con lo que queda demostrado que $(L \otimes \delta)\delta' = (\delta' \otimes H)\delta(a)$.
- **Veamos que ${}^{coL}A = R1_A$:** Supongamos que $a \in {}^{coL}A$. Entonces $\delta'(a) = 1 \otimes 1 \otimes a$, lo que implica que $a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(1)}) = 1 \otimes 1 \otimes a$. Multiplicando los dos últimos factores de la expresión se obtiene por (R1) que $a \otimes 1 = 1 \otimes a$, luego $a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(1)}) = a \otimes 1 \otimes 1$. Aplicando $A \otimes \kappa_r$ a ambos lados de esta igualdad se tiene que $a_{(0)} \otimes 1 \otimes a_{(1)} = a \otimes 1 \otimes 1_H$, y multiplicando los dos primeros factores obtenemos $a_{(0)} \otimes a_{(1)} = a \otimes 1_H$. Esto implica que $a \in A^{coH} = R1_A$. Como es claro que $R1_A \subseteq {}^{coL}A$, concluimos que en efecto ${}^{coL}A = R1_A$.

- **La aplicación $\kappa_l : A \otimes A \to L \otimes A$ es biyectiva**: notemos que en este caso la aplicación de Galois κ_l asociada a A como L-extensión a izquierda está dada por la expresión $a \otimes b \mapsto a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(2)})b$. Tomando $M = (A \otimes A)$ en el teorema 2.20 se tiene que la aplicación $(A \otimes A)^{\mathrm{co}H} \otimes A \to A \otimes A$ dada por $(a' \otimes a'' \otimes b) \mapsto a' \otimes a''b$ es biyectiva. Aplicando esta biyección a $\kappa_l(a \otimes b)$ obtenemos, utilizando (R1), que $a_{(0)} \otimes l_i(a_{(1)})r_i(a_{(2)})b = a \otimes b$. Concluimos así que κ_l es la inversa de esta biyección, de donde se sigue que κ_l es biyectiva.

- **Unicidad de $L(A, H)$**: Sea $(B, \Delta_B, \varepsilon_B)$ otra biálgebra y $\phi : A \to B \otimes A$ una aplicación que convierte a A/R en una extensión B-H bi-Galois. Entonces $\phi \in \mathcal{M}^H(A, B \otimes A)$ y es un homomorfismo de álgebras. Se sigue por la propiedad universal de δ' que existe un único homomorfismo de álgebras $f : L \to B$ tal que el siguiente diagrama conmuta:



Comprobemos que f es un homomorfismo de álgebras y biyectiva. Como $\phi = (f \otimes A)\delta'$, entonces $(B \otimes \phi)\phi = (B \otimes (f \otimes A)\delta')(f \otimes A)\delta' = (f \otimes (f \otimes A)\delta')\delta' = f \otimes (f \otimes A)(L \otimes \delta')\delta' = (f \otimes (f \otimes A))(\Delta \otimes A)\delta' = ((f \otimes f)\Delta \otimes A)\delta'$. Por otro lado, $(B \otimes \phi)\phi = (\Delta_B \otimes A)\phi = ((\Delta_B f) \otimes A)\delta'$. Queda entonces demostrado que $((\Delta_B f) \otimes A)\delta' = ((f \otimes f)\Delta \otimes A)\delta'$. Se sigue por la unicidad de la propiedad universal que $(f \otimes f)\Delta = \Delta_B f$. De la misma forma se procede con ε en el diagrama



y se concluye que $\varepsilon = \varepsilon_B \circ f$. Con esto queda probado que f es homomorfismo de biálgebras. Ahora, sea $\kappa_l' : A \otimes A \to B \otimes A$ el isomorfismo dado por ser una B-extensión de Galois a izquierda. Como $\phi = (f \otimes A)\delta'$, también se cumple que $\kappa_l' = (f \otimes A)\kappa_l$, donde $\kappa_l : A \otimes A \to L \otimes A$ es el isomorfismo que le corresponde por ser una L-extensión de Galois a izquierda. Como tanto κ_l como κ_l' son biyectivas, así lo es f.

□

2.5. El teorema fundamental de la teoría de Galois-Hopf

La peculiaridad de la teoría de Galois-Hopf reside en que la correspondencia de Galois-Hopf de una (L, H)-extensión bi-Galois A/R es entre algunas de sus H-subextensiones a derecha y algunas subestructuras de L.

2.5.1. Los conjuntos Quot(L) y Sub(A)

Definición 2.35 (Coideal)**.** Un R-submódulo I de una R-coálgebra C se dice **coideal** de C si $\Delta(I) \subseteq I \otimes C + C \otimes I$ y $\varepsilon(I) = 0$.

Definición 2.36 (Quot(L) y Sub(A))**.** Sea A una (L,H)-extensión bi-Galois. Definimos los conjuntos:

$$\begin{cases} \text{Sub}(A) := \{H\text{-subcomódulo álgebras de } A\} \\ \\ \text{Quot}(L) := \{\text{Coideales ideales a izquierda de } L\} \end{cases}$$

Nota 2.37. El conjunto Sub(A) está parcialmente ordenado mediante la inclusión. Quot(L) lo está según el siguiente criterio: $I \leq J$ si y solo si $I \subseteq J$.

2.5.2. La conexión de Galois

Definición 2.38 (Conexión de Galois)**.** Sean $(A,\leq)$ y $(B,\leq)$ dos conjuntos parcialmente ordenados. Una **conexión de Galois** entre los conjuntos A y B es un par de funciones monótonas $(F : A \to B, G : B \to A)$ tales que para cualesquiera $a \in A$, $b \in B$ se tiene que $F(a) \leq b$ si y solo si $a \leq G(b)$.

El teorema fundamental de la teoría de Galois-Hopf establecerá una correspondencia biyectiva entre un subconjunto de Sub(A) y un subconjunto de Quot(L). En general, no es posible hacer esto entre los dos conjuntos completos. No obstante, sí que es posible establecer una conexión de Galois entre ellas (más «débil» que una biyección). La proposición siguiente está desarrollada a partir de [13, proposición 3.2].

Proposición 2.39. *Sea A/R una (L,H)-extensión bi-Galois fielmente plana. Entonces se tiene la conexión de Galois*

$$\text{Quot}(L) \underset{\mathcal{G}}{\overset{\mathcal{F}}{\rightleftarrows}} \text{Sub}(A)$$

con $\mathcal{F}(I) = {}^{coL/I}A$ *y* $L/\mathcal{G}(B) := (A \otimes_B A)^{coH}$.

Demostración. Veamos en primer lugar que la aplicación $\mathcal{F}$ está bien definida. Sea $I \in \text{Quot}(L)$, entonces $\mathcal{F}(I) = \left\{b \in A \mid b_{(-1)} \otimes b_{(0)} - 1_L \otimes b \in I \otimes A\right\} = (\delta' - 1_L \otimes A)^{-1}(I \otimes A)$ (esta última expresión refiere a la preimagen de $I \otimes A$ por $\delta' - 1_L \otimes A$). Notamos que para $b, b' \in \mathcal{F}(I)$:

$$b_{(-1)}b'_{(-1)} \otimes b_{(0)}b'_{(0)} - 1_L \otimes bb' = \left(b_{(-1)} \otimes b_{(0)}\right)\left(b'_{(-1)} \otimes b'_{(0)} - 1 \otimes b'\right) + b_{(-1)} \otimes b_{(0)}b' - 1 \otimes bb'. \quad (2.5)$$

Como $b'_{(-1)} \otimes b'_{(0)} - 1 \otimes b' \in I \otimes A$ y I es ideal a izquierda de L se sigue que $(b_{(-1)} \otimes b_{(0)})(b'_{(-1)} \otimes b'_{(0)} - 1 \otimes b') \in I \otimes A$. Módulo $I \otimes A$, la expresión 2.5 proporciona

$$b_{(-1)} \otimes b_{(0)}b' - 1 \otimes bb' = \left(b_{(-1)} \otimes b_{(0)} - 1 \otimes b\right) 1 \otimes b' \in I \otimes A.$$

Concluimos así que $bb' \in \mathcal{F}(I)$, luego $\mathcal{F}(I)$ es subálgebra de A. Ahora, dado $b \in \mathcal{F}(I)$. Para probar que $\mathcal{F}(I)$ es un H-subcomódulo debemos ver que $b_{(0)} \otimes b_{(1)} \in \mathcal{F}(I) \otimes H$. Usando que A es un (L,H)-bicomódulo y aplicando $L \otimes \delta$ a $b_{(-1)} \otimes b_{(0)} - 1_L \otimes b \in I \otimes A$ se sigue que

$$\left(b_{(-1)} \otimes b_{(0)} - 1_L \otimes b_{(0)}\right) \otimes b_{(1)} = b_{(-1)} \otimes b_{(0)} \otimes b_{(1)} - 1_L \otimes b_{(0)} \otimes b_{(1)} \in I \otimes A \otimes H.$$

Esto implica que $(\delta' - 1_L \otimes A) \otimes H(b_{(0)} \otimes b_{(1)}) \in I \otimes A \otimes H$, con lo que $b_{(0)} \otimes b_{(1)} \in F(I) \otimes H$. Queda así demostrado que $\mathcal{F}(I) \in \text{Sub}(A)$. Veamos ahora que $\mathcal{G}$ está también bien definida, es decir, que $\mathcal{G}(B)$ es tanto coideal como ideal a izquierda de L. Atendamos primero a la definición

de $\mathcal{G}(B)$. Notamos que $A \otimes_B A$ es un H-comódulo mediante $a\widehat{\otimes}c \mapsto a_{(0)}\widehat{\otimes}c_{(0)} \otimes a_{(1)}c_{(1)}$ (donde $\widehat{\otimes}$ denota $\otimes_B$), ya que es una aplicación bien definida puesto que, para $b \in B$, $b_{(0)} \in B$ luego

$$\begin{array}{rcl} ab \mathbin{\widehat{\otimes}} c & \longmapsto & a_{(0)}b_{(0)} \mathbin{\widehat{\otimes}} c_{(0)} \otimes a_{(1)}b_{(1)}c_{(1)} \\ & & \| \\ a \mathbin{\widehat{\otimes}} bc & \longmapsto & a_{(0)} \mathbin{\widehat{\otimes}} b_{(0)}c_{(0)} \otimes a_{(1)}b_{(1)}c_{(1)} \end{array}.$$

Se puede entonces considerar la aplicación $A \otimes A \to A \otimes_B A$ dada por $a \otimes c \mapsto a\widehat{\otimes}c$, que es un epimorfismo en $\mathcal{M}^H$. Es más, $A \otimes_B A \in \mathcal{M}_A^H$ de forma natural y este es un epimorfismo en $\mathcal{M}_A^H$. Como por el teorema 2.20 $A \otimes A \cong (A \otimes A)^{\mathrm{co}H} \otimes A$ y $A \otimes_B A \cong (A \otimes_B A)^{\mathrm{co}H} \otimes A$, el anterior epimorfismo se restringe al siguiente:

$$\begin{array}{rccc} \varphi: & (A \otimes A)^{\mathrm{co}H} & \longrightarrow & (A \otimes_B A)^{\mathrm{co}H} \\ & a' \otimes a'' & \longmapsto & a'\widehat{\otimes}a'' \end{array}$$

$\mathcal{G}(B)$ es el núcleo de φ, es decir, $\mathcal{G}(B) = \left\{a'b \otimes a'' - a' \otimes ba'' \in (A \otimes A)^{\mathrm{co}H} \;\middle|\; b \in B\right\}$. Que $\mathcal{G}(B)$ es ideal a izquierda de L es claro, ya que dado $c' \otimes c'' \in L$ (recordamos que el producto es el de $A \otimes A^{\mathrm{op}}$), $c' \otimes c''\,(a'b \otimes a'' - a' \otimes ba'') = c'a'b \otimes a''c'' - c'a' \otimes ba''c''$. Veamos ahora que $\mathcal{G}(B)$ es un coideal de L. Utilizando que $1_A \otimes b = b_{(0)}l_i(b_{(1)}) \otimes r_i(b_{(1)})$ obtenemos:

$$\begin{aligned} &\Delta(a'b \otimes a'' - a' \otimes ba'') = \\ &\quad = a'_{(0)}b_{(0)} \otimes l_i(a'_{(1)}b_{(1)}) \otimes r_i(a'_{(1)}b_{(1)}) \otimes a'' - a'_{(0)} \otimes l_i(a'_{(1)}) \otimes r_i(a'_{(1)}) \otimes ba'' \\ &\quad = a'_{(0)}b_{(0)} \otimes l_i(a'_{(1)}b_{(1)}) \otimes r_i(a'_{(1)}b_{(1)}) \otimes a'' - a'_{(0)} \otimes b_{(0)}l_i(b_{(1)})l_i(a'_{(1)}) \otimes r_i(a'_{(1)}) \otimes r_i(b_{(1)})a'' \end{aligned}$$

Módulo $\mathcal{G}(B) \otimes A + A \otimes \mathcal{G}(B)$ (y «pasando» por tanto a $(A \otimes_B A) \otimes_R (A \otimes_B A)$) nos queda

$$a'_{(0)} \otimes b_{(0)}l_i(b_{(1)})l_i(a'_{(1)}) \otimes r_i(a'_{(1)})r_i(b_{(1)}) \otimes a'' - a'_{(0)} \otimes b_{(0)}l_i(b_{(1)})l_i(a'_{(1)}) \otimes r_i(a'_{(1)})r_i(b_{(1)}) \otimes a'' = 0.$$

Es decir, que $\Delta(\mathcal{G}(B)) \subseteq L \otimes L \cap (\mathcal{G}(B) \otimes A + A \otimes \mathcal{G}(B)) \subseteq \mathcal{G}(B) \otimes L + L \otimes \mathcal{G}(B)$, con lo que queda demostrado que $\mathcal{G}(B)$ es un coideal de L. Tras haber visto que las aplicaciones $\mathcal{F}$ y $\mathcal{G}$ están bien definidas, podemos comprobar que definen una conexión de Galois entre $\mathrm{Quot}(L)$ y $\mathrm{Sub}(A)$. Esto es equivalente a decir que se verifican las siguientes propiedades:

1. **Si $B \subseteq B'$, entonces $\mathcal{G}(B) \subseteq \mathcal{G}(B')$**: vemos fácilmente que

$$\mathcal{G}(B) = \{a'b \otimes a'' - a' \otimes ba'' \in L \mid b \in B\} \subseteq \{a'b \otimes a'' - a' \otimes ba'' \in L \mid b \in B'\} = \mathcal{G}(B').$$

2. **Si $I \subseteq I'$, entonces $\mathcal{F}(I) \subseteq \mathcal{F}(I')$**: en efecto, ya que

$$\mathcal{F}(I) = \left\{b \;\middle|\; b_{(-1)} \otimes b_{(0)} - 1_L \otimes b \in I \otimes A\right\} \subseteq \left\{b \;\middle|\; b_{(-1)} \otimes b_{(0)} - 1_L \otimes b \in I' \otimes A\right\} = \mathcal{F}(I').$$

3. **Veamos que $B \subseteq \mathcal{F}\mathcal{G}(B)$**: observamos que, por la definición de δ',

$$\begin{aligned} \mathcal{F}(\mathcal{G}(B)) &= \left\{a \in A \;\middle|\; a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(1)}) - 1 \otimes 1 \otimes a \in \mathcal{G}(B) \otimes A\right\} \\ &= \left\{a \in A \;\middle|\; a_{(0)}\widehat{\otimes}l_i(a_{(1)}) \otimes r_i(a_{(1)}) = 1\widehat{\otimes}1 \otimes a\right\} \end{aligned}$$

Dado $b \in B$, $b_{(0)}\widehat{\otimes}l_i(b_{(1)}) \otimes r_i(b_{(1)}) = 1\widehat{\otimes}b_{(0)}l_i(b_{(1)}) \otimes r_i(b_{(1)}) = 1\widehat{\otimes}1 \otimes b$ y así $b \in \mathcal{F}\mathcal{G}(B)$.

4. **Veamos que** $\mathcal{GF}(I) \subseteq I$: Consideramos la aplicación $A \otimes A \to L/I \otimes A$ dada por $a' \otimes a'' \mapsto \overline{a'_{(-1)}} \otimes a'_{(0)}a''$. Si $b \in \mathcal{F}(I)$ entonces $b_{(-1)} \otimes b_{(0)} - 1_L \otimes b \in I \otimes A$. Como I es ideal a izquierda de L se sigue que

$$\begin{aligned} a'b \otimes a'' &\longmapsto \overline{a'_{(-1)}b_{(1)}} \otimes a'_{(0)}b_{(0)}a'' = \overline{a'_{(-1)}} \otimes a'_{(0)}ba'' \\ a' \otimes ba'' &\longmapsto a'_{(0)}ba'' \end{aligned}$$

Así queda inducida la aplicación

$$\begin{array}{ccc} A \otimes_{\mathcal{F}(I)} A & \longrightarrow & L/I \otimes A \\ a' \otimes_{\mathcal{F}(I)} a'' & \longmapsto & \overline{a'_{(-1)}} \otimes a'_{(0)}a'' \end{array} \tag{2.6}$$

Si consideramos $A \otimes_{\mathcal{F}(I)} A$ con una coacción codiagonal $a' \otimes_{\mathcal{F}(I)} a'' \mapsto a'_{(0)} \otimes_{\mathcal{F}(I)} a''_{(0)} \otimes a'_{(0)}a''_{(0)}$ (que está bien definida) y $L/I \otimes A$ con la coacción $\overline{x} \otimes a \mapsto \overline{x} \otimes a_{(0)} \otimes a_{(1)}$, entonces la aplicación 2.6 es un morfismo en $\mathcal{M}_A^H$. Se induce entonces:

$$\begin{array}{ccccccc} (A \otimes A)^{\mathrm{co}H}/\mathcal{GF}(I) & \cong & (A \otimes_{\mathcal{F}(I)} A)^{\mathrm{co}H} & \to & (L/I \otimes A)^{\mathrm{co}H} & = & \overline{L/I \otimes 1_A} \\ \overline{a' \otimes a''} & \leftrightarrow & a' \otimes_{\mathcal{F}(I)} a'' & \mapsto & \overline{a'_{(-1)}} \otimes a'_{(0)}a'' & = & \overline{a'_{(0)} \otimes l_i(a'_{(1)})} \otimes r_i(a'_{(1)})a'' \end{array}$$

Así, la imagen de $\mathcal{G}(\mathcal{F}(I)) \subseteq (A \otimes A)^{\mathrm{co}H}$ por $a' \otimes a'' \mapsto a'_{(0)} \otimes l_i(a'_{(1)}) \otimes r_i(a'_{(1)})a''$ está contenida en $I \otimes 1_A$. Notamos que este es precisamente el isomorfismo κ_l entre $A \otimes A$ y $L \otimes A$, cuya inversa es $\kappa_l^{-1} : a' \otimes a'' \otimes b \mapsto a' \otimes a''b$. Concluimos así que $\mathcal{G}(\mathcal{F}(I)) \subseteq \kappa_l^{-1}(I \otimes 1_A) = I$.

□

2.5.3. Elementos admisibles y la correspondencia de Galois-Hopf

En este momento hemos probado la existencia de una conexión de Galois entre $\mathrm{Quot}(L)$ y $\mathrm{Sub}(A)$, pero no de una correspondencia biyectiva. En esta sección veremos como, para establecer la biyección, hay que restringirse a ciertos subconjuntos de $\mathrm{Quot}(L)$ y $\mathrm{Sub}(A)$: los formados por los elementos «admisibles». Introducimos a continuación este nuevo concepto.

Definición 2.40 (Coideal admisible)**.** Sea C una R-coálgebra y $C \to \overline{C}$ una coálgebra cociente. Diremos que $\overline{C}$ es **admisible** a derecha (izquierda) si es R-plana y C es fielmente coplana a derecha (izquierda) sobre $\overline{C}$. Diremos que un coideal $I \subset C$ es admisible a derecha (izquierda) si C/I lo es.

Definición 2.41 (Subálgebra admisible)**.** Sean A una R-álgebra y B una R-subálgebra de A. Diremos que B es **admisible** a derecha (izquierda) si A es fielmente plana como B-módulo a derecha (izquierda).

En ambos casos diremos que un elemento es admisible si lo es tanto a izquierda como a derecha. Con esto ya quedan definidos todos los conceptos que intervienen en el teorema fundamental. La demostracion del mismo puede encontrarse en [13], aunque escapa al alcance de esta memoria. Por ello, nos limitaremos a enunciarlo y estudiar su funcionamiento en la sección de ejemplos.

Teorema 2.42 (Teorema fundamental de la teoría de Galois-Hopf)**.** *Sean H y L dos R-álgebras de Hopf con antípodas biyectivas. Sea A/R una (L,H)-extensión bi-Galois fielmente plana. Las aplicaciones $\mathcal{F}$ y $\mathcal{G}$ de la proposición 2.39 inducen biyecciones (mutuamente inversas) entre los coideales admisibles $I \in \mathrm{Quot}(L)$ y las subálgebras admisibles $B \in \mathrm{Sub}(A)$.*

2.6. Ejemplos

En el siguiente ejemplo aplicaremos la teoría desarrollada al caso clásico. Dado que no hemos encontrado ninguna referencia adecuada, utilizaremos principalmente nuestros propios argumentos. Observaremos como el teorema fundamental generalizado 2.42 no coincide en su totalidad con el teorema fundamental de la teoría de Galois cuando nos restringimos a extensiones de Galois clásicas, ya que en la correspondencia solo participarán los subgrupos y subextensiones normales.

Ejemplo 2.43 (Caso clásico)**.** Sea F/K una extensión de cuerpos de Galois en el sentido clásico, con $\mathrm{Gal}(F/K) = G = \mathrm{Aut}_K(F)$. Realizaremos un estudio completo de la extensión por partes.

F/K es una $K[G]^*$-extensión de Galois a derecha

Consideramos el álgebra grupo $K[G]$ (ver ejemplo 2.4), y definimos la acción a izquierda de $K[G]$ en F dada por

$$\begin{array}{ccc} K[G]\otimes F & \longrightarrow & F \\ \sum_{i=1}^n \alpha_i\sigma_i \otimes a & \longmapsto & \sum_{i=1}^n \alpha_i\sigma_i(a) \end{array},$$

donde $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Dados $a, b \in F$, para cada $i = 1, \ldots, n$ se cumple que $\sigma_i(ab) = \sigma_i(a)\sigma_i(b) = \sigma_{i(1)}(a)\sigma_{i(2)}(b)$ y también que $\sigma_i(1) = 1 = \varepsilon(\sigma)1$. Así F es una $K[G]$-módulo álgebra a izquierda. Notamos que $\tau(a) = a$ para todo $\tau \in G$ si y solo si $a \in K$, luego el conjunto de invariantes por esta acción es $F^{K[G]} = K$. Esto implica que F es además un $K[G]^*$-comódulo álgebra a derecha, donde $K[G]^*$ denota el dual de $K[G]$. Además, $K = F^{K[G]} = F^{\mathrm{co}K[G]^*}$, luego F/K es una $K[G]^*$-extensión a derecha (proposición 2.74). La coacción a derecha de $K[G]^*$ en F inducida por la acción a izquierda de $K[G]$ en F es la siguiente:

$$\begin{array}{ccc} F & \longrightarrow & F\otimes K[G]^* \\ a & \longmapsto & \sum_{i=1}^n \sigma_i(a)\otimes \sigma_i^* \end{array},$$

donde cada σ_i^* es el dual de σ_i (notamos que $\{\sigma_i^*\}_{i=1}^n$ es una K-base de $K[G]^*$). La aplicación de Galois correspondiente es

$$\kappa_r : \begin{array}{ccc} F\otimes F & \longrightarrow & F\otimes K[G]^* \\ \sum_{j=1}^m a_j\otimes b_j & \longmapsto & \sum_{j=1}^m\sum_{i=1}^n a_j(\sigma_i(b_j))\otimes\sigma_i^* \end{array}.$$

El objetivo ahora es probar que esta κ_r es biyectiva. Sea $\omega = \sum_{j=1}^m a_j \otimes b_j \in \ker\kappa_r$. Como F/K es una extensión de Galois en sentido clásico, existe $\xi \in F$ tal que la familia $\{\tau(\xi) \mid \tau \in G\}$ es una K-base de F. Podemos reescribir así nuestros elementos de $F \otimes_K F$ de la forma

$$\sum_{j=1}^m a_j \otimes b_j = \sum_{\tau\in G} a_\tau \otimes \tau(\xi) = \sum_{j=1}^n a_{\sigma_j} \otimes \sigma_j(\xi).$$

Reescribiendo nuestro $\omega \in \ker\kappa_r$ de esta misma manera,

$$\kappa_r(\omega) = \sum_{j=1}^n\sum_{i=1}^n a_{\sigma_j}(\sigma_i(\sigma_j(\xi)))\otimes\sigma_i^* = 0.$$

La independencia de $\{\sigma_i^*\}_{i=1}^n$ implica que $\sum_j a_{\sigma_j}(\sigma_i(\sigma_j(\xi))) = 0$ para cada $i = 1, \ldots, n$. Como F/K es una extensión de Galois en sentido clásico, la acción de G en F es fiel. Se sigue por el teorema de independencia de caracteres que, por la independencia de $\{\sigma_j(\xi)\}_{j=1}^n$, la matriz

$$\begin{pmatrix} \sigma_1(\sigma_1(\xi)) & \cdots & \sigma_n(\sigma_1(\xi)) \\ \vdots & \ddots & \vdots \\ \sigma_1(\sigma_n(\xi)) & \cdots & \sigma_n(\sigma_n(\xi)) \end{pmatrix}$$

es invertible. Esto implica que, para $\lambda_1, \ldots, \lambda_n \in F$, $i = 1, \ldots, n$,

$$\lambda_1\sigma_i(\sigma_1(\xi)) + \cdots + \lambda_n\sigma_i(\sigma_n(\xi)) = 0 \text{ si y solo si } \lambda_1 = \cdots = \lambda_n = 0.$$

Se sigue que $a_{\sigma_j} = 0$ para cada $j = 1, \ldots, n$, luego $\omega = 0$ y queda probada la inyectividad de κ_r. Por otro lado, como tanto $F \otimes_K F$ como $F \otimes_K K[G]^*$ son K-álgebras de la misma dimensión (finita), se sigue la biyectividad de κ_r. Concluimos así que F/K es una $K[G]^*$-extensión de Galois a derecha.

Nota 2.44. La aplicación κ es además un isomorfismo de K-álgebras, ya que $\kappa(a' \otimes b' \cdot a'' \otimes b'') = \kappa(a'a'' \otimes b'b'') = \sum_{\sigma\in G} a'a''\sigma(b'b'') \otimes \sigma^* = \sum_{\sigma\in G} a'\sigma(b')a''\sigma(b'') \otimes \sigma^* = \sum_{\sigma\in G} a'\sigma(b') \otimes \sigma^* + \sum_{\tau\in G} a''\tau(b'') \otimes \tau^* = \kappa(a' \otimes b')\kappa(a'' \otimes b'')$.

Observación 2.45. Se puede probar también que toda $K[G]^*$-extensión de Galois a derecha F/K es, de hecho, una extensión de Galois en el sentido clásico, con $\mathrm{Gal}(F/K) = G$. Recordamos que la coacción a derecha de $K[G]^*$ en F está dada por $a \mapsto \sum_i \sigma_i(a) \otimes \sigma_i^*$. Esta coacción induce la siguiente acción a izquierda de $K[G]$ en F: para $\tau \in G$, $a \in F$,

$$\tau \cdot a = \sum_{i=1}^{n} \sigma_i^*(\tau)\tau(a) = \sum_{i=1}^{n} \delta_{\sigma_i,\tau}\tau(a) = \tau(a).$$

Se sigue que $\tau \cdot a = a$ para todo $\tau \in G$ si y solo si $\tau(a) = a$ para todo $\tau \in G$. Es decir, que $F^{\mathrm{co}K[G]^*} = F^G = K$. Como κ_r es biyectiva, las dimensiones de $F \otimes_K F$ y $F \otimes_K K[G]^*$ como K-álgebras coinciden, luego $[F : K] = |G|$. Concluimos así que F/K es una extensión de Galois en el sentido clásico, con grupo de Galois G.

Para abreviar la notación, el resto del ejemplo utilizará H para referirse a $K[G]^*$.

El álgebra de Hopf $L = L(F, H)$ y los elementos de $\mathrm{Quot}(L)$

El siguiente paso consiste en encontrar el álgebra de Hopf $L(F, K[G]^*)$. Ello requiere comprender la estructura de $F \otimes F$ para así hallar $(F \otimes F)^{\mathrm{co}H}$. Si denotamos por I al elemento neutro del grupo G notamos que, como $1 \otimes I^*$ es un idempotente, así lo es $e_I = \kappa^{-1}(1 \otimes I^*)$. Ahora tomamos ξ tal que $\{\sigma(\xi)\}_{\sigma\in G}$ es una K-base de F y reescribimos e_I de la forma $\sum_{\sigma\in G} \alpha_\sigma \otimes \sigma(\xi)$, para ciertos $\alpha_\sigma \in F$. Notamos que $1 \otimes I^* = \kappa(e_I) = \sum_{\tau,\sigma} \alpha_\sigma\tau\sigma(\xi) \otimes \tau^*$, lo que implica que $\sum_\sigma \alpha_\sigma\tau\sigma(\xi) = \delta_{\tau,I}$ para cada $\tau \in G$. Ahora definimos los elementos $e_\omega := \sum_\sigma \alpha_{\omega\sigma} \otimes \sigma(\xi) = \sum_\sigma \alpha_\sigma \otimes \omega^{-1}\sigma(\xi)$, para cada $\omega \in G$. Observamos que para cada $\omega \in G$ se cumple que

$$\kappa(e_\omega) = \sum_{\tau,\sigma} \alpha_\sigma\tau\omega^{-1}\sigma(\xi) \otimes \tau^* = \sum_\tau \delta_{I,\tau\omega^{-1}} \otimes \tau^* = 1 \otimes \omega^*.$$

Concluimos así que cada e_ω es idempotente y además $\kappa(e_\omega) = 1 \otimes \omega^*$. Dados elementos $\sigma, \tau \in G$, como $1 \otimes \sigma^* \cdot 1 \otimes \tau^* = \delta_{\sigma,\tau} 1 \otimes \sigma^*$ y $\sum_\sigma 1 \otimes \sigma^* = 1 \otimes 1_H$, se sigue que

$$e_\sigma \cdot e_\tau = \delta_{\tau,\sigma} e_\sigma, \quad \sum_\sigma e_\sigma = 1 \otimes 1.$$

Ahora consideramos, para $\tau \in G$, las aplicaciones $\tau \otimes I$ e $I \otimes \tau$. Para todo $\omega \in G$ se cumple que $(I \otimes \tau)(e_\omega) = \sum_\sigma \alpha_{\omega\sigma} \otimes \tau\sigma(\xi) = \sum_\sigma \alpha_{\omega\tau^{-1}\sigma} \otimes \sigma(\xi) = e_{\omega\tau^{-1}}$. Por otra parte, $\kappa(\tau \otimes I(e_\omega)) = \kappa\left(\sum_{\sigma\in G} \tau(\alpha_{\omega\sigma}) \otimes \sigma(\xi)\right) = \sum_{\theta,\sigma\in G} \tau(\alpha_{\omega\sigma})\theta\sigma(\xi) \otimes \theta^* = (\tau \otimes I)\left(\sum_{\theta,\sigma\in G} \alpha_{\omega\sigma}\tau^{-1}\theta\sigma(\xi) \otimes \theta^*\right) = (\tau \otimes I)\left(\sum_{\theta,\sigma} \alpha_{\omega\theta^{-1}\tau\sigma}\sigma(\xi) \otimes \theta^*\right) = (\tau \otimes I)\left(\sum_\theta \delta_{\omega\theta^{-1}\tau,I} \otimes \theta^*\right) = (\tau \otimes I)(1 \otimes (\tau\omega)^*) = 1 \otimes (\tau\omega)^*$. Hemos comprobado así que $(I \otimes \tau)(e_\omega) = e_{\omega\tau^{-1}}$ y $(\tau \otimes I)(e_\omega) = e_{\tau\omega}$, de donde concluimos que

$(\tau\otimes\tau)(e_\omega) = e_{\tau\omega\tau^{-1}}$. Vemos además que $\sum_\sigma \alpha_{\tau\omega\sigma}\otimes\sigma(\xi) = e_{\tau\omega} = (\tau\otimes I)(e_\omega) = \sum_\tau(\alpha_{\omega\sigma})\otimes\sigma(\xi)$, luego $\tau(\alpha_\sigma) = \alpha_{\tau\sigma}$ para todo $\tau,\sigma\in G$, y en particular $\alpha_\sigma = \sigma(\alpha_I)$.

Notamos adicionalmente que para todo $b\in F$, $\omega\in G$ se verifica que $e_\omega\cdot 1\otimes b = \omega(b)\otimes 1\cdot e_\omega$, ya que $\kappa(e_\omega\cdot 1\otimes b) = \kappa(e_\omega)\kappa(1\otimes b) = (1\otimes\omega^*)$ y $\sum_\sigma \sigma(b)\otimes\sigma^* = \omega(b)\otimes\omega^* = \sum_\sigma \omega(b)\otimes\sigma^*\cdot 1\otimes\omega^* = \kappa(\omega(b)\otimes 1)\cdot 1\otimes\omega^* = \kappa(\omega(b)\otimes 1\cdot e_\omega)$.

En lo que sigue será de utilidad el siguiente resultado:

Proposición 2.46. *Todo elemento de $F\otimes F$ se puede expresar de manera única como $\sum_{\sigma\in G}(\beta_\sigma\otimes 1)e_\sigma$, para ciertos elementos $\beta_\sigma\in F$.*

Demostración. Notamos primero que, dados $a\otimes b\in F\otimes F$, $\sigma\in G$, $(a\otimes b)e_\sigma = (a\otimes 1)(1\otimes b)e_\sigma = (a\otimes 1)(\sigma(b)\otimes 1)e_\sigma = a\sigma(b)\otimes 1\cdot e_\sigma \in F\otimes 1\cdot e_\sigma$. Como $\sum_\sigma e_\sigma = 1\otimes 1$, entonces $F\otimes F = F\otimes F\cdot 1\otimes 1 \le \sum_\sigma F\otimes F\cdot e_\sigma = \sum_\sigma F\otimes 1\cdot e_\sigma$. Se sigue que cada elemento de $F\otimes F$ puede expresarse de la forma $\sum_\sigma(\beta_\sigma\otimes 1)e_\sigma$. Supongamos que $\sum_\sigma(\beta_\sigma\otimes 1)e_\sigma = \sum_\sigma(\beta'_\sigma\otimes 1)e_\sigma$. En ese caso podemos aplicar κ a ambos lados y obtenemos que $\sum_\sigma \beta_\sigma\otimes\sigma^* = \sum_\sigma \beta'_\sigma\otimes\sigma^*$, luego $\beta_\sigma = \beta'_\sigma$ para cada $\sigma\in G$. Concluimos así que esta representación es única. □

A continuación estudiamos $(F\otimes F)^{\mathrm{co}H}$, aprovechando estos elementos auxiliares e_ω. Notamos en primer lugar que

$$L = (F\otimes F)^{\mathrm{co}H} = \left\{\sum_i a_i\otimes b_i\in F\otimes F : \sum_{i,\sigma,\tau}\sigma(a_i)\otimes\tau(b_i)\otimes\sigma^*\tau^* = \sum_i a_i\otimes b_i\right\}$$
$$= \left\{\sum_i a_i\otimes b_i\in F\otimes F : (\tau\otimes\tau)\left(\sum_i a_i\otimes b_i\right) = \sum_i a_i\otimes b_i,\ \forall\tau\in G\right\}.$$

Si denotamos por $\mathrm{cl}(\omega)$ a la clase de conjugación de cada $\omega\in G$ se tiene que

$$E_\omega := \sum_{\sigma\in\mathrm{cl}(\omega)} e_\sigma\in L, \quad \text{ya que } (\tau\otimes\tau)(E_\omega) = \sum_{\sigma\in\mathrm{cl}(\omega)}(\tau\otimes\tau)(e_\sigma) = \sum_{\sigma\in\mathrm{cl}(\omega)} e_{\tau\sigma\tau^{-1}} = E_\omega.$$

Denotamos por $\omega_1,\dots,\omega_r$ a los elementos de G tales que $G = \bigcup_{i=1}^r \mathrm{cl}(\omega_i)$. Así $1\otimes 1 = \sum_\sigma e_\sigma = E_{\omega_1}+\cdots+E_{\omega_r}$ y $\{E_{\omega_i}\}_{i=1}^r$ es una familia de idempotentes ortogonales dos a dos. Se sigue que $L = LE_{\omega_1}\oplus\cdots\oplus LE_{\omega_r}$. Nuestro objetivo ahora será utilizar esto para encontrar los ideales y coideales de L que intervendrán en la correspondencia con $\mathrm{Sub}(F)$.

Ideales de L: Sea $\omega\in G$, LE_ω tiene la forma $\sum_{\sigma\in\mathrm{cl}(\omega)}(\beta_\sigma\otimes 1)e_\sigma$. Notamos que, para $\tau\in G$, $(\tau\otimes\tau)(LE_\omega) = \sum_{\sigma\in\mathrm{cl}(\omega)}(\tau(\beta_\sigma)\otimes 1)e_{\tau\omega\tau^{-1}} = \sum_{\sigma\in\mathrm{cl}(\omega)}(\beta_\sigma\otimes 1)e_\omega$. Concluimos de esto que $\tau(\beta_\sigma) = \beta_{\tau\sigma\tau^{-1}}$ para todo $\tau\in G$, $\sigma\in\mathrm{cl}(\omega)$. Si denotamos por $C_G(\omega) = \{g\in G \mid g\omega = \omega g\}$ al centralizador de ω, observamos que $\tau(\beta_\omega) = \beta_{\tau\omega\tau^{-1}} = \beta_\omega$ para todo $\tau\in C_G(\omega)$, luego $\beta_\omega\in\mathrm{Fix}(C_G(\omega))$. Por otro lado, si $\mathrm{cl}(\omega) = \{\tau_i\omega\tau_i^{-1}\}_{i=1}^m$, entonces $\sum_{\sigma\in\mathrm{cl}(\omega)}(\beta_\sigma\otimes 1)e_\sigma = \sum_{i=1}^m(\tau_i(\beta_\omega)\otimes 1)e_{\tau_i\omega\tau_i^{-1}}$. Esto implica que la aplicación

$$\begin{array}{rcl} F_\omega := \mathrm{Fix}(C_G(\omega)) & \longrightarrow & LE_\omega \\ \beta_\omega & \longmapsto & \sum_{i=1}^m(\tau_i(\beta_\omega)\otimes 1)e_{\tau_i\omega\tau_i^{-1}} \end{array}$$

está bien definida. Por la unicidad de la expresión de los elementos de $F\otimes F$ como $\sum_\sigma(\beta_\sigma\otimes 1)e_\sigma$ demostrada en la proposición 2.46 concluimos que además es inyectiva. La sobreyectividad se sigue de la forma de los elementos de LE_ω. Además es un homomorfismo (luego isomorfismo) de álgebras, ya que los e_σ son idempotentes ortogonales dos a dos y $\tau_i(\beta_\omega\beta'_\omega) = \tau_i(\beta_\omega)\tau_i(\beta'_\omega)$.

Concluimos así que $LE_\omega \cong F_\omega = \mathrm{Fix}(C_G(\omega))$ como K-álgebras. Se sigue que L es isomorfo al siguiente producto cartesiano de cuerpos:

$$L \cong \mathrm{Fix}(C_G(\omega_1)) \times \cdots \times \mathrm{Fix}(C_G(\omega_r)).$$

Como cada LE_{ω_i} es un cuerpo, los ideales de L son precisamente $\{\bigoplus_{i\in\Lambda} LE_{\omega_i} \mid \Lambda \subseteq \{1,\dots,r\}\}$.

Coideales de L: Veamos que $\Delta(E_\omega) \in L \otimes L = \bigoplus_{i,j=1}^r LE_{\omega_i} \otimes LE_{\omega_j}$ tiene componente no nula en $LE_{\omega_i} \otimes LE_{\omega_j}$ si y solo si $\omega \in \mathrm{cl}(\omega_i)\,\mathrm{cl}(\omega_j)$, es decir, si y solo si ω es producto de un conjugado de ω_i por uno de ω_j. La fórmula de Δ se hereda de la aplicación $\Delta : F \otimes F \to F \otimes F \otimes F \otimes F$ dada por $\Delta(a \otimes b) = \sum a_{(0)} \otimes l_i(a_{(1)}) \otimes r_i(a_{(1)}) \otimes b$, o lo que es lo mismo,

$$\Delta(a \otimes b) = \sum_{\sigma,i} \sigma(a) \otimes l_i(\sigma^*) \otimes r_i(\sigma^*) \otimes b = \sum_\sigma \sigma(a) \otimes e_\sigma \otimes b.$$

Ahora, dados $\theta, \Omega \in G$, estudiemos cómo es $\Delta(e_I)(e_\theta \otimes e_\Omega)$:

$$\begin{aligned}
\Delta(e_I) \cdot e_\theta \otimes e_\Omega &= \sum_\sigma \Delta(\alpha_\sigma \otimes \sigma(\xi)) \cdot (e_\theta \otimes e_\Omega) = \sum_{\tau,\sigma} (\tau(\alpha_\sigma) \otimes e_\tau \otimes \sigma(\xi)) \cdot (e_\theta \otimes e_\Omega) \\
&= \sum_{\omega,\tau,\sigma} (\alpha_{\tau\sigma} \otimes \alpha_{\tau\omega} \otimes \omega(\xi) \otimes \sigma(\xi)) \cdot (e_\theta \otimes e_\Omega) = \sum_{\omega,\tau,\sigma} (\alpha_{\tau\sigma}\alpha_{\theta\tau\omega} \otimes 1 \otimes \omega(\xi)\Omega\sigma(\xi) \otimes 1) \cdot (e_\theta \otimes e_\Omega) \\
&= \sum_{\omega,\tau,\sigma} (\alpha_{\tau\Omega^{-1}\sigma}\alpha_{\theta\tau\omega} \otimes 1 \otimes \omega(\xi)\sigma(\xi) \otimes 1) \cdot (e_\theta \otimes e_\Omega) = \sum_{\tau=\theta\tau\Omega} (e_{\theta\tau} \otimes 1 \otimes e_{\theta\tau} \otimes 1) \cdot (e_\theta \otimes e_\Omega) \\
&= \sum_{\substack{\tau=\theta\tau\Omega \\ \omega\in G}} (\alpha_{\theta\tau\omega} \otimes 1 \otimes \omega(\xi) \otimes 1) \cdot (e_\theta \otimes e_\Omega) = \sum_{\substack{\tau=\theta\tau\Omega \\ \omega\in G}} (1 \otimes \alpha_{\tau\omega} \otimes \omega(\xi) \otimes 1) \cdot (e_\theta \otimes e_\Omega).
\end{aligned}$$

Se puede deducir fácilmente que $\Delta(e_I)(e_\theta \otimes e_\Omega) = 0$ si θ no es conjugado de Ω^{-1}. Por otro lado, consideramos las aplicaciones $C_{34} : a \otimes b \otimes c \otimes d \mapsto a \otimes b \otimes d \otimes c$ y $p : a \otimes b \otimes c \otimes d \mapsto ac \otimes bd$. Observamos que $\kappa\left(\sum_\sigma \sigma(\xi) \otimes \alpha_{\omega\sigma}\right) = \sum_{\tau,\sigma} \sigma(\xi)\tau(\alpha_{\omega\sigma}) \otimes \tau^* = \sum_\tau \delta_{\tau\omega,I} \otimes \tau^* = 1 \otimes (\omega^{-1})^*$, luego $\sum \sigma(\xi) \otimes \alpha_{\omega\sigma} = e_{\omega^{-1}}$, es decir, que cambiar el orden de los factores de e_ω resulta en $e_{\omega^{-1}}$. A continuación podemos asumir que $\theta = g\Omega^{-1}g^{-1}$ para cierto $g \in G$. De esta forma (los sumatorios sin subíndice son respecto de $\omega \in G$, $\tau \in G$ tal que $\tau = \theta\tau\Omega$):

$$\begin{aligned}
p \circ C_{34} \circ (I \otimes I) \circ (g \otimes g)(\Delta(e_I) \cdot (e\theta \otimes e_\Omega)) &= \\
&= p \circ C_{34} \circ (I \otimes I) \circ (g \otimes g) \left(\sum (1 \otimes \alpha_{\tau\omega} \otimes \omega(\xi) \otimes 1) \cdot (e_\theta \otimes e_\Omega)\right) \\
&= p \circ C_{34} \left(\sum (1 \otimes \alpha_{\tau\omega} \otimes g\omega(\xi) \otimes 1) \cdot (e_\theta \otimes e_{g\Omega g^{-1}})\right) \\
&= p \left(\sum (1 \otimes \alpha_{\tau\omega} \otimes 1 \otimes g\omega(\xi)) \cdot (e_\theta \otimes e_{g\Omega^{-1}g^{-1}})\right) = \sum (1 \otimes \alpha_{\tau\omega} g\omega(\xi)) \cdot e_\theta \\
&= \sum (1 \otimes \alpha_{\tau g^{-1}\omega}\omega(\xi)) \cdot e_\theta = \sum_{\tau=\theta\tau\Omega} (1 \otimes \delta_{\tau g^{-1},I}) \cdot e_\theta = e_\theta \neq 0.
\end{aligned}$$

Concluimos así que $\Delta(e_I) \cdot (e_\theta \otimes e_\Omega) \neq 0$ si y solo si θ es un conjugado de Ω^{-1}. Ahora vemos que $\Delta(e_\sigma)(e_\theta \otimes e_\Omega) = \Delta(I \otimes \sigma^{-1}(e_I))(e_\theta \otimes e_\Omega) = (I \otimes I \otimes I \otimes \sigma^{-1})(\Delta(e_I)(e_\theta \otimes e_\Omega)) \neq 0$ si y solo si existe $\tau \in G$ tal que $\Omega\sigma^{-1} = \tau\sigma^{-1}\tau^{-1}$. Equivalentemente, si y solo si $\sigma = \tau\theta\tau^{-1}\Omega$ para algún $\tau \in G$, es decir, $\sigma \in \mathrm{cl}(\theta)\Omega$. Observamos ahora dos situaciones, para $\omega, \omega', \omega'' \in G$:

- Si $\omega \notin \mathrm{cl}(\omega')\,\mathrm{cl}(\omega'')$ entonces $\mathrm{cl}(\omega) \cap \mathrm{cl}(\omega')\,\mathrm{cl}(\omega'') = \emptyset$ (ya que $\mathrm{cl}(\omega')\,\mathrm{cl}(\omega'')$ es cerrado por conjugación) y en consecuencia $\Delta(E_\omega)(E_{\omega'} \otimes E_{\omega''}) = 0$.
- Si $\omega \in \mathrm{cl}(\omega')\,\mathrm{cl}(\omega'')$ entonces $\omega = g\omega' g^{-1} h\omega'' h^{-1}$ para algunos $g, h \in G$. Notamos que, como $\Delta(a'a'' \otimes b'b'') = \Delta(a' \otimes b')\Delta(a'' \otimes b'')$, entonces $\Delta(e_\omega)\Delta(E_\omega)(E_{\omega'} \otimes E_{\omega''})(e_{g\omega' g^{-1}} \otimes e_{h\omega'' h^{-1}}) = \Delta(e_\omega)(e_{g\omega' g^{-1}} \otimes e_{h\omega'' h^{-1}}) \neq 0$. Concluimos así que $\Delta(E_\omega)(E_{\omega'} \otimes E_{\omega''}) \neq 0$.

Visto esto, si $N \trianglelefteq G$ (N es un subgrupo normal de $G = \mathrm{cl}(\omega_1) \cup \cdots \cup \mathrm{cl}(\omega_r)$), entonces

$$\mathcal{I} := \bigoplus_{\omega_l \notin N} LE_{\omega_l} \trianglelefteq L \quad y \quad \Delta(\mathcal{I}) \subseteq \sum_{\{\omega_i, \omega_j\} \not\subseteq N} LE_{\omega_i} \otimes LE_{\omega_j} \subseteq L \otimes \mathcal{I} + \mathcal{I} \otimes L,\ \varepsilon(\mathcal{I}) = 0,$$

luego $\mathcal{I}$ es un coideal de L.

Recíprocamente, consideramos $\mathcal{I}$ un coideal e ideal de L. Entonces $\mathcal{I} = LE_{\omega_{l_1}} \oplus \cdots \oplus LE_{\omega_{l_s}}$ para algunos $\omega_{l_1} \ldots \omega_{l_s} \in G$. Sea $N := \bigcup_{E_{\omega_i} \notin \mathcal{I}} \mathrm{cl}(\omega_i)$. Como $\mathcal{I}$ es un coideal y $E_I = e_I$ cumple que $\varepsilon(e_I) = 1$, entonces $E_I \notin \mathcal{I}$ y consecuentemente $I \in N$. Supongamos ahora que $E_{\omega'\omega''} \in \mathcal{I}$ para algunos $\omega', \omega'' \in N$. Como $\Delta(E_{\omega'\omega''})$ tiene componente no nula en $LE_{\omega'} \otimes LE_{\omega''}$ y $\Delta(\mathcal{I}) \subseteq L \otimes \mathcal{I} + \mathcal{I} \otimes L$, $E_{\omega'} \cdot E_{\omega''}$ pertenecería a $\mathcal{I}$. Esto es absurdo porque $\omega', \omega'' \in N$ y N es cerrado por conjugación. Concluimos que $E_{\omega'\omega''} \notin \mathcal{I}$, lo que implica que $\omega'\omega''$ es conjugado de algún ω_i tal que $E_{\omega_i} \notin \mathcal{I}$. Así $\omega_i \in N$, luego $\omega'\omega'' \in N$ y concluimos que N es un subgrupo normal de G.

Queda así probado que, en el caso clásico, $\mathcal{I} \in \mathrm{Quot}(L)$ si y solo si existe $N \trianglelefteq G$ tal que $\mathcal{I} = \bigoplus_{\omega_i \notin N} LE_{\omega_i}$. Es decir, que $\mathrm{Quot}(L) = \{\bigoplus_{\omega_i \notin N} LE_{\omega_i} \mid N \trianglelefteq G\}$. Notamos como es posible establecer entonces una correspondencia biyectiva entre los elementos de $\mathrm{Quot}(L)$ y los subgrupos normales del grupo de Galois G de la extensión de Galois F/K:

$$\begin{array}{rcl} \{N \trianglelefteq G\} & \longleftrightarrow & \mathrm{Quot}(L) \\ N & \longleftrightarrow & \mathcal{I}_N := \bigoplus_{\omega_i \notin N} LE_{\omega_i} \end{array}.$$

En lo que sigue aprovecharemos esta notación $\mathcal{I}_N$ (el subíndice N indica el subgrupo normal $N \trianglelefteq G$ a partir del cual se define el coideal). No hemos de olvidar que en general no todos estos elementos de $\mathrm{Quot}(L)$ intervendrán en la correspondencia con $\mathrm{Sub}(F)$, sino que solo lo harán los admisibles. En este caso no hemos comprobado las condiciones de admisibilidad debido a que realmente no hemos determinado con exactitud a L como álgebra de Hopf, sino que hemos realizado el estudio imprescindible para determinar los elementos de $\mathrm{Quot}(L)$. Más adelante veremos cómo el estudio de los elementos admisibles de $\mathrm{Sub}(F)$ implicará inmediatamente que todos los elementos de este $\mathrm{Quot}(L)$ son admisibles.

Los elementos de $\mathrm{Sub}(F)$

Veamos a continuación que los elementos admisibles de $\mathrm{Sub}(F)$ corresponden precisamente a las subextensiones normales de la extensión F/K.

- Sea $A \in \mathrm{Sub}(F)$. Entonces A es en particular una K-subálgebra de F. Como F/K es una extensión algebraica, A es algebraico sobre K, luego todo $r \in A$ distinto de 0 posee un polinomio mínimo $m_r^K(x) = \lambda_n x^n + \cdots + \lambda_1 x + \lambda_0$ con coeficientes en K y con $\lambda_0 \neq 0$ ya que es irreducible. Observamos que si $m_r^K(r) = \lambda_n r^n + \cdots + \lambda_1 r + \lambda_0 = 0$ entonces $\lambda_0 = r(-\lambda_1 - \cdots - \lambda_n r^{n-1})$. Como $\lambda_0 \neq 0$, podemos dividir ambos lados entre λ_0 y concluimos que $r^{-1} = (-\lambda_1 - \cdots - \lambda_n r^{n-1})/\lambda_0 \in A$. Queda así probado que A es un cuerpo intermedio de la extensión F/K. Por otro lado, A es además H-subcomódulo álgebra a derecha de F, luego la aplicación $\delta|_A : A \to A \otimes H$ dada por $\delta|_A(a) = \sum_\sigma \sigma(a) \otimes \sigma^*$ debe estar bien definida. Se sigue que $\sigma(a) \in A$ para todo $a \in A$, es decir, que A/K es además una subextensión normal.
- Sea A/K una subextensión normal de F/K. Es entonces trivial que A es un H-subcomódulo álgebra de F. F/A es también una extensión de cuerpos y F es fielmente plano como A-módulo (consecuencia de ser un módulo libre, ya que A es un cuerpo), luego A es además admisible.

Con esto queda probado que todo elemento $A \in \mathrm{Sub}(F)$ es un cuerpo intermedio de F/K tal que A/K es normal, y que para toda subextensión normal A/K de F/K se cumple que A es un elemento admisible de $\mathrm{Sub}(F)$. Notamos que esto equivale a decir que

$$\{A \in \mathrm{Sub}(F) \mid A \text{ es admisible}\} \;=\; \{\mathrm{Fix}(N) \mid N \trianglelefteq G\}.$$

La correspondencia de Galois-Hopf

Una vez visto cómo son los elementos de $\mathrm{Quot}(L)$ y $\mathrm{Sub}(F)$ podemos comenzar a intuir cómo será la correspondencia de Galois-Hopf, ya que hemos comprobado como los elementos admisibles de $\mathrm{Sub}(F)$ se corresponden con las subextensiones normales de F/K mientras que los elementos de $\mathrm{Quot}(L)$ lo hacen con los subgrupos normales de $G = \mathrm{Gal}(F/K)$. Conocer el teorema fundamental de la teoría de Galois clásica nos permite saber de antemano que hay tantas subextensiones normales de F/K como subgrupos normales de G, luego podemos concluir que todos los elementos de $\mathrm{Quot}(L) = \{\bigoplus_{\omega_i \notin N} LE_{\omega_i} \mid N \trianglelefteq G\}$ son admisibles y por tanto intervienen en la correspondencia de Galois-Hopf (ya que todos los de $\mathrm{Sub}(F)$ lo son). Sea $\mathcal{I}_N = \bigoplus_{\omega_i \notin N} LE_{\omega_i} \in \mathrm{Quot}(L)$,

$$\begin{aligned}
\mathcal{F}(\mathcal{I}_N) = {}^{\mathrm{co}L/\mathcal{I}_N}F &= \{a \in F \mid \delta'(a) \in 1 \otimes 1 \otimes a + \mathcal{I}_N \otimes F\} \\
&= \left\{ a \in F \;\middle|\; \sum_{\tau \in G} \tau(a) \otimes e_\tau \in 1 \otimes 1 \otimes a + \mathcal{I}_N \otimes F \right\} \\
&= \left\{ a \in F \;\middle|\; \sum_{\tau \in G} (\tau(a) \otimes e_\tau) \cdot (E_\omega \otimes 1) = E_\omega \otimes a, \text{ para todo } \omega \in N \right\} \\
&= \left\{ a \in F \;\middle|\; \sum_{\tau \in G} (\tau(a) \otimes e_\tau) \cdot (e_\omega \otimes 1) = e_\omega \otimes a, \text{ para todo } \omega \in N \right\} \\
&= \left\{ a \in F \;\middle|\; \sum_{\tau \in G} (\tau(a) \otimes e_\tau) \cdot (e_\omega \otimes 1) = e_\omega \otimes a \cdot 1 \otimes e_\tau, \text{ para todo } \tau \in G, \omega \in N \right\}.
\end{aligned} \tag{2.7}$$

Utilizando de nuevo el elemento ξ tal que $\{\sigma(\xi)\}_{\sigma \in G}$ es una K-base de F,

$$\begin{aligned}
(\tau(a) \otimes e_\tau) \cdot (1 \otimes e_\tau) &= \sum_{\sigma \in G} (\tau(a) \otimes \alpha_{\tau\sigma} \otimes \sigma(\xi)) \cdot (e_\omega \otimes 1) \\
&= \sum_{\sigma \in G} (\tau(a)\alpha_{\omega\tau\sigma} \otimes 1 \otimes 1)(e_\omega \otimes 1)(1 \otimes 1 \otimes \sigma(\xi)).
\end{aligned} \tag{2.8}$$

Por otro lado,

$$\begin{aligned}
(e_\omega \otimes a) \cdot (1 \otimes e_\tau) &= (e_\omega \otimes 1) \cdot (1 \otimes \tau(a) \otimes 1 \otimes e_\tau) \\
&= \sum_{\sigma \in G} (e_\omega \otimes 1) \cdot (1 \otimes \tau(a) \otimes 1) \cdot (1 \otimes \alpha_{\tau\sigma} \otimes \sigma(\xi)).
\end{aligned} \tag{2.9}$$

Combinando 2.8 y 2.9 se sigue que, como la familia $\{\sigma(\xi)\}_{\sigma \in G}$ es libre, la igualdad que aparece en el último término de 2.7 es cierta si y solo si $(\tau(a)\alpha_{\omega\tau\sigma} \otimes 1) \cdot e_\omega = e_\omega \cdot (1 \otimes \tau(a)\alpha_{\tau\sigma})$ para todo $\sigma \in G$. Concluimos así que la igualdad del último término de 2.7 es cierta si y solo si $\tau(a) = \omega\tau(a)$, o lo que es lo mismo, $a = \tau^{-1}\omega\tau(a)$. Como N es un subgrupo normal,

$$\begin{aligned}
\mathcal{F}(\mathcal{I}_N) = {}^{\mathrm{co}L/\mathcal{I}_N}F &= \left\{ a \in F \;\middle|\; a = \tau^{-1}\omega\tau(a), \text{ para todo } \tau \in G, \omega \in N \right\} \\
&= \{a \in F \mid \omega(a) = a, \text{ para todo } \omega \in N\} = \mathrm{Fix}(N).
\end{aligned}$$

Con esto queda claro cómo cada subgrupo normal $N \trianglelefteq G$ se corresponde con cada $\mathrm{Fix}(N) \in \mathrm{Sub}(F)$, a través de un elemento $\mathcal{I}_N \in \mathrm{Quot}(L)$ y la aplicación $\mathcal{F}$. Solo falta ver la dirección inversa, es decir, estudiar el comportamiento de la aplicación $\mathcal{G} : \mathrm{Sub}(F) \to \mathrm{Quot}(L)$ (y comprobar que $\mathcal{F}$ y $\mathcal{G}$ son mutuamente inversas). Recordamos que estaba definida de tal forma que, para $B \in \mathrm{Sub}(F)$, $L/\mathcal{G}(B) = (F \otimes_B F)^{\mathrm{co}H}$. No obstante, en la demostración de la proposición 2.39 comprobamos que esta definición equivale a $\mathcal{G}(B) := L \cap \ker(F \otimes F \to F \otimes_B F)$. Si tomamos $B \in \mathrm{Sub}(F)$, este será igual a cierto $\mathrm{Fix}(N)$, con $N \trianglelefteq G$. En este caso:

$$\begin{aligned}
\mathcal{G}(\mathrm{Fix}(N)) &:= L \cap \ker(F \otimes F \to F \otimes_{\mathrm{Fix}(N)} F) \\
&= L \cap \mathrm{span}\,\langle ab \otimes c - a \otimes bc \mid a, c \in F,\ b \in B \rangle \\
&= L \cap \mathrm{span}\left\langle \sum_{\sigma \in G} \Big((ab\sigma(c) - a\sigma(b)\sigma(c)) \otimes 1 \Big) \cdot e_\sigma \;\middle|\; a, c \in F,\ b \in B \right\rangle \qquad (2.10) \\
&= L \cap \mathrm{span}\left\langle \sum_{\sigma \notin N} \Big((a(b - \sigma(b))\sigma(c)) \otimes 1 \Big) \cdot e_\sigma \;\middle|\; a, c \in F,\ b \in B \right\rangle
\end{aligned}$$

Denotamos por P a la segunda parte de la intersección de 2.10 (notamos que en el último término de esta expresión $(b - \sigma(b)) \neq 0$). P es un ideal de $F \otimes F$, ya que es el núcleo del cociente $F \otimes F \to F \otimes_{\mathrm{Fix}(N)} F$. Entonces para todo $x \in P$, $\sigma \in G$ se tiene que $e_\sigma \cdot x \in P$. Es claro que $e_\sigma \in P$ si y solo si $\sigma \notin N$, y es entonces inmediato que $P = \bigoplus_{\sigma \notin N} (F \otimes F) e_\sigma$. Ahora bien, como $L = \bigoplus_{i=1}^{r} L E_{\omega_i}$, concluimos que

$$\mathcal{G}(\mathrm{Fix}(N)) = \left(\bigoplus_{\omega_i \in G} L E_{\omega_i} \right) \cap \left(\bigoplus_{\sigma \notin N} (F \otimes F) \cdot e_\sigma \right) = \bigoplus_{\omega_i \notin N} L E_{\omega_i} = \mathcal{I}_N \,.$$

Vemos así como $\mathcal{G}(\mathrm{Fix}(N))$ es precisamente el elemento $\mathcal{I} \in \mathrm{Quot}(L)$ definido a partir de N, luego $\mathcal{F}$ y $\mathcal{G}$ son mutuamente inversas. Con esto queda comprobado como a través del teorema fundamental de la teoría de Galois Hopf es posible establecer una correspondencia biyectiva entre los subgrupos normales de $G = \mathrm{Gal}(F/K)$ y las subextensiones normales de F/K:

$$\begin{array}{ccccccc}
\{N \trianglelefteq G\} & \leftrightarrow & \left\{ \mathcal{I} \in \mathrm{Quot}(L) \text{ admisibles} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} A \in \mathrm{Sub}(F) \\ \text{admisibles} \end{array} \right\} & \leftrightarrow & \left\{ \begin{array}{c} \text{Subext.} \\ \text{normales} \\ \text{de } F/K \end{array} \right\} \\
N & \leftrightarrow & \mathcal{I}_N = \bigoplus_{\omega_i \notin N} L E_{\omega_i} = \mathcal{G}(\mathrm{Fix}(N)) & \underset{\mathcal{G}}{\overset{\mathcal{F}}{\rightleftarrows}} & \mathcal{F}(\mathcal{I}_N) = \mathrm{Fix}(N) & \leftrightarrow & \mathrm{Fix}(N)/K
\end{array}.$$

Para las extensiones de Galois de cuerpos con grupo de Galois abeliano, queda demostrado que el teorema fundamental de la teoría de Galois-Hopf es equivalente al clásico. Para el resto de casos, esta correspondencia no es la clásica, ya que existen subgrupos y subextensiones que no intervienen al utilizar la teoría de Galois-Hopf (en concreto los subgrupos $M < G$ no normales y por tanto las subextensiones $\mathrm{Fix}(M)/K$). Podemos interpretar esta correspondencia como una restricción de la correspondencia de Galois clásica a los subgrupos y subextensiones normales.

Conclusión

La teoría estudiada en este trabajo es, en términos relativos, muy reciente. Es por ello que la redacción de esta memoria ha sido un desafío muy imponente, ya que la cantidad de recursos y artículos matemáticos asequibles al respecto es escasa y sus explicaciones son más técnicas de lo que acostumbra la carrera. He notado esto especialmente con la teoría de Galois-Hopf en el capítulo 2, cuyo estudio ha sido un interesante acercamiento a cómo es el mundo de la investigación. No obstante y tras todas las dificultades, el objetivo de este trabajo está cumplido: comprender una generalización de la teoría de Galois y estudiar el comportamiento del caso clásico.

La teoría de Galois-Hopf aún parece tener mucho camino por recorrer, pues a partir de cierto momento la teoría parece divergir por varios caminos. Como ya se ha visto en el ejemplo 2.43, el teorema fundamental en su estado actual no generaliza bien las extensiones clásicas cuyo grupo de Galois es no abeliano, por lo que aún estamos lejos de una teoría que generalice a extensiones de anillos no conmutativos sin comprometer la teoría de Galois clásica. Lamentablemente el tamaño de este documento no permite profundizar más de lo estrictamente necesario para alcanzar el enunciado del teorema fundamental, obligando a dejar en el tintero algunas observaciones y ejemplos interesantes.

Más allá de todo lo estudiado y aprendido, me llevo la experiencia de enfrentarme a un reto que ha exigido toda mi dedicación. La satisfacción de comprender los pasos a seguir para alcanzar un resultado tras incontables esfuerzos y darle la estructura y redacción adecuadas no tiene igual. Las dificultades de lidiar con una teoría tan reciente y tratar no solo de comprenderla sino también de explicarla dentro de los límites de espacio y tiempo del trabajo me han ayudado a mejorar mi capacidad crítica, mi rigurosidad y mi redacción. Eso es, por encima de todo, lo que se queda conmigo tras el trabajo.

Apéndice I. Módulos

Definición 2.47 (Módulo a izquierda)**.** Sea R un anillo. Un **R-módulo a izquierda** es un grupo abeliano M junto con una acción a izquierda $(r, x) \mapsto rx$ de R en M, tal que:

1. $r(sx) = (rs)x$,
2. $(r + s)x = rx + sx$, $r(x + y) = rx + ry$.

para todo $r \in R$, $x, y \in M$. Si R es unitario, entonces el R-módulo a izquierda M es unitario si $1_R x = x$ para todo $x \in M$.

Nota 2.48. La definición de módulo a derecha es análoga a la de módulo a izquierda, pero con una acción a derecha en lugar de a izquierda. La notación ${}_R M$ (M_R) indica que M es un R-módulo a izquierda (a derecha).

Definición 2.49 (Opuesto de un anillo)**.** Sea $R = (R, +, \cdot)$ un anillo. Llamamos **opuesto** de R al anillo $R^{\text{op}} = (R, +, *)$, cuya multiplicación $*$ está definida por $a * b = b \cdot a$, para todo $a, b \in R$.

Proposición 2.50. *Todo R-módulo a derecha (unitario) es un R^{op}-módulo a izquierda (unitario), y viceversa.*

Corolario 2.51. *Si R es un anillo conmutativo, entonces todo R-módulo a izquierda es también R-módulo a derecha, y viceversa.*

Definición 2.52 (Submódulo)**.** Sea M un R-módulo a izquierda. Un subgrupo aditivo A de M es un **R-submódulo** de M si $x \in A$ implica que $rx \in A$ para todo $r \in R$.

Definición 2.53 (Homomorfismo de módulos a izquierda)**.** Sean A y B dos R-módulos a izquierda. Un **homomorfismo de R-módulos a izquierda** es una aplicación $\varphi : A \to B$ tal que, para todo $x, y \in A$, $r \in R$, se verifican:

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$,
2. $\varphi(rx) = r\varphi(x)$.

Definición 2.54 (Independencia lineal)**.** Sea M un R-módulo a izquierda. Un subconjunto $S \subset M$ se dice **linealmente independiente** sobre R (o R-linealmente independiente) si, dados $r_s \in R$ para cada $s \in S$ y $r_s = 0$ para casi todo $s \in S$, $\sum_{s \in S} r_s s = 0$ implica que $r_s = 0$ para todo $s \in S$. Diremos que S es R-linealmente dependiente si no es linealmente independiente.

Definición 2.55 (Módulo libre)**.** Una **base** de un R-módulo a izquierda M es un subconjunto linealmente independiente de M que genera M. Un módulo es **libre** si tiene alguna base.

Definición 2.56 (Módulo proyectivo)**.** Un R-módulo a izquierda M se dice **proyectivo** si cumple la siguiente propiedad: sean $\varphi : P \to N$ y $\rho : M \to N$ homomorfismos de R-módulos a izquierda, con ρ sobreyectivo. Entonces $\varphi = \rho \circ \psi$ para algún homomorfismo $\psi : P \to M$.

Proposición 2.57. *Todo módulo libre es proyectivo.*

Definición 2.58 (Retracto)**.** Un **retracto** de un módulo M es otro módulo M_0 para el cual existen homomorfismos de módulos $\iota : M_0 \to M$ y $r : M \to M_0$ de modo que $r \circ \iota = id_{M_0}$.

Proposición 2.59. *Un retracto de un módulo proyectivo es proyectivo.*

Proposición 2.60. *Un módulo es proyectivo si y solo si es isomorfo a un sumando directo de un módulo libre.*

Definición 2.61 (Dual de un módulo)**.** Sea M un R-módulo a izquierda (derecha). Denotamos por M^* y llamamos **R-módulo dual** de M al conjunto de homomorfismos de R-módulos que van de M a R, que tiene estructura de R-módulo a derecha (izquierda) con la operación punto por punto.

Proposición 2.62. *Sea F un R-módulo libre a izquierda (derecha) con base finita $\{e_i\}_{i\in I}$. Entonces F^* es también libre y la familia finita $\{e_i^*\}_{i\in I}$ es base de F^*, donde $e_i^*(e_j) = \delta_{i,j}$ para cada $i, j \in I$.*

Apéndice II. Producto tensorial

Definición 2.63 (Aplicación bilineal)**.** Sea R un anillo conmutativo y sean A, B, C R-módulos. Una aplicación $\beta : A \times B \to C$ se dice **bilineal** si para cualesquiera $a, a' \in A$, $b, b' \in B$, $r \in R$ se verifican:

1. $\beta(a + a', b) = \beta(a, b) + \beta(a', b)$
2. $\beta(a, b + b') = \beta(a, b) + \beta(a, b')$
3. $\beta(ra, b) = r\beta(a, b) = \beta(a, rb)$

Proposición 2.64. *Sean R un anillo, A un R-módulo a derecha, B un R-módulo a izquierda, y C un grupo abeliano. Para una aplicación $\beta : A \times B \to C$ equivalen:*

1. *Para todo $a, a' \in A$, $b, b' \in B$, $r \in R$ se cumple que $\beta(a + a', b) = \beta(a, b) + \beta(a', b)$, $\beta(a, b + b') = \beta(a, b) + \beta(a, b')$, y $\beta(ra, b) = \beta(a, rb)$.*
2. *$a \mapsto \beta(a, -)$ es un homomorfismo de módulos de A a $\mathrm{Hom}_{\mathbb{Z}}(B, C)$.*
3. *$b \mapsto \beta(-, b)$ es un homomorfismo de módulos de B a $\mathrm{Hom}_{\mathbb{Z}}(A, C)$.*

Definición 2.65 (Bihomomorfismo)**.** Un **bihomomorfismo** de módulos es una aplicación que satisface las condiciones equivalentes de la proposición 2.64.

Definición 2.66 (Producto tensorial)**.** Sean A un R-módulo a derecha y B un R-módulo a izquierda. Un **producto tensorial** de A y B es un grupo abeliano $A \otimes_R B$ junto con un bihomomorfismo $\tau : A \times B \to A \otimes_R B$, $(a, b) \mapsto a \otimes b$, la aplicación tensorial, tal que para cada grupo abeliano C y bihomomorfismo $\beta : A \times B \to C$ existe un único homomorfismo $\bar{\beta} : A \otimes_R B \to C$ tal que $\beta = \bar{\beta} \circ \tau$.

Proposición 2.67. *Para cualesquiera R-módulo a derecha A y R-módulo a izquierda B, existen $A \otimes_R B$ y su aplicación tensorial. Además, son únicos salvo isomorfismo.*

Corolario 2.68. *Todo elemento de $A \otimes_R B$ es una suma finita $\sum_i a_i \otimes b_i$, donde $a_i \in A$ y $b_i \in B$. Si $\sum_i a_i \otimes b_i = 0$ en $A \otimes_R B$, entonces $\sum_i a_i \otimes b_i = 0$ en $A' \otimes_R B'$ para ciertos submódulos finitamente generados $A' \subseteq A$, $B' \subseteq B$.*

Apéndice III. Álgebras sobre anillos conmutativos

Definición 2.69 (Álgebra sobre un anillo conmutativo)**.** Sea R un anillo conmutativo. Un álgebra sobre R (o R-álgebra) es un R-módulo A con un elemento identidad $1 = 1_A$ y una multiplicación que verifican, para todo $a, b, c \in A$, $r \in R$:

1. $a(b + c) = ab + ac$, $(a + b)c = ac + bc$
2. $(ra)b = a(rb) = r(ab)$
3. $a(bc) = (ab)c$
4. $1a = a = a1$

Definición 2.70 (Homomorfismo de álgebras)**.** Un **homomorfismo de R-álgebras** es un homomorfismo de anillos que además es homomorfismo de R-módulos.

Definición 2.71 (Subálgebra)**.** Sean A una R-álgebra y S un subconjunto de A. S se dice R-subálgebra de A si es a la vez subanillo y R-submódulo de A.

Proposición 2.72. *Si A y B dos R-álgebras, $A \otimes B$ es también un R-álgebra, con la multiplicación $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ para todo $a, a' \in A$, $b, b' \in B$.*

Demostración. Tanto $\otimes$ como las multiplicaciones de A y B son bilineales, luego la aplicación

$$\begin{array}{rcl} A \times B \times A \times B & \longrightarrow & A \otimes B \\ (a, b, a', b') & \longmapsto & aa' \otimes bb' \end{array}$$

es multilineal. Se sigue que existe un único homomorfismo de módulos $\mu : A \otimes B \otimes A \otimes B \to A \otimes B$ tal que $\mu(a \otimes b \otimes a' \otimes b') = aa' \otimes bb'$ para cualesquiera $a, a' \in A$, $b, b' \in B$. □

Apéndice IV. Dual de un álgebra de Hopf

Proposición 2.73. *Sean R un anillo conmutativo unitario y $H = (H, m, \eta, \Delta, \varepsilon, S)$ una R-álgebra de Hopf de rango finito. Entonces su dual $H^* = (H^*, \Delta^*, \varepsilon^*, m^*, \eta^*, S^*)$ es también una R-álgebra de Hopf.*

Proposición 2.74. *Sean R un anillo conmutativo unitario y $H = (H, m, \eta, \Delta, \varepsilon, S)$ una R-álgebra de Hopf de rango finito. Si A es un H-comódulo álgebra a derecha (izquierda), entonces es también un H^*-módulo álgebra a izquierda (derecha) mediante la acción*

$$h \cdot a := f(a_{(1)})a_{(0)},$$

con $h \in H^*$ y $a \in A$ (entendemos que hemos omitido el sumatorio), y $A^{H^*} = A^{coH}$. Dualmente, si B es un H-módulo álgebra a izquierda (derecha) entonces B es además un H^*-comódulo álgebra a derecha (izquierda) y $B^H = B^{coH^*}$.

Bibliografía

[1] S. Caenepeel y J. Vercruysse Hopf algebras, *Vrije Universiteit Brussel*, (2018).

[2] H. Cartan y S. Eilenberg Homological Algebra, *Princeton University Press*, (1956).

[3] S. U. Chase, D. K. Harrison y A. Rosenberg, Galois theory and cohomology of commutative rings, *Amer. Math. Soc.* **52**, (1965).

[4] S. U. Chase y M. E. Sweedler, Hopf algebras and Galois theory, *Lecture Notes in Math.* **97**, (1969).

[5] F. Chamizo, ¡Qué bonita es la teoría de Galois!, *Universidad Autónoma de Madrid*, (2005).

[6] T. Crespo, A. Rio y M. Vela, From Galois to Hopf Galois: theory and practice, *Spanish Science Ministry*, (2014).

[7] Y. Doi y M. Takeuchi, Hopf-Galois extensions of algebras, the Miyashita-Ulbrich action, and Azumaya algebras, *J. Algebra* **121**, (1989).

[8] A. Elduque, Groups and Galois Theory, *Universidad de Zaragoza*, (2009).

[9] P. A. Grillet, Abstract Algebra, *Grad. Texts in Math., Springer*, (2007).

[10] S. Montgomery, Hopf Galois Theory: A survey, *Geometry & Topology Monographs* **16**, (2009).

[11] P. Schauenburg, Hopf bigalois extensions, *Comm. Alg.* **24(12)**, (1996), 3797–3825.

[12] P. Schauenburg, A bialgebra that admits a Hopf-Galois extension is a Hopf algebra, *Proc. Amer. Math. Soc.* **125(1)**, (1997).

[13] P. Schauenburg, Galois Correspondences for Hopf Bigalois Extensions, *J. Algebra* **20**, (1998).

[14] P. Schauenburg, Hopf-Galois and Bi-Galois Extensions, *Fields Inst. Commun.*, (2004).

[15] H. J. Schneider, Representation theory of Hopf-Galois extensions, *Israel I. of Math.* **72**, (1990).