UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Extensions finites Hopf Galois

Autor: Yasmina Bañuelos Villanueva

Director: Dra. Teresa Crespo
Realitzat a: Departament de Matemàtiques i Informàtica
Barcelona, 20 de juny de 2021

Abstract

Galois theory is one of the most famous in the mathematics field. This theory usually uses groups as the main structure of study. We'll work to find a generalization of this theory, which will consist of using a more complex structure, the Hopf algebra. In the end, we'll be able to find a relationship between a Hopf algebra associated with a Hopf Galois extension and a regular subgroup of permutations. This final result will be the one that will enable us to explicitly compute a Hopf algebra given the regular subgroup.

Resum

La teoria de Galois és una de les més famoses de les matemàtiques. Aquesta fa servir grups com a estructura principal. En aquest treball veurem una generalització d'aquesta teoria, usant àlgebres de Hopf, obtindrem un resultat que ens donarà una bijecció entre el conjunt d'estructures Hopf Galois i el conjunt de subgrups regulars d'un cert grup de permutacions. Aquest resultat serà el que ens permetrà recuperar una àlgebra de Hopf a partir del subgrup regular associat.

2020 Mathematics Subject Classification. 11R32, 11S20, 12F10, 57T05, 16T05, 16T10

Agraïments

Vull agrair als meus pares, el suport durant aquests anys. A les meves amigues de tota la vida, la seva infinita paciència. A la meva àvia per haver estat una fan incondicional. Als amics de la facultat, que els portaré al cor sempre, haver-me ajudat a resoldre infinitat de problemes. I en especial a la tutora del treball, sense la qual aquest treball no hagués estat possible de realitzar. Gràcies.

Índex

1 Introducció

En aquest capítol donarem les definicions bàsiques que ens caldran per veure els resultats que proverem endevant. Començarem donant la definició general de producte tensorial i algunes propietats d'aquest [7]. Usarem aquestes per definit l'estructura d'àlgebra sobre un cos K que notarem per (A, m_A, λ_A). Aleshores extendrem aquesta definició usant el dual obtenint la coàlgebra $(C, \Delta_c, \epsilon_C)$, i a continuació la biàlgebra $(B, m_B, \lambda_B, \Delta_B, \epsilon_B)$. Finalment veurem com es defineix una àlgebra de Hopf sobre un cos K, estructura que usarem freqüentment als següents capítols.

1.1 Producte tensorial

Siguin R un anell, $M_1, M_2, \dots M_n$ n R-mòduls on n és un natural $n \geq 2$, i A un R-mòdul.

Definició 1.1. Una aplicació $f : M_1 \times M_2 \times \cdots \times M_n \longrightarrow A$ és R-n-**lineal** si per a tot i, $1 \leq i \leq n$, i tot $a_i, a_{i'} \in M_i$, $r \in R$,

(i) $f(a_1, a_2 \dots, a_i + a_{i'}, \dots, a_n) = f((a_1, a_2 \dots, a_i, \dots, a_n) + f(a_1, a_2 \dots, a_{i'}, \dots, a_n)$,

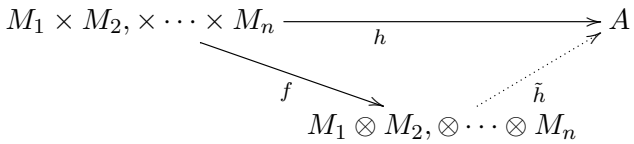
(ii) $f(a_1, a_2 \dots, ra_i, \dots, a_n) = rf(a_1, a_2 \dots, a_i, \dots, a_n)$.

Notem que si una aplicació és R-bilineal és equivalent a que sigui R-2-lineal.

Definició 1.2. Definim el **producte tensorial** de $M_1, M_2, \dots M_n$ sobre R com un R-mòdul $M_1 \otimes M_2, \otimes \cdots \otimes M_n$ amb una aplicació R-n-lineal

$$f : M_1 \times M_2, \times \cdots \times M_n \longrightarrow M_1 \otimes M_2, \otimes \cdots \otimes M_n.$$

De manera per qualsevol R-mòdul A i per qualsevol funció R-n-lineal $h : M_1 \times M_2, \times \cdots \times M_n \to A$ existeix un únic morfisme de R-mòduls $\tilde{h} : M_1 \otimes M_2, \otimes \cdots \otimes M_n \to A$, $\tilde{h}f = h$, i el següent diagrama commuta.



Parlem de "producte tensorial en algun tipus d'associació"quan fem referència a un producte tensorial els factors del qual són productes tensorials o productes tensorials de productes tensorials.

Per exemple pels R-mòduls M_1, M_2, M_3 podem considerar els seus productes associats

$$M_1 \otimes (M_2 \otimes M_3) \text{ i } (M_1 \otimes M_2) \otimes M_3,$$

aleshores podem definir l'isomorfisme d'R-mòduls de la manera natural.

$$\begin{array}{rccc} \varphi : & M_1 \otimes M_2 \otimes M_3 & \to & (M_1 \otimes M_2) \otimes M_3 \\ & a_1 \otimes a_2 \otimes a_3 & \longmapsto & (a_1 \otimes a_2) \otimes a_3. \end{array}$$

Proposició 1.3. Siguin $M_1, M_2, \dots, M_n$ R-mòduls. Sigui S un producte tensorial iterat de $M_1, M_2, \dots, M_n$ en algun tipus d'associació. Aleshores existeix un isomorfisme natural de manera que $M_1 \otimes M_2 \otimes \cdots \otimes M_n \cong S$.

1.2 Àlgebres

Per a les següents definicions del capítol K serà un cos.

Definició 1.4. Una K-**àlgebra** és un triplet (A, m_A, λ_A), on A és un espai vectorial sobre K, $m_A : A \otimes_K A \longrightarrow A$ i $\lambda_A : K \longrightarrow A$ són aplicacions K-lineals satisfent les següents propietats.

(i) El següent diagrama és commutatiu.

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{I_a \otimes m_A} & A \otimes A \\ \downarrow{\scriptstyle m_A \otimes I_A} & & \downarrow{\scriptstyle m_A} \\ A \otimes A & \xrightarrow[m_A]{} & A \end{array}$$

On $I_A : A \to A$ denota la aplicació identitat, i les aplicacions $I_A \otimes m_A, m_A \otimes I_A : A \otimes A \otimes A \longrightarrow A \otimes A$ estan definides per $a \otimes b \otimes c \longmapsto a \otimes m_A(b \otimes c)$, $a \otimes b \otimes c \longmapsto m_A(a \otimes b) \otimes c$, per tot $a, b, c \in A$. I les aplicacions $s_1 : K \otimes A \to A, s_2 : A \otimes K \to A$ estan definides per $r \otimes a \longmapsto ra$ i $a \otimes r \longmapsto ra$ respectivament. Anomenem m_A l'aplicació producte. De la commutativitat del diagrama obtenim la **propietat associativa** definida de la següent manera.

$$m_A(I_A \otimes m_A)(a \otimes b \otimes c) = m_A(m_A \otimes I_A)(a \otimes b \otimes c),\ a, b, c \in A. \tag{1.1}$$

(ii) El següent diagrama és commutatiu.

$$\begin{array}{ccc} A \otimes K & \xrightarrow{I_a \otimes \lambda_A} & A \otimes A \\ \downarrow{\scriptstyle s_2} & \searrow^{m_A} & \uparrow{\scriptstyle \lambda_A \otimes I_A} \\ A & \xleftarrow{s_1} & K \otimes A \end{array}$$

On les aplicacions $I_A \otimes \lambda_A$, $\lambda_A \otimes I_A$ estan definides per $a \otimes r \longmapsto a \otimes \lambda_A(r)$, $r \otimes a \longmapsto \lambda_A(r) \otimes a$, per tot $a \in A$, $r \in K$. Anomenem aplicació unitat a λ_A. De la commutativitat del diagrama obtenim la **propietat unitat** definida de la següent manera.

$$m_A(I_A \otimes \lambda_A)(a \otimes r) = ra = m_A(\lambda_A \otimes I_A)(r \otimes a),\ a, b, c \in A. \tag{1.2}$$

Observació 1.5. Posant $ab = \lambda_A(a \otimes b)$, per a $a, b \in A$, i $1_A = \lambda_A(1_K)$, recuperem la definició habitual (anterior) de K-àlgebra amb unitat 1. A continuació farem servir ambdues notacions.

Definició 1.6. Diem que una K-àlgebra (A, m_A, λ_A) és **commutativa** si

$$m_A \tau = m_A,$$

on τ denota la aplicació transposició definida per $\tau(a \otimes b) = b \otimes a$, per $a, b \in A$.

Definició 1.7. Donada una K-àlgebra (A, m_A, λ_A), aquesta serà **finita** si i només si té dimensió finita com a K espai vectorial.

Siguin A, B K-àlgebres. El producte tensorial $A \otimes B$ té l'estructura de K-àlgebra amb aplicació producte: $m_{A\otimes B} : (A\otimes B)\otimes(A\otimes B) \longrightarrow A\otimes B$ definida per $(a\otimes b)\otimes(a'\otimes b') \longmapsto m_A(a \otimes a') \otimes m_B(b \otimes b')$; notem que apliquem una permutació de manera que $a' \longmapsto b$. L'aplicació unitat de la K-àlgebra serà:

$$\begin{aligned} \lambda_{A\otimes B} : & K \longrightarrow A \otimes B \\ & r \longmapsto \lambda_A(r) \otimes 1_B. \end{aligned}$$

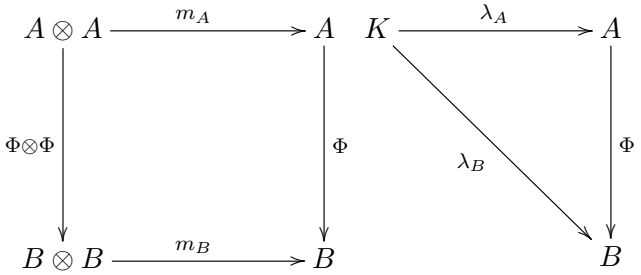
Definició 1.8. Siguin $(A, m_A, \lambda_A), (B, m_B, \lambda_B)$ K-àlgebres. Un **morfisme de K-àlgebres** de A a B és una aplicació Φ que satisfà les condicions següents.

(i) Φ és K-lineal.

(ii) $\Phi \circ m_A = m_B \circ (\Phi \otimes \Phi)$.

(iii) $\lambda_B = \Phi \circ \lambda_A$.

Observem que les dos darreres condicions equivalen a que els següents diagrames siguin commutatius.



Exemple 1.9. Sigui G un grup finit qualsevol amb element unitat 1. L'**àlgebra de grup** denotada per $K[G]$ és una K-àlgebra formada per elements que podem expressar com

$$K[G] = \left\{ \sum_{g\in G} \lambda_g g : \lambda_g \in K \right\}.$$

Notem que podem donar les aplicacions producte i unitat d'aquesta àlgebra només pels elements de G. Aquestes estan definides per $m_{K[G]} : K[G] \otimes_K K[G] \to K[G]$ amb $g \otimes h \longmapsto gh$, i $\lambda_{K[G]} : K \to K[G]$ amb $r \longmapsto r1$, per qualsevol $g, h \in G, r \in K$.

Observem que com K és un cos, la imatge per $\lambda_{K[G]}$ de K és isomorfa a K; per tant $K[G]$, com a K-espai vectorial, té dimensió igual a l'ordre de G; ho podem veure fent servir la identificació $\phi : K \to K[G]$, $r \longmapsto r1$.

1.3 Coalgebres

A continuació definirem les coàlgebres, estructura que podem pensar com el dual d'una àlgebra. Essencialment definim les coàlgebres "donant la volta"a les fletxes de les aplicacions estructurals que defineixen l'àlgebra.

Definició 1.10. Una K**-coàlgebra** és una tripleta $(C, \Delta_C, \epsilon_C)$ formada per un espai vectorial C sobre K i aplicacions K-lineals $\Delta_C : C \longrightarrow C \otimes_K C$ i $\epsilon_C : C \longrightarrow K$ que satisfan les condicions següents.

(i) El diagrama commuta:

$$\begin{array}{ccc} C & \xrightarrow{\Delta_C} & C \otimes C \\ {\scriptstyle \Delta_C}\downarrow & & \downarrow{\scriptstyle I_C \otimes \Delta_C} \\ C \otimes C & \xrightarrow[\Delta_C \otimes I_C]{} & C \otimes C \otimes C \end{array}$$

On $I_C : C \to C$ denota l'aplicació identitat, i les aplicacions $I_C \otimes \Delta_C : C \otimes C \to C \otimes C \otimes C$, $\Delta_C \otimes I_C : C \otimes C \to C \otimes C \otimes C$ estan definides respectivament per $a \otimes b \longmapsto a \otimes \Delta_C(b)$ i $a \otimes b \longmapsto \Delta_C(a) \otimes b$ per tot $a, b \in C$. Anomenem coproducte l'aplicació Δ_C. De la mateixa manera, per la commutativitat del diagrama obtenim la **propietat coassociativa** definida de la següent manera.

$$(I_C \otimes \Delta_C)\Delta_C(c) = (\Delta_C \otimes I_C)\Delta_C(c), \ \forall c \in C. \tag{1.3}$$

(ii) El diagrama commuta:

$$\begin{array}{ccc} C & \xrightarrow{1 \otimes -} & K \otimes C \\ {\scriptstyle -\otimes 1}\downarrow & \searrow^{\Delta_C} & \uparrow{\scriptstyle \epsilon_C \otimes I_C} \\ C \otimes K & \xleftarrow[I_C \otimes \epsilon_C]{} & C \otimes C \end{array}$$

Les aplicacions $-\otimes 1$ i $1 \otimes -$ estan definides per $c \longmapsto c \otimes 1$, $c \longmapsto 1 \otimes c$ respectivament. Anomenem counitat l'aplicació ϵ_C. De la mateixa manera, se satisfan les següents propietats per la commutativitat del diagrama.

$$(\epsilon_C \otimes I_C)\Delta_C(c) = 1 \otimes c, \ (I_C \otimes \epsilon_C)\Delta_C(c) = c \otimes 1, \ \forall c \in C \tag{1.4}$$

Definició 1.11. Diem que una K-coalgebra C és **cocomutativa** quan satisfà:

$$\tau(\Delta_C(c)) = \Delta_C(c) \text{ per tot } c \in C.$$

Exemple 1.12. Un cos K és un K-espai vectorial sobre ell mateix i una K-coàlgebra, on el coproducte $\Delta_K : K \to K \otimes K$ ve donat per $\Delta_K(a) = a \otimes 1$. I la counitat $\epsilon_K : K \to K$ és definida per $\epsilon_K(a) = a$. Aquesta K-coàlgebra s'anomena la **coàlgebra trivial**.

Definició 1.13. Sigui C una K-coàlgebra. Un element no nul de c de C serà **grupal** si satisfà que $\Delta_C(c) = c \otimes c$.

Proposició 1.14. Sigui c un element grupal de la K-coàlgebra C. Llavors $\epsilon_C(c) = 1$.

Proposició 1.15. Sigui C una K-coàlgebra i posem $G(C)$ al conjunt dels elements grupals de C. Aleshores $G(C)$ és un subconjunt K-linealment independent de C.

Donem ara un petit resultat sobre elements grupals extret de [5].

Corołari 1.16. *Un element f de $H^* = Hom(H, K)$ és grupal si i només si f és un homomorfisme de K-àlgebres de H a K. Determinat per*

$$\Delta(f)(x \otimes y) = f(xy).$$

Així $\Delta(f) = f \otimes f$ si i només si $f(xy) = f(x)f(y)$ per tot $x, y \in H$.

Observem que existeix una relació via el dual entre les àlgebres i les coàlgebres. Veiem que donat un K-espai vectorial V podem considerar l'aplicació

$$\begin{array}{rccc} \varphi: & V^* \otimes V^* & \longrightarrow & (V \otimes V)^* \\ & w_1 \otimes w_2 \to v_1 \otimes v_2 & \longmapsto & w_1(v_1)w_2(v_2) \end{array}$$

que és un monomomorfisme, i és isomorfisme si només si $\dim(V) < \infty$. Aleshores quan considerem el dual de les aplicacions producte i unitat d'una K-àlgebra A

$$m_A : A \otimes A \to A \;\Rightarrow\; (m_A)^* : A^* \to (A \otimes A)^*,$$

$$\lambda_A : K \longrightarrow A \;\Rightarrow\; (\lambda_A)^* : A^* \longrightarrow K.$$

Aleshores, identificant $(A \otimes A)^*$ amb $A^* \otimes A^*$ obtenim que $(A^*, m_A^*, \lambda_A^*)$ és una coàlgebra si A és una K-àlgebra finita. I, donada C una K-coàlgebra, el seu dual serà una K-àlgebra amb producte i unitat induïdes pel dual del coproducte i la counitat independentment de la dimensió de C.

Introdiïm ara la **notació de Sweedler** que usem per reescriure la imatge per l'aplicació coproducte. Sigui C una K-coalgebra, per a $c \in C$ la imatge d'aquest element per Δ_C és una suma de la forma $\sum_{(i)} a_i \otimes b_i$.

La notació de Sweedler proposa simplificar l'expressió anterior usant que per a operacions on només es fan transformacions lineals no cal indexar per (i), d'on obtenim que

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

Usant la notació de Sweedler podem reescriure l'expressió de la propietat coassociativa. Expressem la primera banda de la igualtat com

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

$$\sum_{(c),(c_{(2)})} c_{(1)} \otimes c_{(2_{(1)})} \otimes c_{(2_{(2)})}, \tag{1.5}$$

i la segona com

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

$$= \sum_{(c_{(1)}),(c)} c_{(1_{(1)})} \otimes c_{(1_{(2)})} \otimes c_{(2)}. \tag{1.6}$$

Tenint en compte que les expressions que obtenim a 1.5 i 1.6 han de ser iguals, podem justificar estendre la notació reduïda de Sweedler a

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

Observem que podem reescriure l'imatge per l'aplicació counitat d'un element $c \in C$ com

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

Donem ara la definició de coacció d'una K-coàlgebra finita C. Notarem la seva àlgebra dual com $A = C^*$.
Suposem $\Omega : G \times A \to G$ una acció de G un grup sobre A. Aleshores usant la propietat universal (veure [8]), tenim que aquesta acció indueix una coacció $\Omega^* : G \to G \otimes C$ sobre C.

Podem estendre l'ús de la notació de Sweedler per a una coacció qualsevol d'una K-coàlgebra C. Sigui V un K-espai vectorial, considerem $\rho : V \to V \otimes C$ una coacció d'una K-coàlgebra C definida per $\rho(v) = \sum v_{(0)} \otimes v_{(1)}$. Podem rescriure la igualtat 1.3 per a ρ i $v \in V$, obtenint l'axioma de la coacció:

$$(Id_V \otimes \Delta_C) \circ \rho = (\rho \otimes Id_C) \circ \rho.$$

Aleshores podem posar

$$\sum_{(v)} v_{(1)} \otimes v_{(2)} \otimes v_{(3)} := \sum_{(v_{(1)})(v)} v_{(1)_{(1)}} \otimes v_{(1)_{(2)}} \otimes v_{(3)}$$

$$= \sum_{(v)(v_{(2)})} v_{(1)_{(1)}} v_{(1)} \otimes v_{(2)_{(1)}} \otimes v_{(2)_{(2)}}.$$

1.4 Biàlgebres

Definició 1.17. Una K-**biàlgebra** és un K-espai vectorial B juntament amb aplicacions $m_B, \lambda_B, \Delta_B, \epsilon_B$ que satisfan les següents condicions:

(i) (B, m_B, λ_B) és una K-àlgebra i $(B, \Delta_B, \epsilon_B)$ és una K-coàlgebra.

(ii) Les aplicacions Δ_B i ϵ_B són morfismes de K-àlgebres.

Observació 1.18. La condició que $\Delta_B : B \to B \otimes B$ sigui un morfisme d'àlgebres implica:

$$\begin{aligned}
\Delta_B(ab) &= \sum_{(a,b)} (ab)_{(1)} \otimes (ab)_{(2)}, \\
&= \Delta_B(a)\Delta_B(b), \\
&= \left(\sum_{(a)} a_{(1)} \otimes a_{(2)} \right) \left(\sum_{(b)} b_{(1)} \otimes b_{(2)} \right), \\
&= \sum_{(a,b)} a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)},
\end{aligned}$$

per tot $a, b \in B$.

Definició 1.19. Sigui B una K-biàlgebra. Un **element primitiu** de B és un element $b \in B$ pel qual se satisfà $\Delta_B(b) = 1 \otimes b + b \otimes 1$.

Exemple 1.20. Siguin K un cos i G un grup. Recordem la K-àlgebra de grup $K[G]$ com a una K-àlgebra $(K[G], m_{K[G]}, \lambda_{K[G]})$ definida a l'exemple 1.9.
Sigui $\Delta_{K[G]} : K[G] \to K[G] \otimes K[G]$ l'aplicació coproducte definida com a

$$\Delta_{K[G]}\left(\sum_{g\in S} r_g g\right) = \sum_{g\in G} r_g (g \otimes g),$$

i sigui $\epsilon_{K[G]} : K[G] \to K$ l'aplicació counitat està definida per

$$\epsilon_{K[G]}\left(\sum_{g\in G} r_g g\right) = \sum_{g\in G} r_g.$$

Aleshores $(K[G], \Delta_{K[G]}, \epsilon_{K[G]})$ és una K-coàlgebra. Per tant com les aplicacions $\Delta_{K[G]}$ i $\lambda_{K[G]}$ són morfismes de K-àlgebres.

$$(K[G], m_{K[G]}, \lambda_{K[G]}, \Delta_{K[G]}, \epsilon_{K[G]})$$

és K-biàlgebra, anomenada **biàlgebra de grup**.

Siguin B una biàlgebra i A una àlgebra que és també un B-mòdul per l'esquerra amb acció denotada per "$\cdot$". Diem que A és una B-**mòdul àlgebra per l'esquerra** si

$$b \cdot (aa') = \sum_{(b)} (b_{(1)} \cdot a)(b_{(2)} \cdot a'), \tag{1.7}$$

i

$$b \cdot 1_A = \epsilon(b) 1_A, \tag{1.8}$$

per a qualsevol $a, a' \in A$, $b \in B$.

1.5 Àlgebres de Hopf

Definició 1.21. Una K-**àlgebra de Hopf** és una biàlgebra sobre un cos K

$$H = (H, m_H, \lambda_H, \Delta_H, \epsilon_H)$$

juntament amb una aplicació K-lineal $\sigma_H : H \to H$ que satisfà

$$m_H(I_H \otimes \sigma_H)\Delta_H(h) = \epsilon_H(h)1_H = m_H(\sigma_H \otimes I_H)\Delta_H(h), \tag{1.9}$$

per tot $h \in H$. Anomenem **coinversa** (o aplicació antipodal) a σ_H, i a la igualtat 1.9 l'anomenem **propietat coinversa** (o antipodal).

Proposició 1.22. Una K-àlgebra de Hopf H és **commutativa** si H és una àlgebra commutativa, i H serà cocommutativa si és una coàlgebra cocommutativa.

Exemple 1.23. El cos K en ell mateix és una K-Àlgebra de Hopf, si prenem $\sigma_H = I_H$; l'anomenem **àlgebra de Hopf trivial**.

Exemple 1.24. Sigui G un grup finit i $K[G]$ la biàlgebra de l'exemple 1.20. L'aplicació coinversa $\sigma_{K[G]} : K[G] \to K[G]$ ve donada per

$$\sigma_{K[G]}(\tau) = \tau^{-1},$$

per tot $\tau \in G$. Aleshores $K[G]$ és una K-àgebra de Hopf. Aquesta K-àlgebra és cocommutativa, i és commutativa si i només si G és abelià.

2 Extensions de Hopf Galois

En aquest capítol donarem la definició d'extensió Hopf Galois, que va ser introduïda per Chase i Sweedler [2]. Per fer això veurem que L és una extensió de Galois de K amb grup G si i només si L és una $K[G]$-extensió de Galois de K. Finalment veurem com generalitzar una $K[G]$-extensió de Galois a extensions Hopf Galois.

Notem que donada una extensió finita L de K, si $Aut_K(L)$ és el grup dels automorfismes de L que fixen K, i G és un subgrup de $Aut_K(L)$. Aleshores tenim que L és $K[G]$-mòdul on l'acció de $K[G]$ sobre L ve donada per

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

on $\lambda_g \in K, g \in G, x \in L$.

Proposició 2.1. Sigui L una extensió finita de K. Sigui G un subgrup de $Aut_K(L)$. Llavors L és una $K[G]$-mòdul àlgebra.

Demostració. Recordem els següents punts.

- $K[G]$ és l'àlgebra de grup definida a l'exemple 1.9, i també és una biàlgebra.
- L és una K-àlgebra finita.
- Un element $h \in K[G]$ és de la forma

  $$h = \sum_{g\in G}\lambda_g g,\ \ \lambda_g \in K[G], g \in G.$$

  Per tant donat $g \in G$ podem identificar g amb l'element de $K[G]$ $1g$, llavors naturalment $g \in K[G]$.

Notarem amb "$\cdot$"l'acció de $K[G]$ sobre L definida anteriorment. Llavors, sigui $g \in G$ qualsevol, se satisfà

$$g\cdot(xy) =_{(i)} g(xy) =_{(ii)} g(x)g(y) =_{(i)} (g\cdot x)(g\cdot y),$$

i

$$g\cdot 1_L =_{(i)} g(1_L) =_{(ii)} 1_L = \epsilon_{K[G]}(g)1_L,$$

per qualsevol $x, y \in L$. Vegem ara que L és una $K[G]$-mòdul àlgebra. Sigui $h \in K[G]$ definit com anteriorment i siguin $x, y \in L$ qualsevol. Usant les igualtats anteriors veiem que se satisfà:

$$\begin{aligned} h\cdot(xy) &=_{(i)} \sum_{g\in G}\lambda_g g(xy),\\ &=_{(ii)} \sum_{g\in G}\lambda_g (g\cdot x)(g\cdot y),\\ &=_{(iii)} \sum_{(h)}(h_{(1)}\cdot x)(h_{(2)}\cdot y), \end{aligned}$$

i

$$h \cdot 1_L = \sum_{g \in G} \lambda_g g(1_L) = \sum_{g \in G} \lambda_g 1_L = \epsilon_{K[G]}(h) 1_L.$$

Per tant tenim que L és una $K[G]$-modul àlgebra. Observem que per obtenir les igualtats anteriors hem fet servir:

(i) La definició d'acció de G sobre L.

(ii) Com $g \in G \leq Aut_K(L)$, g és un automorfisme de L.

(iii) Usem la definició del coproducte amb la notació de Sweedler, i la definició de l'acció de $K[G]$ sobre L com a G-mòduls definida a 1.7.

$$\Delta_K(\sum_{g \in G} \lambda_g g) = \sum_{g \in G} \lambda_g (g \otimes g).$$
$$\Delta_K(h) \cdot (x) = \sum_{g \in G} \lambda_g (g(x) \otimes g(x)) = \sum_{(h)} (h \cdot x)_{(1)} (h \cdot x)_{(2)}.$$

□

Introduïm ara els conceptes necessaris per poder donar la definició de extensió Hopf Galois. Sigui L un cos extensió finita de K llavors tenim que L és un K-espai vectorial, de manera que podem considerar

$$End_K(L) = Hom_K(L, L)$$

el conjunt de les aplicacions K-lineals $\Phi : L \to L$. Notem que sobre K el conjunt $End_K(L)$ és un espai vectorial amb la suma i producte escalar definits com

$$(\Phi + \psi)(x) = \Phi(x) + \psi(x) \text{ i } (r\Phi)(x) = r\Phi(x),$$

per a $r \in K$, $x \in L$. Com G és un conjunt de K-automorfismes de L que fixen K, G és un subconjunt de $End_K(L)$. Aleshores tenim un homomorfisme d'espais vectorials

$$j : L \otimes_K K[G] \to End_K(L) \tag{2.1}$$

definit per $j(x \otimes h)(y) = x(h \cdot y)$, per $x, y \in L$, $h \in K[G]$.

Lema 2.2. *Sigui L un cos extensió finita de K i G un subgrup de $Aut_K(L)$. Els elements de G formen un conjunt linealment independent de vectors sobre l'extensió L.*

Demostració. Posem els elements de G com a $g_0, g_1, \cdots, g_{n-1}$. Suposem que el conjunt de vectors $\{g_0, g_1, \cdots, g_{n-1}\}$ no és linealment independent sobre L, aleshores existeixen $m \in \mathbb{N}$ mínim amb $1 \leq m \leq n$, i un conjunt d'enters diferents dos a dos $i_1, i_2 \cdots i_m$ amb $0 \leq i_1, \cdots i_m \leq n-1$ de manera que

$$a_1 g_{i_1} + a_2 g_{i_2} + \cdots + a_{m-1} g_{i_{m-1}} + a_m g_{i_m} = 0, \tag{2.2}$$

amb $a_1, a_2, \cdots, a_m$ coeficients no nuls. Llavors com $g_{i_m} \neq g_{i_{m-1}}$, tenim que existeix $l \in L$ de manera que $g_{i_m}(l) \neq g_{i_{m-1}}(l)$ amb $g_{i_m}(l) \neq 0$. Aleshores per a qualsevol $x \in L$,

$$a_1 g_{i_1}(xl) + a_2 g_{i_2}(xl) + \cdots + a_{m-1} g_{i_{m-1}}(xl) + a_m g_{i_m}(xl) = 0.$$

Usant linealitat dels termes g_j, $0 \leq j \leq n-1$ tenim

$$a_1 g_{i_1}(l)g_{i_1}(x) + a_2 g_{i_2}(l)g_{i_2}(x) + \cdots + a_{m-1} g_{i_{m-1}}(l)g_{i_{m-1}}(x) + a_m g_{i_m}(l)g_{i_m}(x) = 0,$$

llavors com x és un element qualsevol de L

$$a_1 g_{i_1}(l)g_{i_1} + a_2 g_{i_2}(l)g_{i_2} + \cdots + a_{m-1} g_{i_{m-1}}(l)g_{i_{m-1}} + a_m g_{i_m}(l)g_{i_m} = 0. \tag{2.3}$$

Ara dividint pel terme $g_{i_m}(l) \neq 0$ per hipòtesi obtenim

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

Considerem la diferència entre l'anterior igualtat i 2.2 obtenint

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

Observem que el terme $a_{m-1}\Big(\frac{g_{i_{m-1}}(l)}{g_{i_m}(l)}\Big) - a_{m-1}$ és no nul, ja que $g_{i_m}(l) \neq g_{i_{m-1}}(l)$ per hipòtesi. El que ens porta a una contradicció, ja que havíem suposat m el mínim enter tal que 2.2 és cert. Per tant podem afirmar que els elements de G són un conjunt linealment independent sobre L. □

Donem ara una caracterització de les extensions Galois que portarà a la definició d'extensió Hopf-Galois.

Proposició 2.3. Sigui K un cos, sigui L una extensió finita i separable de K i sigui G un subgrup de $Aut_K(L)$. Llavors l'aplicació

$$j : L \otimes_K K[G] \to End_K(L)$$

és bijectiva si i només si L és una extensió de Galois de K amb grup G.

Demostració. Suposem primer L és una extensió de Galois de K amb grup G, volem veure que j definida a l'enunciat és bijectiva. Siguin $h = \sum_{i=0}^{n-1} \lambda_i g_i \in K[G], x \in L$, satisfent que

$$j\left(x \otimes \sum_{i=0}^{n-1} \lambda_i g_i\right)(y) = \left(x \otimes \sum_{i=0}^{n-1} \lambda_i g_i\right) \cdot y = \sum_{i=0}^{n-1} x\lambda_i g_i(y) = 0,$$

per tot $y \in L$. Pel Lemma 2.2 sabem que el conjunt de vectors $\{g_0, g_1, \cdots, g_{n-1}\}$ és linealment independent sobre L. Per tant $x\lambda_i = 0$ per tot i, d'on obtenim que $Ker(j) = \{0\}$, és a dir j és injectiva.
Veiem l'exhaustivitat de j mitjançant la igualtat de dimensions següent

$$\dim(L \otimes_K K[G]) = [L : K] \cdot |G| = [L : K]^2 = \dim(\mathrm{End}_K(L)).$$

Observem que per obtenir la igualtat anterior fem servir que la dimensió de L com a K-espai vectorial és $[L : K]$, que L/K és Galois amb grup G i per tant $|G| = [L : K]$, i que donat un K-espai vectorial V la dimensió de $\mathrm{End}_K(V)$ és $\dim(V)^2$.

Veiem ara la implicació contrària, suposem que l'aplicació j és bijectiva. Sabem doncs que les dimensions de $L \otimes_K K[G]$ i $End_K(L)$ han de ser necessàriament la mateixa, és

a dir $[L:K]\cdot|G| = [L:K]^2$, per tant necessàriament $|G| = [L:K]$. Llavors posem $L = K(\alpha)$ i considerem el polinomi $p(x) = Irr(\alpha, K)$ de grau $[L:K]$. Aleshores com els automorfismes de G envien α a les distintes arrels β de $p(x)$, és a dir L és el cos de descomposició de $p(x)$, d'on obtenim que l'extensió L/K és Galois. Denotem $Gal(L/K)$ el grup de Galois de L sobre K. Tenim que G és un subgrup de $Gal(L/K)$. Aleshores com tenim la igualtat d'ordres $|Gal(L/K)| = [L:K] = |G|$, obtenim que $G = Gal(L/K)$ i per tant L és Galois sobre K amb grup G. □

Hem vist que la noció de que L sigui una extensió de Galois de K amb grup G és equivalent a que L sigui una $K[G]$ mòdul àlgebra per la qual tenim definida l'aplicació

$$j : L \otimes_K K[G] \to End_K(L)$$

donada per $j(x \otimes h)(y) = x(h \cdot y)$, $x, y \in L$, $h \in K[G]$, i és bijectiva.

Usant la proposició anterior podem generalitzar el concepte d'extensió de Galois a extensió Hopf Galois.

Definició 2.4. Siguin H una K-àlgebra finita de Hopf cocommutativa, L/K una extensió finita de cossos. Llavors diem que L és una **extensió Hopf Galois de K amb àlgebra de Hopf** H, quan L és una H-mòdul àlgebra amb acció que notem per $h \cdot l$, per a $h \in H, l \in L$, i l'aplicació

$$j : L \otimes_K H \to End_K(L),$$

definida per $j(x \otimes h)(y) = x(h \cdot y)$, $x, y \in L$, $h \in H$ és un isomorfisme de K-espais vectorials. També podem dir que L/K **és H-Galois**.

Exemple 2.5. Donem ara un cas particular d'extensió Hopf Galois que no és Galois. Un exemple clàssic d'extensió no normal és $\mathbb{Q}(\sqrt[3]{2})$, ja que no existeixen automorfismes de $\mathbb{Q}(\sqrt[3]{2})$, diferents de la identitat, de manera que tots els elements de $\mathbb{Q}$ siguin fixos. Posem $w = \sqrt[3]{2}$, aleshores com $\{1, \omega, \omega^2\}$ és $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt[3]{2})$, podem definir dos aplicacions $\mathbb{Q}$-lineals de $\mathbb{Q}(\sqrt[3]{2})$ en ell mateix, determinant només les imatges dels elements de la base. Definim aquestes aplicacions, que anomenarem c i s, de la següent manera.

$$\begin{aligned} c(1) &= 1, & c(w) &= -\frac{1}{2}w, & c(w^2) &= -\frac{1}{2}w^2, \\ s(1) &= 0, & s(w) &= \frac{1}{2}w, & s(w^2) &= \frac{1}{2}w^2, \end{aligned}$$

per tant un element $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ estarà a $\mathbb{Q}$ si i només si $c(\alpha) = \alpha$, $s(\alpha) = 0$. D'aquesta manera podem pensar $\mathbb{Q}$ com el cos format pels elements fixos per c i s. Observem que les aplicacions que hem definit no són automorfismes ja que no satisfan $f(\alpha\beta) = f(\alpha)f(\beta)$, $\alpha, \beta \in \mathbb{Q}(\sqrt[3]{2})$. Tot i així aquestes aplicacions satisfan unes condicions properes a les necessàries per ser un d'automorfisme d'anells. Les condicions que compleixen són, per a tot $\alpha, \beta \in \mathbb{Q}(\sqrt[3]{2})$:

$$\begin{aligned} c(\alpha\beta) &= c(\alpha)\cdot c(\beta) - 3\cdot s(\alpha)\cdot s(\beta); \\ s(\alpha\beta) &= c(\alpha)\cdot s(\beta) + s(\alpha)\cdot c(\beta). \end{aligned} \tag{2.4}$$

Ara escollim una H concreta de manera que aquesta tingui estructura de $\mathbb{Q}$-àlgebra de Hopf. Posem H com l'anell quocient:

$$\mathbb{Q}[c, s]/(3s^2 + c^2 - 1), (2c + 1)s, (2c + 1)(c - 1)).$$

Determinem ara la imatge de aplicacions coproducte, counitat i coinversa en funció de c i s definides anteriorment.

$$\begin{aligned} \Delta(c) &= c \otimes c - 3s \otimes s, & \Delta(s) &= c \otimes s + s \otimes c, \\ \epsilon(c) &= 1, & \epsilon(s) &= 0, \\ \sigma(c) &= c, & \sigma(s) &= -s. \end{aligned}$$

Les igualtats 2.4 dónen que $Q(\sqrt[3]{2})$ té estructura de H-mòdul àlgebra, amb les aplicacions estructurals definides anteriorment. Aquest exemple s'ha extret de l'article d'en Greither-Pareigis [6].

A continuació donem una versió general del Teorema fonamental de la teoria de Galois; on les condicions que demanarem no inclouran subextensions i tampoc subgrups regulars.

Teorema 2.6. *Suposem L és un cos extensió de K amb àlgebra de Hopf associada H. Aleshores si definim per a una K-subàlgebra de Hopf W de H*

$$Fix(W) = \{x \in L | \mu(w)(x) = \epsilon(w)\dot{x}, \textit{per a totw} \in W\},$$

on $\mu : H \otimes L \to L$ és l'acció de H sobre L. Aleshores l'aplicacació Fix:

$$\{W \subset H \textit{és una subàlgebra de Hopf}\} \to \{E | K \subset E \subset K, \textit{amb } E \textit{ un cos}\}$$

és injectiva i inverteix les inclusions.

Aquest resultat correspon al Teorema 7.6 de [2]. Per conèixer les implicacions que obtenim a partir d'aquest Teorema, veure el capítol 5 de [6].

Per acabar el capítol un resultat que farem servir més endavant. Aquest resultat ens dóna una caracterització de l'extensió Hopf-Galois en termes de l'àlgebra de Hopf dual.

Proposició 2.7. Sigui H una K-àlgebra de Hopf finita. Sigui S una K-àlgebra commutativa i alhora un H-mòdul àlgebra per l'esquerra. Aleshores

$$\begin{array}{ccc} S \otimes H & \xrightarrow{j} & End_K(S) \\ (s \otimes h) \to t & \longmapsto & sh(t) \end{array}$$

és un isomorfisme si i només si

$$\begin{gathered} \gamma : S \longrightarrow S \otimes H^* \\ \gamma(s \otimes t) = (s \otimes 1)\alpha(t) \end{gathered}$$

és un isomorfisme.

Demostració. Considerem el següent diagrama.

$$\begin{array}{ccc} S \otimes H & \xrightarrow{\quad j \quad} & Hom_K(S,S) \\ \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \beta} \\ Hom_S(S \otimes H^*, S) & \xrightarrow{\quad \gamma^* \quad} & Hom_S(S \otimes S, S) \end{array}$$

On les aplicacions anterios són les definides per $\eta(s \otimes h)(t \otimes f) = st < h, f >$ i $\beta(f)(s \otimes t) = sf(t)$. Notem que $<,>: H \otimes H^* \to K$ és l'aplicació natural que evalua un element de H per un de H^*, i η, β són isomorfismes.

Aleshores un cop veiem que el diagrama és commutatiu, veure amb més detall [4], obtenim com a conseqüència que com que γ és un isomorfisme j també ho és. Per tant j serà un isomorfisme si i només si γ també ho és. □

3 Teoria de Greither-Pareigis

L'objectiu d'aquest capítol és donar una descripció una mica més acurada de les àlgebres de Hopf associades a les extensions Hopf Galois. Per fer això veurem un resultat que ens relacionarà l'àlgebra de Hopf amb un subgrup regular de permutacions, que posteriorment definirem i calcularem.

Proposició 3.1. Siguin L una extensió finita separable de K i E la seva clausura normal de manera que $Gal(E/K) = G$. Sigui $Gal(E/L) = G'$. Aleshores l'aplicació

$$\overline{\gamma}' : E \otimes_K L \to Map(G/G', E) \tag{3.1}$$

definida per

$$\overline{\gamma}'(n \otimes l)(\overline{\sigma}) = n\sigma(l)$$

és un isomorfisme de E-àlgebres i G-mòduls, on l'acció de G sobre $Map(G/G', E)$ ve donada per

$$\tau(f)(\overline{\sigma}) = \tau(f(\overline{\tau^{-1}\sigma})),$$

per a $\tau \in G$, $\overline{\sigma} \in G/G'$ el conjunt quocient de G per G' per l'esquerra, $\sigma \in G$ i $f \in Map(G/G', E)$.

Demostració. Per tal de veure que l'aplicació $\overline{\gamma}'$ és un isomorfisme de E-àlgebres i G-mòduls hem de veure que $Map(G/G', E)$ té l'estructura demanada i que $\overline{\gamma}'$ és un isomorfisme.

Vegem primer que $Map(G/G', E)$ té estructura de G-mòdul i de E-àlgebra. Siguin $f, g \in Map(G/G', E)$. Recordem que com E és una K-àlgebra també té estructura de K-espai vectorial. Observem que podem definir l'acció de E sobre $Map(G/G', E)$. Com E té estructura de cos, podem usar el seu producte intern per definir l'acció

$$(\lambda f)(\overline{\sigma}) = \lambda f(\overline{\sigma}),\ \lambda \in E, f \in Map(G/G', E). \tag{3.2}$$

Aquesta acció està ben definida ja que com $f \in Map(G/G', E)$ aleshores $f(\overline{\sigma}) \in E\ \forall \overline{\sigma} \in G/G'$, i per tant $\lambda f(\overline{\sigma}) \in E$. Definim ara la suma i el producte intersn de $Map(G/G', E)$ usant la suma i el producte de E.

$$(f + g)(\overline{\sigma}) = f(\overline{\sigma}) + g(\overline{\sigma}), f, g \in Map(G/G', E), \overline{\sigma} \in G/G'. \tag{3.3}$$

$$(fg)(\overline{\sigma}) = f(\overline{\sigma})g(\overline{\sigma}), f, g \in Map(G/G', E), \overline{\sigma} \in G/G'. \tag{3.4}$$

Notem que tant la suma com el producte tenen element neutre, i en el cas de la suma també oposats ben definits. Per a la suma són de la forma:

(i) El neutre per la suma serà una aplicació de $Map(G/G', E)$, $0 : G/G' \to E$ definida per $\overline{\sigma} \longmapsto 0_E$ per tot $\overline{\sigma} \in G/G'$.

(ii) L'oposat per la suma d'un element $f \in Map(G/G', E)$ serà $-(f)(\overline{\sigma}) = -f(\overline{\sigma})$, per a tot $f \in Map(G/G', E)$, $\overline{\sigma} \in G/G'$.

I pel producte tenim:

(i) El neutre pel producte serà una aplicació de $Map(G/G', E)$, $1 : G/G' \to E$ definida per $\overline{\sigma} \longmapsto 1_E$, $\forall \overline{\sigma} \in G/G'$.

Vegem que com E té estructura de cos, les operacions que hem definit satisfan les propietats associativa, distributiva i commutativa.

(i) Propietat associativa de la suma: Considerem $f, g, h \in Map(G/G', E)$ i $\overline{\sigma} \in G/G'$, aleshores

$$(f)(\overline{\sigma}) + (g + h)(\overline{\sigma}) = f(\overline{\sigma}) + g(\overline{\sigma}) + h(\overline{\sigma}) = (f + g)(\overline{\sigma}) + (h)(\overline{\sigma}).$$

(ii) Propietat associativa del producte. Considerem $f, g, h \in Map(G/G', E)$ i $\overline{\sigma} \in G/G'$, aleshores

$$(f)(\overline{\sigma})(gh)(\overline{\sigma}) = f(\overline{\sigma})g(\overline{\sigma})h(\overline{\sigma}) = (fg)(\overline{\sigma})(h)(\overline{\sigma}).$$

(iii) Propietat distributiva: Considerem $f, g, h \in Map(G/G', E)$ i $\overline{\sigma} \in G/G'$, aleshores

$$(f)(g + h)(\overline{\sigma}) = f(\overline{\sigma})(g(\overline{\sigma}) + h(\overline{\sigma})) = (fg)(\overline{\sigma}) + (fh)(\overline{\sigma}) = (fg + fh)(\overline{\sigma}).$$

Per tant com les tres operacions necessàries estan ben definides, obtenim que $Map(G/G', E)$ té estructura de E-àlgebra.

Considerarem l'aplicació $\gamma' : E \otimes L \to Map(G, E)$, que és una restricció de

$$\gamma : E \otimes E \to Map(G, E),$$

definida per $\gamma(n \otimes m)(\sigma) = n\sigma(m)$. Si veiem que γ és morfisme de E-àlgebres i de G-mòduls, obtindrem directament que γ' ho serà, ja que tenim la següent composició d'aplicacions:

$$\begin{array}{ccccc} E \otimes L & \xrightarrow{i'} & E \otimes E & \xrightarrow{\gamma} & Map(G, E) \\ \Big| & & & & \uparrow \\ \Big| & & & & \uparrow \\ \Big| & & \xrightarrow{\gamma'} & & \uparrow \end{array}$$

Notem que l'aplicació γ està ben definida ja que $n \in E$ i $\sigma(m) \in E$, per $\sigma \in G$. Tenim el producte definit per $\lambda(n \otimes m) = \lambda n \otimes m$, i l'acció sobre $E \otimes E$ definida per $\sigma(n \otimes m) = \sigma(n) \otimes m$. Veiem doncs que γ és morfisme de E-àlgebres i de G-mòduls. Per tal de veure-ho definim l' acció de G com a l'enunciat. Siguin $\tau \in G$, $f \in Map(G, E)$, aleshores definim l'acció de G sobre $Map(G, E)$ com

$$\tau(f)(\sigma) = \tau(f(\tau^{-1}\sigma)),$$

per a qualsevol $\sigma \in G$. Vegem ara que γ és morfisme de G-mòduls i de E-àlgebres.

(i) $\gamma(\tau(n \otimes m))(\sigma) =^{?} \tau(\gamma(n \otimes m))(\sigma)$, per a tot $\sigma \in G$.
Per una banda tenim: $\gamma(\tau(n \otimes m))(\sigma) = \gamma(\tau(n) \otimes m)(\sigma) = \tau(n)\sigma(m)$. I per l'altre: $\tau(\gamma(n \otimes m))(\sigma) = \tau(\gamma(n \otimes m))(\tau^{-1}\sigma) = \tau(n(\tau^{-1}\sigma)(m)) = \tau(n)\sigma(m)$.

Observem que com hem definit les operacions suma i producte pels descomponibles de E, aleshores la suma (producte) d'imatges és la imatge de suma (producte).

(ii) $\gamma(\lambda n \otimes m)(\sigma) =^{?} \lambda(\gamma(n \otimes m)(\sigma), \sigma) \in G$.
Per una banda tenim: $\gamma(\lambda n \otimes m)(\sigma) = \lambda n\sigma(m)$, i per l'altre $\lambda(\gamma(n \otimes m)(\sigma) = \lambda(n\sigma(m)) = \lambda n\sigma(m)$.

Observem que podem definir una aplicació injectiva entre $Map(G/G', E)$ i $Map(G, E)$ de la següent manera:

$$\begin{aligned} i : Map(G/G', E) &\longrightarrow Map(G, E) \\ f \to \sigma &\longmapsto f(\overline{\sigma}),\ \sigma \in G. \end{aligned}$$

Comprovem la injectivitat de i.

Suposem $f, g \in Map(G/G', E)$ tals que $i(f) = i(g)$. Llavors, naturalment $f = g$.

Donem explícitament el conjunt d'aplicacions que formen la imatge de $Map(G, E)$ per l'aplicació i.

$$Imi = \{g \in Map(G, E) \text{ tals que } g(\sigma) = g(\sigma') \text{ sempre que } \overline{\sigma} = \overline{\sigma}';\ \sigma, \sigma' \in G\}.$$

Veiem que $\gamma'(n \otimes l) \in Imi$ per a qualsevol $n \in E$, $l \in L$. Notem que estem fent servir la γ' com a la composició de morfismes que hem vist abans. Suposem que $\overline{\sigma} = \overline{\sigma}'$, aleshores existeix $\tau \in G'$ tal que $\sigma' = \sigma\tau$. D'on $\gamma'(n \otimes l)(\sigma) = n\sigma(l)$ i $\gamma'(n \otimes l)(\sigma') = n\sigma'(l) = n(\sigma\tau)(l) = n\sigma(l)$. Ja que $\tau(l) = l$ per a qualsevol $\tau \in G'$, $l \in L$. Així obtenim l'exhaustivitat de $\overline{\gamma'}$.

Com tenim que γ és morfisme de E-àlgebres i de G-mòduls, només ens queda veure la seva bijectivitat. Veiem primer la injectivitat.

Suposem $\gamma(n \otimes m)(\sigma) = 0$ per a qualsevol $\sigma \in G$, aleshores necessàriament $n\sigma(m) = 0$, i com E és un cos o bé $n = 0$ o bé $\sigma(m) = 0$. En el primer cas tenim que si $n = 0$ aleshores $(n \otimes m) = 0$. En el segon tenim que si $\sigma(m) = 0$ aleshores $m = 0$, ja que $\sigma \in G$; i per tant $n \otimes m = 0$. En ambdós casos obtenim $Ker(\gamma) = \{0\}$.

Finalment, com γ' és la restricció de γ tenim pel que hem vist anteriorment que γ' és morfisme de E-àlgebres, de G-mòduls i injectiva. D'on obtenim que $\overline{\gamma}'$ també té aquestes propietats. □

A continuació donarem unes definicions que són necessàries per a poder continuar.

Definició 3.2. Sigui $Perm(X)$ el grup de permutacions del conjunt X. Un subgrup $N \subset Perm(X)$ és **regular** si se satisfà dues qualsevol de les condicions següents:

(i) N i X tenen el mateix cardinal.

(ii) N actua transitivament sobre X. Equivalenment, si per a tot $x, y \in X$ existeix $\eta \in N$ tal que $\eta x = y$.

(iii) L'estabilitzador $Sta_N(x) = \{\eta \in N : \eta x = x\}$ és trivial. És a dir l'únic element que conté $Sta_N(x)$ és la identitat de N per a tot $x \in X$.

Vegem que si se satisfan dos de les condicions anteriors se satisfà la tercera. Suposem que se satisfan (i), (ii) i que no se satisfà (iii). Aleshores com tenim $|N| = |X|$, posem expressar els conjunts com $\{x_1, \dots x_n\}$, $\{\eta_1, \dots \eta_n\}$. Ara, podem suposar que η_1 deixa fix x_1 i mou els altres elemenst de X entre ells de la forma $\eta(x_i) = x_{i+1}$, això últim ho

podem fer per (ii). Aleshores si suposem que la resta d'elements de N es comporten de la mateixa manera, arribem a una contradicció, ja que tindriem n més la identitat, per tant $n+1$ elements a N i n a X.

Podem simplificar les condicions anteriors per: $N \subset Perm(X)$ serà regular si i només si per algun $x \in X$, l'aplicació de N en X definida per $\eta \longmapsto \eta(x)$ és bijectiva.

Siguin X un conjunt finit, E un cos i per a $x \in X$ definim l'aplicació $u_x : X \to E$ definida per $u_x(y) = \delta_{x,y}$ per tot $y \in X$. Aleshores el conjunt $\{u_x : x \in X\}$ és una E-base de $Map(X, E)$. Ara donem el primer teorema per caracteritzar estructures Hopf Galois sobre una *split* àlgebra $Map(X, E)$.

Teorema 3.3. *Siguin X un conjunt finit, E un cos i $Map(X, E)$ el conjunt de les aplicacions de X en E. Si H és una E-àlgebra de Hopf de manera que $Map(X, E)$ és una extensió Hopf Galois de E amb àlgebra de Hopf H, aleshores H serà la biàlgebra $E[N]$, per algun grup N amb mateix cardinal que X. N es pot identificar amb un subgrup de $Perm(X)$ on l'acció de N sobre X està definida per $u_{\eta(x)} = \eta(u_x)$ per tot $x \in X, \eta \in N$ de manera que N serà un subgrup regular de $Perm(X)$. Recíprocament, si N és un subgrup regular de $Perm(X)$, aleshores $Map(X, E)$ serà $E[N]$- Galois.*

Demostració. Recordem que podem definir el següent isomorfisme

$$Map(X, E) \cong E \times \cdots \times E \ (n \text{ còpies}),$$

on $n = |X| = [L : K]$. Ho veiem de la forma següent. Sigui $f \in Map(X, E)$, com X és un conjunt finit podem suposar que és de la forma $X = \{\overline{\sigma_1}, \ldots, \overline{\sigma_n}\}$. Ara podem considerar les imatges dels elements de X per f, és a dir:

$$\begin{array}{ccc} \sigma_1 & \longmapsto & f(\sigma_1) \\ \vdots & & \vdots \\ \sigma_n & \longmapsto & f(\sigma_n) \end{array}$$

Recordem que tots els elements $f(\sigma) \in E$, per a $\sigma \in G$. Per tant podem pensar aquestes imatges com a les components d'un vector de la forma $\Big(f(\sigma_1), \ldots, f(\sigma_n)\Big)$. Naturalment aquest vector pertany al K-espai vectorial $E \times \cdots^{n)} \times E$.

Veiem ara la primera implicació del teorema.Suposem $Map(X, E)$ és una extensió Hopf Galois de E amb àlgebra de Hopf H. Aleshores se satisfan els següents isomorfismes:

$$\begin{array}{rcc} E \times \cdots \times E \ (n^2 \text{ còpies}) & \cong_{(i)} & Map(X \times X, E), \\ & \cong_{(ii)} & Map(X, E) \otimes_E Map(X, E), \\ & \cong_{(iii)} & Map(X, E) \otimes_E H^*, \\ & \cong_{(iv)} & H^* \times \cdots \times H^* \ (n \text{ còpies}), \end{array}$$

on hem aplicat el següent per a cada isomorfisme.

(i) Apliquem l'isomorfisme que hem vist a l'inici de la demostració, però per al producte $X \times X$.

(ii) Fem restriccions a la primera/segona component de $X \times X$ i expressem el conjunt com el producte d'aquestes restriccions.

(iii) Apliquem la proposició 2.7.

(iv) Usem que per la teoria d'anells semisimples se satifà

$$H^* \cong E \times \cdots \times E \ (n \text{ còpies})$$

com a E-àlgebres.

Definim aplicacions $\eta_i : H^* \to E$, definides per $\eta_i(h^*) = \eta_i((e_1, \ldots, e_n)) = e_i$, on $h^* \in H^*$ i $(e_1, \ldots, e_n) \in E \times \cdots \times E$. Tenim doncs que η_i serà la funció que retorna la coordenada i. Observem que aquestes aplicacions estan ben definides ja que $e_i \in E$ per a qualsevol $1 \leq i \leq n$. Llavors tenim que el conjunt $N = \{\eta_i\}$ és una base de $H^{**} \cong H$, ja que per com estan definides son linealment independent i tenim exactament n. Observem que per a cada i, η_i és un homomorfisme de E-àlgebres i per tant pel corol·lari 1.16 aquest conjunt està format per elements grupals. Com els elements grupals d'una àlgebra de Hopf sobre un cos són linealment independents, aleshores els elements de N són exactament els elements grupals de H, d'on obtenim que N és un grup i H és l'àlgebra de grup $E[N]$.

Veiem ara que N actua com a grup de permutacions sobre X. Recordem que un conjunt d'elements $\{u_x\}$ idempotents i ortogonals satisfà:

$$\begin{cases} u_x u_x &= u_x, \\ u_x u_y &= 0. \end{cases}$$

Sigui $\{u_x | x \in X\}$ una base ortogonal i idempotent de $Map(X, E)$, on els elements estan definits per $u_x(y) = \delta_{x,y}$ per a qualsevol $x, y \in X$. Com $Map(X, E)$ és una $H = E[N]$-mòdul àlgebra, per a $\eta \in N$ se satisfà:

$$\eta(u_x) = \eta(u_x \cdot u_x) = \Delta(\eta)(u_x \otimes u_x) = \eta(u_x)\eta(u_x),$$

amb $x \in X$. També tenim $0 = \eta(u_x \cdot u_y) = \eta(u_x)\eta(u_y)$ per a $u_x \neq u_y$. Per tant els elements η apliquen els elements idempotents primitius de $Map(X, E)$ en elements idempotents dos a dos ortogonals de $Map(X, E)$. Volem veure ara que apliquen idempotents primitius en idempotents primitius.

Observem que la identitat de N és 1, la identitat de $E[N]$. Aleshores per tot $\eta \in N$ i $x \in X$, $1 \cdot u_x = \eta^{-1}\eta(u_x) = u_x$, per tant $\eta(u_x) \neq 0$. També tenim que $\eta(1) = \epsilon(\eta) = 1$, ja que η és un element grupal de H i podem expressar la identitat de $Map(X, E)$ com a $1 = \sum_{x \in X} u_x$. D'aquesta manera obtenim que / amb tot això veiem que

$$1 = \eta(1) = \eta\left(\sum_{x \in X} u_x\right) = \sum_{x \in X} \eta(u_x).$$

Recordem que $\eta(u_x)$ és la suma d'elements idempotents primitius de $Map(X, E)$. Com $1 = \sum_{x \in X} \eta(u_x)$ i $\eta(u_x)\eta(u_y) = 0$ per a $x \neq y$, podem pensar que cada element idempotent primitiu és una suma de $\eta(u_x)$ per a exactament un $x \in X$. Com $\sum_{x \in X} \eta(u_x)$ és la suma de $|X|$ elements no nuls i en total és la suma de $|X|$ elements idempotents primitius, és a dir cada $\eta(u_x)$ ha de ser igual a un element u_y idempotent, per a algun $y \in X$. Així obtenim que podem identificar N amb un subgrup de $Perm(X)$, on les aplicacions η són permutacions definides per $\eta(x) = y$ sempre que $\eta(u_x) = u_y$, per a $x, y \in X$.

Notem que per provar la primera implicació del teorema hem de veure que N és subgrup regular de $Perm(X)$. Observem que $|X| = |N|$ ja que $E[N] = H$ i $Map(X, E)$ és H-Galois sobre E.

Suposem ara que $Nu_x = \{u_y | y \in Y\}$ on Y és un subconjunt de X diferent del total. Aleshores podem prendre $z \in X \setminus Y$ i definir $e_{xz} \in End_E(E[N])$ com $e_{xz(u_x)} = u_z$, $e_{xz}(u_y) = 0$ per a $y \neq x$. Llavors si

$$j : Map(X, E) \otimes E[N] \to End_E(E[N])$$

és l'isomorfisme definit a 2.3, tenim que e_{xz} no pertany a la imatge de j, ja que

$$\left(\sum_{w \in X, \eta \in N} l_{w,\eta} u_w \eta \right)(u_x) \in \sum_{y \in Y} E u_y.$$

Llavors arribem a una contradicció, ja que havíem suposat que $Map(X, E)$ era una extensió $E[N]$-Galois de E, i per tant que j és isomorfisme. Llavors N actua de manera transitiva sobre X , i per tant és un subrup regular de $Perm(X)$.

Recíprocament, suposem que N és un subgrup regular de $Perm(X)$ i veiem que $Map(X, E)$ és una extensió $E[N]$-Galois de E. Definim e_{xz} com anteriorment per a $x, z \in X$, aleshores $\{e_{xz} | x, z \in X\}$ és una E-base de $End_E(Map(X, E))$. Aleshores com hem suposat que N és regular, existeix $\eta \in N$ amb $\eta(x) = z$, i així $\eta(u_x) = u_z$. Llavors podem considerar l'aplicació j definida per

$$j(u_z \otimes \eta) = e_{xz}.$$

Per tant l'aplicació $j : Map(X, E) \otimes E[N] \to End_E(Map(X, E))$ és exhaustiva, i de la igualtat $|X| = |N|$ obtenim la injectivitat de j. És a dir obtenim que $Map(X, E)$ és una extensió $E[N]$-Galois de E. □

La motivació d'aquest capítol és aplicar la caracterització d'estructura Hopf Galois a extensions $Map(X, E)/E$, per a obtenir informació sobre les estructures Hopf Galois que són extensions de cossos.

Fem una petita recopilació del que hem provat fins ara per tal de donar una idea del que veurem a continuació. Suposem L és un cos extensió finita de K amb clausura normal E. Siguin $G = Gal(E/K)$, $G' = Gal(E/L)$ i $X = G/G'$. Suposem ara que L/K té estructura Hopf Galois,

$$H \otimes_K L \to L$$

A continuació farem un canvi de base a E de l'isomorfisme j. Tenim l'isomorfisme

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

D'on podem considerem l'aplicació

$$(E \otimes_K H) \otimes_E (E \otimes_K L) \to (E \otimes_K L) \tag{3.5}$$

Aleshores, usant la Proposició 3.1 ens dóna com a resultat que $\gamma : E \otimes_K L \to Map(X, E)$ és un isomorfisme. Ara, sabem que pel Teorema 3.3 existeix un subgrup regular N de $Perm(X)$ de manera que $E \otimes H \cong E[N]$, i per tant l'aplicació 3.5 serà isomorfa a una acció

$$E[N] \otimes_E Map(X, E) \to Map(X, E). \tag{3.6}$$

L'acció de G sobre E indueix accions de G sobre $E[N]$i sobre $Map(X, E)$, i així tenim que l'isomorfisme 3.6 és equivariant. Per explicar aquesta acció, introduïm la translació per l'esquerra.

Lema 3.4. *Suposem que estem sota les hipòtesis anteriors. Sigui*

$$\lambda : G \to Perm(X),$$

definida per $\lambda(\tau)(\overline{\sigma}) = \overline{\tau\sigma}$. *Aleshores* λ *és injectiva.*

Demostració. Fem una observació inicial, λ és morfisme de grups, comprovem-ho. Per a qualsevol τ, τ_1, $\tau_2 \in G$, $\overline{\sigma} \in G$ tenim:

$$\lambda(\tau\tau')(\overline{\sigma}) = \overline{(\tau_1\tau_2)\sigma} = (\overline{\tau_1\sigma})(\overline{\tau_2\sigma}) = \lambda(\tau_1)(\sigma)\lambda(\tau_2)(\sigma).$$

Posem $M = Ker(\lambda)$, aleshores

$$M \subset G' = \{\sigma \in G | \lambda(\sigma) \text{fixa la classe de la identitat } G' \text{ de } X\}.$$

Llavors E^M és un cos extensió normal de K que conté L. Però com E és la clausura normal de l'extensió L/K no podem tenir un cos intermedi que sigui normal sobre K. Per tant usant el Teorema fonamental de la teoria de Galois podem afirmar que $E = E^M$, és a dir que $Ker(\lambda)$ és trivial. □

4 Teorema de Greither Pareigis

Un cop arribem a aquest capítol ja tenim les eines necessàries per a provar el teorema de Greither Pareigis. Veurem com podem trobar explícitament els elements que formen l'algebra de Hopf associada a una extensió L/K amb clausura normal E. Finalment tornarem enrere i donarem amb més detall l'exemple extret de l'article [6], juntament amb un altre exemple on calcularem i recuperarem l'àlgebra de Hopf. Per tal de fer això ens caldrà donar unes definicions i resultats extra.

Proposició 4.1. Sigui L/K una extensió Hopf Galois amb clausura normal E, sigui $G = Gal(E/K)$, sigui $G' = Gal(E/L)$ i sigui $X = G/G'$. Aleshores per canvi de base a l'acció de Galois de H sobre L obtenim l'acció

$$(E \otimes_K H) \otimes_E (E \otimes_K L) \longrightarrow (E \otimes_K L)$$

que és equivalent a una acció

$$E[N] \otimes_E Map(G/G', E) \to Map(G/G', E)$$

de $E \otimes H \cong E[N]$ en $Map(G/G', E)$ que correspon a una inclusió regular de N en $Perm(X)$ satisfent que si $\lambda : G \to Perm(X)$ és translació per l'esquerra, llavors $\lambda(G)$ normalitza la imatge de N en $Perm(X)$.

Demostració. Per començar la demostració veiem que l'acció de G en $E \otimes_K H$ induïda per l'acció de G sobre E ens dóna una acció de G sobre $E[N]$ definida per

$$\tau(ln) = \tau(l)(\lambda(\tau)\eta\lambda(\tau^{-1})),$$

per a $l \in E$, $\eta \in N$, $\tau \in G$. Això implica que l'acció de G sobre N s'obté via una conjugació en $Perm(X)$ de $\lambda(G)$.

Vegem que tenim aquesta acció ben definida. Recordem que tenim una base d'elements ortogonals i idempotents de $Map(G/G', E)$ com $\{u_x | x \in X\}$ i podem expressar aquesta base com

$$\{u_{\overline{\sigma}} | \overline{\sigma} \in X\},$$

per a $\overline{\tau}$, $\overline{\sigma} \in G/G'$ satisfent $u_{\overline{\sigma}}(\overline{\tau}) = \delta_{\overline{\sigma},\overline{\tau}}$. Aleshores, com G actua sobre $Map(E, G/G')$ i sobre E, obtenim que existeix una acció de G en $Hom_E(Map(E, G/G'), E)$ definida per:

$$\tau(f)(y) = \tau(f(\tau^{-1}(y))),$$

on $\tau \in G$, $f \in Hom_E(Map(E, G/G'), E)$, $y \in Map(E, G/G')$. Observem que estem fent servir l'acció de G sobre $Map(G/G', E)$ definida a la Proposició 3.1. Per tant

$$\tau(u_{\overline{\sigma}})(\overline{\rho}) = \tau(u_{\overline{\sigma}}(\overline{\tau^{-1}\rho})) = u_{\overline{\sigma}}(\overline{\tau^{-1}\rho}) = u_{\overline{\tau\sigma}}(\overline{\rho}) = u_{\lambda(\tau)\overline{\sigma}}(\overline{\rho}). \tag{4.1}$$

Així l'acció de $\tau \in G$ sobre els elements idempotents $\{u_{\overline{\sigma}} | \overline{\sigma} \in X\}$ es correspon amb la translació per l'esquerra de les classes laterals $\tau G'$, $\tau \in G$.

Per tant l'acció de N sobre $\{u_{\overline{\sigma}} | \overline{\sigma} \in X\}$ es correspon amb una injecció de N en $Perm(X)$ definida per $\eta(u_{\overline{\sigma}}) = u_{\eta(\overline{\sigma})}$.

Ara, l'acció

$$(E \otimes_K H) \otimes_E (E \otimes_K L) \to (E \otimes_K L)$$

és G-equivariant on G actua sobre E. Així, identificant $E \otimes H$ amb $E[N]$ i usant que $\overline{\gamma}' : E \otimes_K L \to Map(G/G', E)$ és un homomorfisme de G-mòduls tenim que l'acció

$$E[N] \otimes Mpa(G/G', E) \to Map(G/G', E)$$

és G-equivariant. Com G manté l'estructura de àlgebra de Hopf de $E[N]$, G actúa sobre N, el conjunt d'elements grupals de $E[N]$, i per tant per a $\eta \in N$, $\overline{\sigma} \in X$, $\tau \in G$ se satisfà

$$\tau(\eta)\tau(u_{\overline{\sigma}}) = \tau(\eta u_{\overline{\sigma}}) = \tau(u_{\eta\overline{\sigma}}).$$

Ara tenim

(i) Com $\tau(\eta) \in N$ ja que $\eta \in N$ i τ és l'acció de G, se satisfà $\tau(u_{\overline{\sigma}}) = u_{\overline{\tau\sigma}}$.

(ii) La definició de λ és: $\lambda(\tau)(\overline{\sigma}) = \overline{\tau\sigma}$.

Per una banda tenim que $\tau(\eta)\tau(u_{\overline{\sigma}}) = \tau(\eta)(u_{\lambda(\tau)(\overline{\sigma})}) = u_{\tau(\eta)(\lambda(\tau)(\overline{\sigma}))}$. Per la darrera igualtat fem servir la definició d'aplicar $\eta \in N$ a un element u_y.

Per l'altre banda tenim que

$$\tau(u_{\eta(\overline{\sigma})}) = u_{\lambda(\tau)\eta(\overline{\sigma})} = u_{\tau(\eta)(\lambda(\tau)(\overline{\sigma}))},$$

i com sabem que els elements $u_{\overline{\sigma}}$ estan indexats per X obtenim

$$\lambda(\tau)(\eta(\overline{\sigma})) = \tau(\eta)(\lambda(\tau)(\overline{\sigma})).$$

Anomenem $\overline{\rho} = \lambda(\tau)(\overline{\sigma})$ i com λ és bijectiva tenim que $\lambda(\tau^{-1})(\rho) = \overline{\sigma}$.

D'on obtenim que

$$\tau(\eta)(\overline{\rho}) = \lambda(\tau)\eta(\lambda(\tau^{-1})(\overline{\rho})), \text{ per a tot } \overline{\rho} \in G'.$$

La acció de τ de G sobre $\eta \in N$ és via conjugació per $\lambda(\tau)$ a $Perm(G)$.

□

Definició 4.2. Siguin E una extensió de Galois de K, $Gal(E/K) = G$. Sigui F un grup amb acció de G. Definim un 1**-cocicle** de G en F com una aplicació

$$\begin{aligned} p : \quad & G \to F \\ & \sigma \longmapsto p_\sigma \end{aligned}$$

tal que $p_{\sigma\tau} = p_\sigma \cdot \sigma(p_\tau)$ per a tot parell σ, $\tau \in G$.

El conjunt d'aquests cocicles serà $C^1(G, F) := \{1 - \text{cocicles de } G \text{ en } F\}$. Definim els **cocicles cohomòlegs**, per tal de fer això donem una relació d'equivalència entre cocicles:

$$p \sim q \iff \exists a \in F : q_\sigma = a^{-1} p_\sigma \sigma(a),$$

per a tot $\sigma \in G$. Comprovem que aquesta relació és d'equivalència:

(i) Propietat reflexiva: Sigui p_σ un 1-cocicle. Aleshores si prenem $1 \in F$ obtenim que

$$p_\sigma = 1 p_\sigma \sigma(1)$$

(ii) Propietat simètrica: Siguin p_σ, q_σ dos 1-cocicles. Suposem que $p_\sigma \sim q_\sigma$, és a dir existeix $a \in F$ amb $q_\sigma = a^{-1}p_\sigma\sigma(a)$. Observem que com σ és un morfisme, aleshores $\sigma(a)^{-1} = \sigma(a^{-1})$. Per tant $a^{-1} \in F$ i així tenim que $p_\sigma = aq_\sigma(\sigma(a^-1))$.

(iii) Propietat transitiva: Siguin $p_\sigma, q_\sigma, r_\sigma$ 1-cocicles satisfent $p_\sigma \sim q_\sigma$ i $q_\sigma \sim r_\sigma$. Aleshores sabem que per una banda existeixen $a, b \in F$ tal que $q_\sigma = a^{-1}p_\sigma\sigma(a)$ i $r_\sigma = b^{-1}q_\sigma\sigma(b)$. Aleshores tenim que:

$$r_\sigma = b^{-1}q_\sigma\sigma(b) = b^{-1}a^{-1}p_\sigma\sigma(a)\sigma(b) = c^{-1}p_\sigma\sigma(c),$$

on $c = ab$, $c \in F$.

Aleshores usant aquesta relació d'equivalència definim

$$H^1(G, F) = C^1(G, F)/\sim .$$

Donem ara una definició que ens serà necessària per continuar. En el nostre cas prendrem E/K una extensió Galois amb grup $G = Gal(E/K)$, i A un espai vectorial amb estructura adicional, com per exemple una K-àlgebra o una K-àlgebra de Hopf. Llavors direm que B, una K-àlgebra o una K-àlgebra de Hopf, és una E/K**-forma** de A si existeix un isomorfisme $E \otimes_K B \cong E \otimes_K A$. Tenim definida l'acció de G sobre el factor de l'esquerra de $E \otimes_K A$ mitjançant automorfismes de E, llavors per conjugació, també tindrem una acció de G en $Hom(E \otimes_K A, E \otimes_K B)$ on A, B són K-àlgebres o K-àlgebres de Hopf.

Teorema 4.3. *El conjunt de E-formes de A mòdul K-isomorfisme té una correspondència bijectiva amb el conjunt de cohomologia $H^1(G, Aut_E(E \otimes A))$. Aquest resultat es correspon a la proposició 4 del capítol X de [9].*

Definició 4.4. Siguin A_1, A_2 K-àlgebres de Hopf, sigui E/K una extensió de Galois de cossos. Llavors un morfisme de E-àlgebres de Hopf $f : E \otimes A_1 \to E \otimes A_2$ és **descendible** si existeixen (E/K)-formes B_1, B_2 de A_1, A_2 i un morfisme $g : B_1 \to B_2$ de manera que el següent diagrama és commutatiu.

$$\begin{array}{ccc} E \otimes A_1 & \xrightarrow{\quad f \quad} & E \otimes A_2 \\ \uparrow{\scriptstyle \Phi_1} & & \uparrow{\scriptstyle \Phi_2} \\ E \otimes B_1 & \xrightarrow[id \otimes g]{} & E \otimes B_2 \end{array}$$

Si existeix aquest morfisme g, aleshores és únic.

Proposició 4.5. Una aplicació $f : E \otimes A_1 \to E \otimes A_2$ és descendible si i només si

$$f \circ p_\sigma^{(1)} = p_\sigma^{(2)} \circ \sigma(f), \text{ per a tot } \sigma \in G.$$

On $p_\sigma^{(1)}$ és l'1-cocicle associat a B_1 com a forma de A_1 i $p_\sigma^{(2)}$ és l'1-cocicle associat a B_2 com a forma de A_2. Per tant $p_\sigma^{(1)} \in Aut(E \otimes A_1)$, $p_\sigma^{(2)} \in Aut(E \otimes A_2)$.

Teorema 4.6. *Sigui L/K una extensió separable de cossos amb clausura normal E. Siguin $G = Gal(E/K)$, $G' = Gal(E/L)$ i $X = G/G'$. Aleshores existeix una bijecció entre el conjunt de subgrups regulars N de $Perm(X)$ normalitzats per $\lambda(G)$ i el conjunt d'estructures Hopf-Galois de L/K.*

Si N és subgrup regular de $Perm(X)$ normalitzat per $\lambda(G)$ aleshores $Map(X,E)/E$ és una extensió Hopf Galois amb àlgebra de Hopf $E[N]$. Per tant tenim ben definida l'acció:

$$\begin{array}{ccc} E[N]\otimes Map(X,E) & \xrightarrow{\Phi} & Map(X,E) \\ \sum\limits_{n\in N}\mu_n n\otimes\tau & \longmapsto & \sum\limits_{n\in N}\tau(\mu_n)n. \end{array}$$

Ara, usant la proposició 3.1 tenim que

$$Map(X,E)\cong E\otimes L$$

és un isomorfisme de E-àlgebres i de G-mòduls. Vegem com definim aquest isomorfisme. Recodem que els elements $u_{\overline{\tau}}$ que formen base de X satisfan $u_{\overline{\tau}}(\sigma)=\delta_{\overline{\tau\sigma}}$, i observem que podem expressar un element $l\in L$ com $l=\sum\limits_{\tau\in X}\tau(l)u_{\overline{\tau}}(\overline{1})$. Aleshores l'homomorfisme anterior serà el donat per:

$$\begin{array}{ccc} E\otimes L & \longrightarrow & Map(X,E) \\ \mu\otimes l & \longmapsto & \mu\sum\limits_{\tau\in X}\tau(l)u_{\overline{\tau}}(\overline{1}). \end{array}$$

I, llavors l'acció anterior la podem escriure com

$$E[N]\otimes_E(E\otimes L)\xrightarrow{\psi}E\otimes L.$$

Observem que ψ és morfisme de E-mòduls. Llavors usant tot això veiem que $E\otimes L/E$ és Hopf Galois amb àlgebra $E[N]$.

Demostració. El propòsit d'aquesta demostració es veure que existeix una K-àlgebra de Hopf que notarem per H, de manera que se satisfan les següents condicions.

(i) L/K és Hopf galois amb àlgebra H.

(ii) $E\otimes H\cong E[N]$.

Començem considerant el següent isomorfisme de K-àlgebres.

$$E[N]\cong E\otimes K[N]$$

Notarem $E\otimes K[N]=A$. Justifiquem ara que podem definir l'isomorfisme. Sigui V un K-espai vectorial, aleshores $dim_E(E\otimes V)=dim_K(V)$. Per tant si fem el producte tensorial

$$\begin{array}{ccc} E\otimes K[N] & \to & E[N] \\ 1\otimes n & \to & n. \end{array}$$

Notem que el que estem fent quan definim aquesta aplicació és: Si considerem $v_1,\dots,v_n$ una K-base de V, aleshores $1\otimes v_1,\dots,1\otimes v_n$ serà una E-base de $E\otimes V$. I, tenim l'isomorfisme $E[N]\cong E\otimes K[N]$ ja que la base que considerem està indexada per N.

Sigui A una K-àlgebra de Hopf fixada, aleshores considerem el conjunt

$$\bigstar=\{H|\ H \text{ és una } K\text{-àlgebra de Hopf satisfent } E\otimes H\cong E\otimes A\}/(K-\text{isomorfisme}).$$

Aleshores, pel teorema 4.3 existeix la següent bijecció:

$$\bigstar\longleftrightarrow H^1(G,Aut(E\otimes A)),$$

on $H^1(G, Aut(E \otimes A))$ és el conjunt de cohomologia. Ens cal veure que tenim una acció de G en $Aut(E \otimes A)$. Per tal de veure això considerarem un automorfisme $\sigma \in G$ fixat, i començarem per definir una acció de G en $E \otimes A$.
Sigui $\lambda \otimes a$ un element qualsevol de $E \otimes A$, definim l'acció de G per $E \otimes A$ per $\sigma(\lambda \otimes a) = \sigma(\lambda) \otimes a$. Llavors l'acció definida sobre els automorfismes de $E \otimes A$ serà: Sigui $f \in Aut(E \otimes A)$ un automorfisme qualsevol, l'acció de G en $Aut(E \otimes A)$ és definida per $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$. Observem que estem pensant σ com l'automorfisme definit per

$$\begin{array}{rccc} \sigma : & E \otimes A & \rightarrow & E \otimes A \\ & \lambda \otimes a & \longmapsto & \sigma(\lambda) \otimes a. \end{array}$$

Vegem ara que tenim la bijecció que ens cal per veure (ii): Donada H tal que $E \otimes H \cong^g E \otimes A$, podem definir $\sigma(g) = \sigma \circ g \circ \sigma^{-1}$, ja que estem aplicant σ a un element de E. Tenim el següent diagrama commutatiu.

$$E \otimes H \xrightarrow{\sigma^{-1}} E \otimes H \xrightarrow{g} E \otimes A \xrightarrow{\sigma} E \otimes A, \qquad E \otimes H \xrightarrow{\sigma(g)} E \otimes A$$

Llavors, podem considerar l'1-cocicle definit com:

$$\begin{array}{ccc} G & \rightarrow & Aut(E \otimes A) \\ \sigma & \longmapsto & g^{-1} \circ \sigma(g). \end{array}$$

Observem que donat $p_\sigma : G \rightarrow Aut(E \otimes A)$ un 1-cocicle, podem associar-li l'àlgebra H donada per

$$H = \{x \in E \otimes A : p_\sigma(\sigma(x)) = x\};$$

notem que la condició que imposem per escollir l'àlgebra està ben definida, ja que $\sigma(x)$ és un element de $E \otimes A$ i p_σ és un automorfisme de $E \otimes A$. Es pot veure que H és una K-àlgebra de Hopf tal que $E \otimes H \cong E \otimes A$. Per teoria general de formes, si se satisfà que $E \otimes H \cong E \otimes A$ diem que H és una E/K-forma de A.

Fem una petita observació al marge de la demostració. Volem aconseguir que la ψ inicial sigui de la forma $H \otimes L \rightarrow L$. Per tal de fer això, veurem que existeix un 1-cocicle de manera que ψ és descendible.

Per tal de veure lo anterior, comencem prenent l'1-cocicle p_σ definit per

$$\begin{array}{rccl} p_\sigma : & N \rightarrow & N & \\ & n \longmapsto & \sigma n \sigma^{-1}, & \text{on } n \in N, \sigma \in G, \end{array} \tag{4.2}$$

i on identifiquem G amb $\lambda(G)$. Si ara passem a l'àlgebra de grup, podem redefinir p_σ com

$$\begin{array}{rccc} p_\sigma : & E[N] & \rightarrow & E[N] \\ & \sum_{n \in N} \mu_n n & \longmapsto & \sum_{n \in N} \lambda_n(\sigma n \sigma^{-1}), \end{array}$$

on $\lambda_n \in E$ per a tot $n \in N$. Per tant el nostre cocicle serà el determinat per

$$\begin{array}{rcc} p_\sigma : & G \rightarrow & Aut(E[N]) \\ & \sigma \longmapsto & p_\sigma. \end{array}$$

Recordem ara que hem definit ψ com l'aplicació donada per

$$E[N] \otimes_E (E \otimes L) \xrightarrow{\psi} E \otimes L.$$

Per construir el diagrama commutatiu, considerarem L com a forma de L. Aleshores el cocicle que li associarem serà el trivial. Definim H com la forma de $K[N]$ associada al cocicle p_σ,

$$H \text{ és una forma de } K[N] \leftrightarrow \text{Tenim el cocicle } p_\sigma \text{definit com anteriorment.}$$

Vegem que el següent diagrama és commutatiu.

$$\begin{array}{ccc} E[N] \otimes (E \otimes L) & \xrightarrow{\sigma(\psi)} & E \otimes L \\ \downarrow{\scriptstyle p_\sigma \otimes id} & & \| \\ E[N] \otimes (E \otimes L) & \xrightarrow{\psi} & E \otimes L \end{array}$$

Per fer la comprovació més senzilla, provarem que l'aplicació Φ definida a l'inici de la demostració és descendible, ja que si veiem que Φ és descendible obtenim que ψ també ho és. L'aplicació Φ està definida per:

$$\begin{array}{ccc} E[N] \otimes_E Map(X,E) & \xrightarrow{\Phi} & Map(X,E) \\ \rho \otimes \lambda u_{\overline{\tau}} & \longmapsto & \lambda u_{\rho\overline{\tau}}, \end{array}$$

per a $\rho \in N$, $\tau \in G$. Notem que estem pensant $Map(X,E)$ com a E-espai vectorial. I recordem que per hipòtesis N és un subgrup regular de $Perm(X)$ normalitzat per $\lambda(G)$. Per tant volem comprovar que el diagrama

$$\begin{array}{ccc} E[N] \otimes_E Map(X,E) & \xrightarrow{\sigma(\Phi)} & Map(X,E) \\ \downarrow{\scriptstyle p_\sigma \otimes id} & & \| \\ E[N] \otimes_E Map(X,E) & \xrightarrow{\Phi} & Map(X,E) \end{array}$$

és commutatiu.

Observem que el cocicle que escollim serà el definit a 4.2. Podem identificar G amb $\lambda(G)$ perquè $\lambda : G \to Perm(X)$, i per definició sabem que $\sigma(\Phi) = \sigma \circ \Phi \circ \sigma^{-1}$.

Per una banda tenim que, per a $\rho \otimes \mu u_{\overline{\tau}} \in E[N] \otimes Map(X,E)$ qualsevol, el valor de $\sigma(\Phi)(\rho \otimes \mu u_{\overline{\tau}})$ és:

$$\rho \otimes \mu u_{\overline{\tau}} \xrightarrow{\sigma^{-1}} \rho \otimes \sigma^{-1}(\mu) u_{\overline{\sigma^{-1}\tau}} \xrightarrow{\Phi} \sigma^{-1}(\mu) u_{\rho(\overline{\sigma^{-1}\tau})} \xrightarrow{\sigma} \mu u_{\overline{\sigma}\rho(\overline{\sigma^{-1}\tau})}$$

Vegem ara el valor de $\Phi \circ (p_\sigma \otimes id)$ aplicat a $\rho \otimes \mu u_{\overline{\tau}} \in E[N] \otimes Map(X,E)$.

$$\rho \otimes \mu u_{\overline{\tau}} \xrightarrow{p_\sigma \otimes id} \sigma\rho\sigma^{-1} \otimes \mu u_{\overline{\tau}} \xrightarrow{\Phi} \mu u_{(\sigma\rho\sigma^{-1})(\overline{\tau})}$$

Observem que hem simplificat la notació posant σ enlloc de $\lambda(\sigma)$. Ara comprovem que efectivament obtenim el mateix resultat per les dues bandes:

$$\overline{\sigma}\rho(\overline{\sigma^{-1}\tau}) = (\lambda(\sigma)\rho\lambda(\sigma^{-1}))(\overline{\tau}).$$

Recordem que $\lambda(\sigma)(\overline{\tau}) = \overline{\sigma\tau}$, per qualsevol $\sigma, \tau \in G$. Aleshores si fem el càlcul obtenim que $(\lambda(\sigma)\rho\lambda(\sigma^{-1}))(\overline{\tau})$ per definició és:

$$\overline{\tau} \xrightarrow{\lambda(\sigma^{-1})} \overline{\sigma^{-1}\tau} \xrightarrow{\rho} \rho(\overline{\sigma^{-1}\tau}) \xrightarrow{\lambda(\sigma)} \overline{\sigma}\rho(\overline{\sigma^{-1}\tau})$$

Com tenim igualtat de termes, obtenim que el morfisme Φ és descendible, i com a conseqüència també ho és ψ. Llavors hem vist que $E[N] \otimes (E \otimes L) \leftrightsquigarrow H \otimes L$, descendeix a $E \otimes L \leftrightsquigarrow K \otimes L \cong L$. Això últim és cert H és l'àlgebra de Hopf que correspon al cocicle p_σ i per tant estem sobre els elements fixos per l'acció de G. □

Usant el darrer teorema, podem veure que és possible calcular explícitament l'àlgebra de Hopf associada a una extensió Hopf Galois, ja que tenim les dues implicacions és a dir un si i només si.

Vegem a continuació com recuperem l'àlgebra de Hopf d'un parell de casos particulars.

El primer cas que veurem amb una mica de detall serà l'exemple 2.5. Usant la notació del teorema anterior tenim que $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, $E = \mathbb{Q}(\xi_3, \sqrt[3]{2})$. Tenim que el grup de Galois $G = S_3$, i l'aplicació $\lambda : G \hookrightarrow S^3$ és bijectiva. El grup de Galois G' tindrà dos elements i N el subgrup regular normalitzar per $\lambda(G)$ serà el subgrup alternat d'ordre 3.

Vegem ara amb més detall com recuperem explícitament l'àlgebra de Hopf en un cas en què G té ordre 4.

Començem seleccionant l'extensió amb la que treballarem, per aquest exemple usarem una extensió de Galois biquadràtica $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Com aquesta extensió és normal, usant la notació anterior tenim que $E = L$. Notem que com tenim una extensió normal, el grup de Galois $G' = Gal(E/L)$ serà trivial, i per tant $X = G$.
Notarem els automorfismes que formen el grup de Galois per $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$. Notem que com el grau de l'extensió és 4, $Perm(X) \cong S_4$. Determinem ara les imatges dels automorfismes del grup de Galois.

$$\begin{array}{cccc} \sigma_1 : \sqrt{2} \longmapsto \sqrt{2} & \sigma_2 : \sqrt{2} \longmapsto \sqrt{2} & \sigma_3 : \sqrt{2} \longmapsto -\sqrt{2} & \sigma_4 : \sqrt{2} \longmapsto -\sqrt{2} \\ \sqrt{3} \longmapsto \sqrt{3} & \sqrt{3} \longmapsto -\sqrt{3} & \sqrt{3} \longmapsto \sqrt{3} & \sqrt{3} \longmapsto -\sqrt{3} \end{array}$$

A continuació determinem l'aplicació $\lambda : G \to S_4$, recordem que aquesta actúa per translació a l'esquerra. Donem el càlcul explícit per a σ_2, posem $\Sigma_2 = \lambda(\sigma_2)$.

$$\begin{aligned} \sigma_2\sigma_1 = \sigma_2 &\Rightarrow \Sigma_2(1) = 2, \\ \sigma_2\sigma_2 = \sigma_1 &\Rightarrow \Sigma_2(2) = 1, \\ \sigma_2\sigma_3 = \sigma_4 &\Rightarrow \Sigma_2(3) = 4, \\ \sigma_2\sigma_4 = \sigma_3 &\Rightarrow \Sigma_2(4) = 3. \end{aligned}$$

Anàlogament obtenim les permutacions que definiran la imatge dels altres automorfismes, obtenint:

$$\begin{array}{rccc} \lambda : & G & \to & S_4 \\ & \sigma_1 & \longmapsto & Id \\ & \sigma_2 & \longmapsto & (12)(34) \\ & \sigma_3 & \longmapsto & (13)(24) \\ & \sigma_4 & \longmapsto & (14)(23) \end{array}$$

El següent pas serà trobar el subgrup regular N normalitzat per l'aplicació λ que acabem de definir. Com $|N| = 4$, els possibles subgrups de $Perm(X)$ que poden funcionar seran:

$$\begin{array}{rcll} V_4 & = & \{Id, (12)(34), (13)(24), (14)(23)\} & := \lambda(G) \\ < (1234) > & = & \{Id, (1234), (13)(24), (1432)\} & \\ < (1324) > & = & \{Id, (1324), (12)(34), (1423)\} & \\ < (1243) > & = & \{Id, (1243), (14)(23), (1324)\} & \end{array}$$

Per fer el càlcul usarem el grup generat per $< c := (1234) >$, i notarem els seus elements per c^0, c, c^2, c^3. Per veure que aquesta és una bona elecció, hem de comprovar que $N =< (1234) >$ està normalitzat per $\lambda(G)$. Vegem que $\lambda((\sigma_i)^{-1})c^j\lambda(\sigma_i) \in N$ per a qualsevol parella (i, j) amb $0 \leq i, j \leq 3$. Donem el càlcul per a $\lambda(\sigma_2)$:

$$\begin{array}{rcl} (12)(34)(Id)(12)(34) & = & (Id), \\ (12)(34)(1234)(12)(34) & = & (1423), \\ (12)(34)(13)(24)(12)(34) & = & (13)(24), \\ (12)(34)(1432)(12)(34) & = & (1234). \end{array}$$

D'aquesta manera obtenim que N és el subgrup que busquem, aleshores podem expressar elements de $E[N]$ com a

$$\sum_{i=0}^{3} x_i c^i, \text{ amb } x_i \in E.$$

Per tant l'àlgebra de Hopf que busquem serà de la forma

$$H = \left\{ \sum_{i=0}^{3} x_i c^i \in E[N] : \sigma_j(\sum_{i=0}^{3} x_i c^i) = \sum_{i=0}^{3} x_i c^i, \text{ per a qualsevol } \sigma \in G \right\}.$$

Calculem ara els elements fixos per $\sigma \in G$. A continuació simplificarem la notació i usarem σ com a $\lambda(\sigma)$. Calculem els elements fixos per σ_2 usant que del càlcul anterior tenim el sistema:

$$\left\{ \begin{array}{ll} (\sigma_2)^{-1}\ c\ \sigma_2 & = c^3 \\ (\sigma_2)^{-1}\ c^2\ \sigma_2 & = c^2 \\ (\sigma_2)^{-1}\ c^3\ \sigma_2 & = c \end{array} \right.$$

Calculem la imatge de $\sum_{i=0}^{3} x_i c^i$ per σ_2 usant el sistema anterior.

$$\sigma_2\Big(\sum_{i=0}^{3} x_i c^i\Big) = \sigma_2(x_0)c^0 + \sigma_2(x_1)c^3 + \sigma_2(x_2)c^2 + \sigma_2(x_3)c.$$

I imposant que aquest element sigui fix obtenim:

$$\begin{array}{ll} x_0 = \sigma_2(x_0), & x_2 = \sigma_2(x_2), \\ x_1 = \sigma_2(x_3), & x_3 = \sigma_2(x_1). \end{array}$$

A continuació expressem aquest element en la base natural de L. Si $x \in L$, aleshores

$$\begin{array}{c} x = a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6}, \\ \sigma_2(x) = a_0 + a_1\sqrt{2} - a_2\sqrt{3} - a_3\sqrt{6}, \end{array}$$

amb $a_i \in \mathbb{Q}$. Imposant la condició d'element obtenim $a_2 = a_3 = 0$ i per tant $x_0, x_2 \in \mathbb{Q}(\sqrt{2})$.

Fent un raonament anàleg per a σ_3 i σ_4 obtenim les condicions per als elements fixos. Com σ_2 i σ_3 generen el grup de Galois, no cal fer els càlculs per a σ_4. Aleshores, imposant $x = \sigma_3(x)$ obtenim les condicions:

$$\begin{aligned} x_0 &= \sigma_3(x_0), & x_2 &= \sigma_3(x_2), \\ x_1 &= \sigma_3(x_1), & x_3 &= \sigma_3(x_3). \end{aligned}$$

Per tant, $x_0, x_1, x_2, x_3 \in \mathbb{Q}(\sqrt{3})$. En total, com $x_0, x_2 \in \mathbb{Q}(\sqrt{2})$ i $x_0, x_2 \in \mathbb{Q}(\sqrt{3})$, aleshores $x_0, x_2 \in \mathbb{Q} = \mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3})$. Ara, com $x_1 \in \mathbb{Q}(\sqrt{3})$, podem posar $x_1 = a + b\sqrt{3}$, amb $a, b \in \mathbb{Q}$. Com teniem $x_3 = \sigma_2(x_1)$, obtenim que $x_3 = a - b\sqrt{3}$. En conclusió, un element de l'àlgebra de Hopf H serà de la forma

$$x = x_0 + (a + b\sqrt{3})c + x_2c^2 + (a - b\sqrt{3})c^3 = x_0 + a(c + c^3) + x_2c^2 + b(\sqrt{3}c - \sqrt{3}c^3),$$

amb x_0, a, x_2, b elements de $\mathbb{Q}$. És a dir H és $\mathbb{Q}$-àlgebra amb base $\{1, c+c^3, c^2, \sqrt{3}c-\sqrt{3}c^3\}$ i dimensió 4 sobre $\mathbb{Q}$.

5 Conclusions

La teoria de Galois és una de les més conegudes teories de caire algebraic. Llevat això, al grau de matemàtiques no es profunditza gaire en aquesta. Si bé es donen teoremes molt importants com el teorema d'Artin, la teoria que s'estudia és per a extensions finites i en general separables, on les estructures són grups. Els casos particulars que es veuen més rellevants són els cossos ciclotòmics, les extensions sobre cossos finits amb característica diferent de 0. i les extensions quadràtiques. Després del que hem vist, aconseguim una imatge més general de la teoria de Galois, si bé no hem vist extensions infinites, ja que requeria teoria més avançada, hem vist que aquesta teoria és generalitzable a estructures més complexes a la de grup.

Els coneixements amb els quals partíem eren majorment de l'assignatura d'Equacions algebraiques i Estructures algebraiques. Un cop hem avançat en el tema hem hagut de trobar fonts per tal d'aprendre nous conceptes que ens eren necessaris per poder continuar. Les fonts d'on s'ha obtingut informació han estat en general en format paper, tot i que també hem usat el format digital quan ha estat necessari.

Finalment podem concloure que la teoria de Galois és molt versàtil, i que quan es fan servir estructures diferent de les usuals, el que s'obté és una versió d'aquesta on es poden estudiar casos que amb la teoria tradicional no podríem, com el de les extensions no normals.

Referències

[1] Underwood, R. G: Fundamentals of Hop Algebra, Springer, 2015.

[2] Chase, S; Sweedler, M: Hopf Algebras and Galois Theory, Lecture Notes in Math, Vol.97, Springer-Verlag, New York, (2, 6), 1969.

[3] Childs, L. N: Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, American Mathematical Society, 47-55, 2000.

[4] Childs, L. N: Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, American Mathematical Society, 19-20, 2000.

[5] Childs, L. N: Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, American Mathematical Society, Remark, 11, 2000.

[6] Greither, C; Pareigis, B: Hopf Galois Theory for Separable Field Extensions, Journal of Algebra 106, Mathematisches Institut der Universität München, juny 1987.

[7] Lang, S: Algebra, Third edition, Addison-Wesley Publishing Company, Inc, juny 1994.

[8] Leinster, T: Basic Categoty Theory, `arXiv:1612.09375v1 [math.NT]`, desembre de 2016.

[9] Serre, J. P: Local fields, Graduate texts in Mathematics 67, Springer 1979.