ALGORITHMIC HOPF GALOIS THEORY

Marta Salguero García

Adviser: Teresa Crespo Vicente

MASTER'S FINAL THESIS

Department of Mathematics and Computer Science
University of Barcelona
Barcelona, September 11, 2019

Contents

Abstract

Chase and Sweedler introduce Hopf Galois theory, which is a generalization of Galois theory. The point is to replace the Galois group by a Hopf algebra and the Galois action (by automorphisms) by an action by endomorphisms called Hopf action. This pair gives the so-called Hopf Galois structure. In the case of separable field extensions Greither and Pareigis characterize Hopf Galois structures in terms of groups. This characterization gives a method to determine all Hopf Galois structures of a given separable extension.

In this thesis we present two algorithms written in the computational algebra system Magma to compute all Hopf Galois structures of a given separable extension. Moreover they determine two important properties of the computed Hopf Galois structures. The first algorithm is based on Greither-Pareigis' theorem. It is very efficient but it just reaches degree 11. In order to go further, we develop the second algorithm, which is based on Byott's translation theorem. Therefore in this memory we also detail the proofs of both theorems.

Acknowledgments

I want to thank my adviser, Professor Teresa Crespo, for all the help and time she has spent with me these last years. I have no words to thank her for trusting me, encouraging me and introducing me to research world.

I want to thank my family, especially my parents, and my church in Barcelona for its support during my master studies.

Moreover, I want to thank Sergi, with whom I have spent so many hours studying and solving problems all along this master period. I am also very grateful to my best Bachelor friends: Abel, Stefano, Álex, Cris, David, Marc and Mireia. And I cannot forget Miguel, one my best highschool friends, who moved to Barcelona three years ago.

And finally, but not least, I want to thank God, the Great Mathematician and Creator of the Universe. Thank you, Jesus, for giving me a new life and for giving real meaning to what I am and do.

"Man finds God behind every door science manages to open"

Albert Einstein

Chapter 1

Introduction

Galois theory, named after Évariste Galois, provides a connection between field theory and group theory. Using Galois theory, certain problems in field theory can be reduced to group theory, which is, in some sense, simpler and better understood. Galois theory classifies intermediate fields of a Galois field extension $L|K$ by means of the subgroups of the group $G = \mathrm{Gal}(L|K)$ of K-automorphisms of L.

The Galois action of G on L induces an action of the group algebra $K[G]$ on L. Replacing $K[G]$ with a proper algebra we can generalize Galois theory. In the 1960s, Chase and Sweedler define the notion of Hopf Galois structure on a field extension as a pair $(H, \cdot)$, where H is a Hopf algebra and $\cdot$ is a Hopf action. They are considered the fathers of Hopf Galois theory since they elaborated Galois theory for Hopf Galois field extensions, and they applied it to study inseparable extensions.

The first example of a Hopf algebra was observed in algebraic topology by Heinz Hopf in 1941. This was the homology of a connected Lie group, which is even a graded Hopf algebra. Starting with the late sixties, Hopf algebras became a subject of study from a strictly algebraic point of view, and by the end of the eighties, research in this field grew fastly by the connections with quantum mechanics (the so-called quantum groups are in fact noncommutative and noncocommutative Hopf algebras). Furthermore, Hopf algebras appear in all fields of mathematics: from number theory (formal groups) to algebraic geometry (affine group schemes), for instance.

Later on, Greither and Pareigis studied the Hopf Galois theory of separable field extensions and characterize Hopf Galois structures on a separable extension in terms of groups. This characterization allows running explicit computations and implementation in a computational algebra system as Magma. In particular, a Galois extension with Galois group G is Hopf Galois with Hopf algebra $K[G]$, and this structure is called the classical Galois structure. In general, a field extension may admit several Hopf Galois structures.

Recently a connection between Hopf Galois theory and noncommutative algebra has been found. In 2005 Rump introduced the notion of braces, a generalization of Jacobson radical rings, as a tool for investigating solutions of the Yang-Baxter equation. Roughly speaking, a brace is a set endowed with two group structures related by a sort of distributivity. The quantum Yang-Baxter equation appeared in a paper on statistical mechanics by Yang. It is one of the basic equations in mathematical physics and it laid foundations of the theory of quantum groups.

Moreover, Hopf Galois theory has also applications in number theory in the study of integral normal basis and ramification. Let $L|K$ be a Galois extension of number fields with group G. The Normal Basis Theorem states that there exists an element $z \in L$ such that the set $\{\sigma(z) : \sigma \in G\}$ is a K-basis for L (a normal basis). This is equivalent to L being a free module of rank one over the group algebra $K[G]$. It is natural to wonder whether analogous results hold for the corresponding integer ring extension $\mathcal{O}_L|\mathcal{O}_K$. By Noether's theorem, $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$ if and only if $L|K$ is at most tamely ramified. To study freeness questions for wildly ramified extensions, $\mathcal{O}_K[G]$ is replaced by a proper $\mathcal{O}_K$-Hopf algebra H.

In this dissertation, we start reviewing the construction of a Hopf algebra. Firstly we define algebras as vector spaces endowed with two linear maps satisfying certain properties that may be presented via commutative diagrams, and coalgebras as their dual objects formed by reversing the arrows. Then we define bialgebras as vector spaces which are both algebras and coalgebras such that the two structures satisfy a compatibility relation. Afterwards, a Hopf algebra is a bialgebra with an additional linear map satisfying a condition which may be expressed using the algebra and coalgebra structures. Finally, we use Hopf algebras to define the concept of Hopf Galois structure on a field extension as a pair made up of a Hopf algebra and a certain action by endomorphisms, and state the fundamental theorem of Hopf Galois theory (Chase and Sweedler).

In what follows, we restrict to the case of a separable extension since Greither and Pareigis stablished a bijection between Hopf Galois structures and certain permutations groups. This characterization allows us to use Magma for obtaining explicit computations. So first of all, we introduce the concepts and prove the results that are neeeded to understand the detailed proof of Greither-Pareigis' theorem. Furthermore, we use it to design our first algorithm, which is based on the small program developed in my graduate thesis [Sa]. The first algorithm computes all Hopf Galois structures on a separable extension of given degree and determine two important properties of those in a very efficient way, but we realized it just reaches degree 11. The collected data has enormously helped us to understand the behaviour of separable extensions and has inspired us to obtain some general results on this subject which may be found in our papers [C-S1] and [C-S2].

Therefore in order to overcome the computational problems involving the first algorithm, we need Byott's translation theorem, which gives an equivalent condition to the Hopf Galois character computationally more effective. Hence as previouly, we both develop its proof with all details and implement it in Magma leading to the second algorithm, which shares the structure and properties of the first one with some significant improvements. Moreover, the study of the computational output has allowed us to obtain new results that can be found in our preprint [C-S3].

Chapter 2

Preliminaries

In this chapter we set the foundations of this thesis. It is essentially a summary of the first four chapters of my graduate thesis [Sa], which were based on [Un]. The proofs omitted here may be found in [Sa].

In order to reach to Hopf Galois structures, we need some previous knowledge. We start defining algebras as vector spaces endowed with two linear maps satisfying certain properties which may be presented via commutative diagrams. Next we define coalgebras as co-objects to algebras formed by reversing the arrows in the diagrams for algebras. Then bialgebras come up as vector spaces which are both algebras and coalgebras. Afterwards, we construct Hopf algebras as bialgebras with an additional map. Finally, the point is to replace Galois groups by Hopf algebras and the Galois action by a 'Hopf action' by endomorphisms. This pair gives the so-called Hopf Galois structures.

Let K be a field and denote $\otimes := \otimes_K$.

2.1 Algebras and coalgebras

In this section we present the diagram-theoretic definition of an algebra and define coalgebras as co-objects to algebras. Then we state the main results about duality.

Definition 2.1.1. A K-**algebra** is a triple (A, m_A, λ_A) consisting of a K-vector space A and K-linear maps $m_A : A \otimes A \to A$ and $\lambda_A : K \to A$ that satisfy:

$$\begin{tikzcd}
A \otimes A \otimes A \arrow[r, "I_A \otimes m_A"] \arrow[d, "m_A \otimes I_A"'] & A \otimes A \arrow[d, "m_A"] \\
A \otimes A \arrow[r, "m_A"'] & A
\end{tikzcd}$$

Associative property

$$\begin{tikzcd}
A \otimes A \arrow[rd, "m_A"] & K \otimes A \arrow[l, "\lambda_A \otimes I_A"'] \arrow[d, "s_1"] \\
A \otimes K \arrow[u, "I_A \otimes \lambda_A"] \arrow[r, "s_2"'] & A
\end{tikzcd}$$

Unit property

The map $I_A : A \to A$ is the identity map on A, the map $s_1 : K \otimes A \to A$ is defined by $r \otimes a \mapsto ra$ and the map $s_2 : A \otimes K \to A$ is defined by $a \otimes r \mapsto ra$.

The map m_A is called **multiplication map** and λ_A is called **unit map**.

The K-algebra A is **commutative** if $m_A \tau = m_A$, where $\tau := \tau_{A \otimes A}$ denotes the **twist map** defined as $\tau(a \otimes b) = b \otimes a$.

Remark 2.1.2. We can recover the usual definition of algebra by writing the product as $m_A(a \otimes b) = ab$, for all $a, b \in A$, and unit as $\lambda_A(1_K) = 1_A$. In the sequel we will use both notations.

Example 2.1.3. The field K as a vector space over itself is a commutative K-algebra called the **trivial algebra**:

$$\begin{array}{rcrcl} m_K & : & K \otimes K & \to & K \\ & & r \otimes s & \mapsto & rs \end{array} \qquad \begin{array}{rcrcl} \lambda_K & : & K & \to & K \\ & & r & \mapsto & r \end{array}$$

Example 2.1.4. The polynomial ring $K[x]$ is a commutative K-algebra called the **polynomial algebra**:

$$\begin{array}{rcrcl} m_{K[x]} & : & K[x] \otimes K[x] & \to & K[x] \\ & & x^i \otimes x^j & \mapsto & x^{i+j} \end{array} \qquad \begin{array}{rcrcl} \lambda_{K[x]} & : & K & \to & K[x] \\ & & r & \mapsto & r \end{array}$$

Example 2.1.5. Let G be a finite group with identity element 1_G. The group ring $K[G] = \left\{ \sum\limits_{g \in G} r_g g \ : \ r_g \in K \right\}$ is a K-algebra called the **group algebra**:

$$\begin{array}{rcrcl} m_{K[G]} & : & K[G] \otimes K[G] & \to & K[G] \\ & & x \otimes y & \mapsto & xy \end{array} \qquad \begin{array}{rcrcl} \lambda_{K[G]} & : & K & \to & K[G] \\ & & r & \mapsto & r1_G \end{array}$$

Clearly, $K[G]$ is commutative if, and only if, G is abelian.

Example 2.1.6. Let C be a finite set. Then $\mathrm{Map}(C, K) =: M$ is a K-algebra:

$$\begin{array}{rcrcl} m_M & : & M \otimes M & \to & M \\ & & f \otimes g & \mapsto & m_M(f \otimes g)(c) = f(c)g(c) \end{array}$$

and

$$\begin{array}{rcrcl} \lambda_M & : & K & \to & M \\ & & r & \mapsto & \lambda_M(r)(c) = r \end{array}$$

Notice that $\{f_c : \ c \in C\}$ is a K-basis, where:

$$\begin{array}{rcrcl} f_c & : & C & \to & K \\ & & d & \mapsto & f_c(d) = \begin{cases} 1 & \text{if } d = c \\ 0 & \text{otherwise} \end{cases} \end{array}$$

Hence $\dim_K(\mathrm{Map}(C, K)) = |C|$ as a K-vector space.

Definition 2.1.7. Let A, B be K-algebras. The **tensor product of algebras** $A \otimes B$ has the structure of a K-algebra with multiplication map given by

$$\begin{array}{rccl} m_{A\otimes B} & : & (A \otimes B) \otimes (A \otimes B) & \rightarrow & A \otimes B \\ & & (a \otimes b) \otimes (c \otimes d) & \mapsto & (m_A \otimes m_B)(I_A \otimes \tau \otimes I_B)(a \otimes (b \otimes c) \otimes d) \end{array}$$

that is,

$$(a \otimes b)(c \otimes d) = ac \otimes bd$$

and unit map defined as

$$\begin{array}{rccl} \lambda_{A\otimes B} & : & K & \rightarrow & A \otimes B \\ & & 1_K & \mapsto & \lambda_A(1_K) \otimes \lambda_B(1_K) = 1_A \otimes 1_B \end{array}$$

Definition 2.1.8. Let (A, m_A, λ_A) and (B, m_B, λ_B) be K-algebras. A K-**algebra homomorphism** from A to B is a K-linear map $\phi : A \rightarrow B$ that preserves the algebra structure, that is:

$$\phi \circ m_A = m_B \circ (\phi \otimes \phi) \qquad\qquad \phi \circ \lambda_A = \lambda_B$$

A K-algebra homomorphism that is injective and surjective is a K-**algebra isomorphism**.

We will now describe objects that are dual (in some sense) to algebras: they are obtained by reversing the arrows in the structure maps for algebras and are called coalgebras.

Definition 2.1.9. A K-**coalgebra** is a triple $(C, \Delta_C, \varepsilon_C)$ consisting of a K-vector space C and K-linear maps $\Delta_C : C \rightarrow C \otimes C$ and $\varepsilon_C : C \rightarrow K$ that satisfy:

$$\begin{tikzcd}
C \arrow[r, "\Delta_C"] \arrow[d, "\Delta_C"'] & C \otimes C \arrow[d, "\mathrm{I}_C \otimes \Delta_C"] \\
C \otimes C \arrow[r, "\Delta_C \otimes \mathrm{I}_C"'] & C \otimes C \otimes C
\end{tikzcd}$$

Coassociative property

$$\begin{tikzcd}
C \arrow[r, "1_K \otimes \mathrm{I}_C"] \arrow[d, "\mathrm{I}_C \otimes 1_K"'] \arrow[dr, "\Delta_C"] & K \otimes C \\
C \otimes K & C \otimes C \arrow[l, "\mathrm{I}_C \otimes \varepsilon_C"] \arrow[u, "\varepsilon_C \otimes \mathrm{I}_C"']
\end{tikzcd}$$

Counit property

The map $I_C : C \rightarrow C$ is the identity map on C and the map $1_K : C \rightarrow K$ is defined by $c \mapsto 1_K$.

The map Δ_C is called **comultiplication map** and ε_C is called **counit map**.

The K-coalgebra C is **cocommutative** if $\tau\Delta_C = \Delta_C$.

We will now introduce **Sweedler notation** to write the image of comultiplication map. Sweedler notation is a special notation for the operations in a coalgebra. Given a K-coalgebra C and an element $c \in C$, Sweedler suggests not to make up new symbols but rather use composed symbols:

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

Example 2.1.10. The field K as a vector space over itself is a cocommutative K-coalgebra called the **trivial coalgebra**:

$$\begin{array}{rcccl} \Delta_K & : & K & \to & K \otimes K \\ & & r & \mapsto & r \otimes 1_K \end{array} \qquad \begin{array}{rcccl} \varepsilon_K & : & K & \to & K \\ & & r & \mapsto & r \end{array}$$

In the next examples of coalgebras, comultiplication and counit maps are defined on basic elements and extended by linearity to the whole coalgebra.

Example 2.1.11. Let G be a finite group. The group ring $K[G]$ (defined as in Example 2.1.5) is a cocommutative K-coalgebra called the **group coalgebra**:

$$\begin{array}{rcccl} \Delta_{K[G]} & : & K[G] & \to & K[G] \otimes K[G] \\ & & g & \mapsto & g \otimes g \end{array} \qquad \begin{array}{rcccl} \varepsilon_{K[G]} & : & K[G] & \to & K \\ & & g & \mapsto & 1_K \end{array}$$

Example 2.1.12. Let $K[x]$ be the K-vector space of polynomials in the indeterminate x with canonical basis $\{1, x, x^2, \dots\}$. We can endow $K[x]$ with two structures of cocommutative K-coalgebras: the **polynomial coalgebra**

$$\begin{array}{rcccl} \Delta_{K[x]} & : & K[x] & \to & K[x] \otimes K[x] \\ & & x^m & \mapsto & x^m \otimes x^m \end{array} \qquad \begin{array}{rcccl} \varepsilon_{K[x]} & : & K[x] & \to & K \\ & & x^m & \mapsto & 1_K \end{array}$$

and the so-called **divided power coalgebra**

$$\begin{array}{rcccl} \Delta_{K[x]} & : & K[x] & \to & K[x] \otimes K[x] \\ & & x^m & \mapsto & \sum_{i=0}^{n} \binom{m}{i} x^i \otimes x^{m-i} \end{array} \qquad \begin{array}{rcccl} \varepsilon_{K[x]} & : & K[x] & \to & K \\ & & x^m & \mapsto & \delta_{0,m} \end{array}$$

Definition 2.1.13. Let C, D be K-coalgebras. The **tensor product of coalgebras** $C \otimes D$ has the structure of a K-coalgebra with comultiplication map given by

$$\begin{array}{rcccl} \Delta_{C\otimes D} & : & C \otimes D & \to & (C \otimes D) \otimes (C \otimes D) \\ & & c \otimes d & \mapsto & (I_C \otimes \tau \otimes I_D)(\Delta_C \otimes \Delta_D)(c \otimes d) \end{array}$$

and counit map defined as

$$\begin{array}{rcccl} \varepsilon_{C\otimes D} & : & C \otimes D & \to & K \\ & & c \otimes d & \mapsto & (\varepsilon_C \otimes \varepsilon_D)(c \otimes d) = \varepsilon_C(c)\varepsilon_D(d) \end{array}$$

Definition 2.1.14. Let C be a K-coalgebra. A non-zero element $c \in C$ for which $\Delta_C(c) = c \otimes c$ is a **grouplike element** of C.

Remark 2.1.15. Let G be a finite group and consider the coalgebra $K[G]$. By definition of $\Delta_{K[G]}$, it follows that the set of grouplike elements of $K[G]$ is G.

Proposition 2.1.16. *If c is a grouplike element of a K-coalgebra C, then $\varepsilon_C(c) = 1$.*

Proposition 2.1.17. *Let C be a K-coalgebra and let $G(C)$ denote the set of grouplike elements of C. Then $G(C)$ is a linearly independent subset of C.*

Definition 2.1.18. Let $(C, \Delta_C, \varepsilon_C)$, $(D, \Delta_D, \varepsilon_D)$ be K-coalgebras. A K-**coalgebra homomorphism** from C to D is a K-linear map $\phi : C \to D$ that preserves the coalgebra structure, that is:

$$(\phi \otimes \phi) \circ \Delta_C = \Delta_D \circ \phi \qquad\qquad \varepsilon_C = \varepsilon_D \circ \phi$$

A K-coalgebra homomorphism that is injective and surjective is a K-**coalgebra isomorphism**.

Proposition 2.1.19. *Let C be a K-coalgebra. Then the counit map $\varepsilon_C : C \to K$ is a K-coalgebra homomorphism.*

Theorem 2.1.20. *Let A be a finite dimensional K-vector space. Then A is a (commutative) K-algebra if and only if A^* is a (cocommutative) K-coalgebra, where the structure maps of A^* are induced from the transpose of the structure maps of A, and reciprocally.*

2.1.1 Modules and comodules

In this section we present the diagram-theoretic definition of a module over an algebra, which is nothing but the structure given by the action of an algebra on a vector space. Similarly, we define comodules as co-objects to modules over a coalgebra.

Let (A, m_A, λ_A) be a K-algebra.

Definition 2.1.21. A **left** A-**module** is a pair (M, μ_M) consisting of a K-vector space M and a K-linear action $\cdot := \mu_M : A \otimes M \to M$ that satisfies:

$$\begin{tikzcd}
A \otimes A \otimes M \arrow[r, "I_A \otimes \mu_M"] \arrow[d, "m_A \otimes I_M"'] & A \otimes M \arrow[d, "\mu_M"] \\
A \otimes M \arrow[r, "\mu_M"'] & A
\end{tikzcd}$$

Associative property

$$\begin{tikzcd}
K \otimes M \arrow[rr, "\sim"] \arrow[dr, "\lambda_A \otimes \mathrm{I}_M"'] & & M \\
& A \otimes M \arrow[ur, "\mu_M"'] &
\end{tikzcd}$$

Unit property

The map $K \otimes M \to M$ is the isomorphism defined by $1_K \otimes m \mapsto m$.

1. The associative property is equivalent to: for all $a, b \in A$, $m \in M$,
$$(ab) \cdot m = a \cdot (b \cdot m)$$

2. The action μ_M is called **scalar multiplication** and the unit property is equivalent to: for all $m \in M$,
$$m = 1_A \cdot m$$

Let $(C, \Delta_C, \varepsilon_C)$ be a K-coalgebra.

Definition 2.1.22. A **left C-comodule** is a pair (N, α_N) consisting of a K-vector space N and a K-linear coaction $\alpha_N : N \to C \otimes N$ that satisfies:

$$\begin{tikzcd}
N \arrow[r, "\alpha_N"] \arrow[d, "\alpha_N"'] & C \otimes N \arrow[d, "\Delta_C \otimes \mathrm{I}_N"] \\
C \otimes N \arrow[r, "\mathrm{I}_C \otimes \alpha_N"'] & C \otimes C \otimes N
\end{tikzcd}
\qquad
\begin{tikzcd}
N \arrow[rr, "\sim"] \arrow[dr, "\alpha_N"'] & & K \otimes N \\
& C \otimes N \arrow[ur, "\varepsilon_C \otimes \mathrm{I}_N"'] &
\end{tikzcd}$$

Coassociative property **Counit property**

The map $N \to K \otimes N$ is the isomorphism defined by $n \mapsto 1_K \otimes n$ and the Sweedler notation for coaction is: for an element $n \in N$,
$$\alpha_N(n) = \sum_{(n)} n_{(0)} \otimes n_{(1)}.$$

2.2 Bialgebras

In this section, we introduce bialgebras, which are vector spaces that are both algebras and coalgebras such that the algebra operations are coalgebra homomorphisms or, equivalently, the coalgebra operations are algebra homomorphisms.

Afterwards we show how a bialgebra can act on an algebra and on a coalgebra endowing them with the structure of module algebra and module coalgebra, resp. Similarly, we show how a bialgebra B can *co*act on an algebra and on a coalgebra giving them the structure of *co*module algebra and *co*module coalgebra, resp.

Definition 2.2.1. A K-**bialgebra** is K-vector space B together with K-linear maps m_B, λ_B, Δ_B, ε_B that satisfy that:

1. (B, m_B, λ_B) is a K-algebra,

2. $(B, \Delta_B, \varepsilon_B)$ is a K-coalgebra,

3. Δ_B and ε_B are K-algebra homomorphisms (or equivalently, m_B and λ_B are K-coalgebra homomorphisms).

A K-bialgebra B is **commutative** if it is a commutative algebra; B is **cocommutative** if it is a cocommutative coalgebra.

Definition 2.2.2. Let B be a bialgebra. A **primitive element** of B is an element $b \in B$ such that $\Delta_B(b) = 1 \otimes b + b \otimes 1$.

Example 2.2.3. The field K as a vector space over itself is a commutative and cocommutative K-bialgebra (see Examples 2.1.3 and 2.1.10). It is called the **trivial** K**-bialgebra**.

Example 2.2.4. Let G be a finite group. From Example 2.1.5 and Example 2.1.11, $K[G]$ has the structure of an algebra and a cocommutative coalgebra. It is easy to check that comultiplication and counit maps are algebra homomorphisms, so that $K[G]$ is a cocommutative bialgebra. It is called the **group bialgebra**. It is commutative if, and only if, G is abelian.

Example 2.2.5. Let $K[x]$ be the K-vector space of polynomials. From Example 2.1.4 we know that $K[x]$ has the structure of a commutative algebra. Moreover, in Example 2.1.12, we showed that it can be endowed with two structures as a cocommutative coalgebra, which induce two distinct bialgebra structures that are, surprisingly, the only bialgebra structures on $K[x]$ up to isomorphism:

- The polynomial coalgebra induces the so-called **polynomial bialgebra with** $\boldsymbol{x}$ **grouplike**, since x is grouplike: $\Delta_{K[x]}(x) = x \otimes x$.

- The divided power coalgebra induces the so-called **polynomial bialgebra with** $\boldsymbol{x}$ **primitive**, since x is primitive: $\Delta_{K[x]}(x) = 1 \otimes x + x \otimes 1$.

Definition 2.2.6. Let B, B' be K- bialgebras. Since B and B' are algebras and coalgebras, $B \otimes B'$ is an algebra and a coalgebra (Definitions 2.1.7 and 2.1.13). It is easy to show that $\Delta_{B\otimes B'}$ and $\varepsilon_{B\otimes B'}$ are algebra homomorphisms, and hence the **tensor product of bialgebras** $B \otimes B'$ has the structure of a K-bialgebra.

Definition 2.2.7. Let B, B' be bialgebras. A K-**bialgebra homomorphism** from B to B' is a K-linear map $\phi : B \to B'$ which is both an algebra and a coalgebra homomorphism. A K-bialgebra homomorphism that is injective and surjective is a K-**bialgebra isomorphism**.

Theorem 2.2.8. *Let B be a finite dimensional K-vector space. Then B is a K-bialgebra if and only if B^* is a K-bialgebra, where the structure maps of B^* are induced from the transpose of the structure maps of B, and reciprocally.*

2.2.1 Module algebras and module coalgebras

In this section, we show how a bialgebra B can act on an algebra giving it the structure of a B-module algebra, and similarly how B can act on a coalgebra.

Let $(B, m_B, \lambda_B, \Delta_B, \varepsilon_B)$ be a K-bialgebra.

Definition 2.2.9. A **left B-module K-algebra** is a K-vector space M together with K-linear maps $m_M : M \otimes M \to M$, $\lambda_M : K \to M$, and a K-linear action $\cdot := \mu_M : B \otimes M \to M$ that satisfies:

1. (M, μ_M) is a B-module,
2. (M, m_M, λ_M) is a K-algebra,
3. Any of these three equivalent conditions:

   (a) The action of B on M is compatible with the operations of M as an algebra, that is, the following conditions hold or the diagrams commute:

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

$$\begin{tikzcd}
B \otimes M \otimes M \arrow[r, "I_B \otimes m_M"] \arrow[d, "\Delta_B \otimes I_{M\otimes M}"'] & B \otimes M \arrow[r, "\mu_M"] & M \\
B \otimes B \otimes M \otimes M \arrow[r, "I_B \otimes \tau \otimes I_M"'] & B \otimes M \otimes B \otimes M \arrow[r, "\mu_M \otimes \mu_M"'] & M \otimes M \arrow[u, "m_M"']
\end{tikzcd}$$

   Unit: $b \cdot 1_M = \varepsilon_B(b) 1_M, \ \forall \ b \in B$

$$\begin{tikzcd}
B \otimes M \arrow[rr, "\mu_M"] \arrow[dr, "\varepsilon_B \otimes I_M"'] & & M \\
& K \otimes M \arrow[ur, "\sim"'] &
\end{tikzcd} \tag{2.1}$$

   (b) the algebra operations m_M and λ_M are B-module homomorphisms:

   Multiplication: $m_M : M \otimes M \to M$, where M is already a B-module, so that we have to endow $M \otimes M$ with a B-module structure, ie, we have to define an action $* = \mu_{M\otimes M}$ of B on $M \otimes M$ such that the diagram commutes:

$$\begin{tikzcd}
B \otimes M \otimes M \arrow[r, "\mu_{M\otimes M}"] \arrow[d, "\Delta_B \otimes \mathrm{I}_{M\otimes M}"'] & M \otimes M \\
B \otimes B \otimes M \otimes M \arrow[r, "\mathrm{I}_B \otimes \tau \otimes \mathrm{I}_M"'] & B \otimes M \otimes B \otimes M \arrow[u, "\mu_M \otimes \mu_M"']
\end{tikzcd}$$

or equivalently, the following condition holds: for every $b \in B$, $m, n \in M$,

$$b * (m \otimes n) = \sum_{(b)} (b_{(1)} \cdot m) \otimes (b_{(2)} \cdot n)$$

Therefore, multiplication m_M satisfies that for every $b \in B$, $m, n \in M$,

$$m_M(\mu_{M\otimes M}(b \otimes (m \otimes n)) = \mu_M(b \otimes m_M(m \otimes n))$$

<u>Unit</u>: $\lambda_M : K \to M$, where M is already a B-module, so that we have to endow K with a B-module structure, ie, we have to define an action μ_K of B on K, which we denote by juxtaposition, such that the diagram commutes:

$$\begin{tikzcd}
B \otimes K \arrow[rr, "\mu_K"] \arrow[dr, "\sim"'] & & K \\
& B \arrow[ur, "\varepsilon_B"'] &
\end{tikzcd}$$

or equivalently, the following condition holds: for every $b \in B$,

$$b\ 1_K = \varepsilon_B(b)$$

Therefore, unit λ_M satisfies that for every $b \in B$

$$\lambda_M(\mu_K(b \otimes 1_K) = \mu_M(b \otimes \lambda_M(1_K))$$

(c) the action μ_M is a K-algebra homomorphism:

Since the action is defined over algebras and is linear, it remains to impose that it preserves the inner product of M: for every $a, b \in B$, $m, n \in M$,

$$(ab) \cdot (mn) = (a \cdot m)(b \cdot n)$$

or equivalently, the following diagram commutes:

$$\begin{tikzcd}
B \otimes M \otimes B \otimes M \arrow[r, "m_{B\otimes M}"] \arrow[d, "\mu_M \otimes \mu_M"'] & B \otimes M \arrow[d, "\mu_M"] \\
M \otimes M \arrow[r, "m_M"'] & M
\end{tikzcd}$$

Remark 2.2.10. If A is a left $K[G]$-module K-algebra, then:

$$\sigma(ab) = \sigma(a)\sigma(b), \text{ for every } a, b \in A, \ \sigma \in G.$$

Definition 2.2.11. Let M, M' be left B-module K-algebras. A **left B-module K-algebra homomorphism** from M to M' is a K-linear map $\phi : M \to M'$ which is both an algebra and a left B-module homomorphism.

In a similar way, we define a left module coalgebra (with not so many details).

Definition 2.2.12. A **left B-module K-coalgebra** is a K-vector space M together with K-linear maps $\Delta_M : M \to M \otimes M$, $\varepsilon_M : M \to K$, and a K-linear action $\cdot := \mu_M : B \otimes M \to M$ that satisfies:

1. (M, μ_M) is a B-module,
2. $(M, \Delta_M, \varepsilon_M)$ is a K-coalgebra,
3. Any of these three equivalent conditions:
   (a) The action of B on M is compatible with the operations of M as a coalgebra, that is, the following conditions hold or the diagrams commute:

<u>Comultiplication</u>: $\Delta_M(b \cdot m) = \sum_{(b,m)} (b_{(1)} \cdot m_{(1)}) \otimes (b_{(2)} \cdot m_{(2)}), \ \forall \ b \in B, \ m \in M$

$$\begin{tikzcd}
B \otimes M \arrow[r, "\mu_M"] \arrow[d, "\Delta_B \otimes \Delta_M"'] & M \arrow[r, "\Delta_M"] & M \otimes M \\
B \otimes B \otimes M \otimes M \arrow[rr, "\mathrm{I}_B \otimes \tau \otimes \mathrm{I}_M"'] & & B \otimes M \otimes B \otimes M \arrow[u, "\mu_M \otimes \mu_M"']
\end{tikzcd}$$

<u>Counit</u>: $\varepsilon_M(b \cdot m) = \varepsilon_B(b)\varepsilon_M(m), \ \forall \ b \in B, \ m \in M$

$$\begin{tikzcd}
B \otimes M \arrow[rr, "\varepsilon_{B \otimes M}"] \arrow[dr, "\mu_M"'] & & K \\
& M \arrow[ur, "\varepsilon_M"'] &
\end{tikzcd}$$

   (b) the coalgebra operations Δ_M and ε_M are B-module homomorphisms.
   (c) the action μ_M is a K-coalgebra homomorphism.

Definition 2.2.13. Let M, M' be left B-module K-coalgebras. A **left B-module K-coalgebra homomorphism** from M to M' is a K-linear map $\phi : M \to M'$ which is both a coalgebra and a left B-module homomorphism.

2.2.2 Comodule algebras and comodule coalgebras

In this section, we show how a bialgebra B can *co*act on an algebra giving it the structure of a B-*co*module algebra, and similarly how B can *co*act on a coalgebra.

Let $(B, m_B, \lambda_B, \Delta_B, \varepsilon_B)$ be a K-bialgebra.

Definition 2.2.14. A **left B-comodule K-algebra** is a K-vector space N together with K-linear maps $m_N : N \otimes N \to N$, $\lambda_N : K \to N$, and a K-linear coaction $\alpha_N : N \to B \otimes N$ that satisfies:

1. (N, α_N) is a B-comodule,

2. (N, m_N, λ_N) is a K-algebra,

3. Any of these three equivalent conditions:

   (a) The coaction of B on N is compatible with the operations of N as an algebra, that is, the following conditions hold or the diagrams commute:

   Multiplication: $\alpha_N(mn) = \sum_{(m,n)} (m_{(0)}n_{(0)}) \otimes (m_{(1)}n_{(1)}),\ \forall\ m, n \in N$

$$\begin{tikzcd}
N \otimes N \arrow[r, "m_N"] \arrow[d, "\alpha_N \otimes \alpha_N"'] & N \arrow[r, "\alpha_N"] & B \otimes N \\
B \otimes N \otimes B \otimes N \arrow[rr, "\mathrm{I}_B \otimes \tau \otimes \mathrm{I}_N"'] & & B \otimes B \otimes N \otimes N \arrow[u, "m_B \otimes m_N"']
\end{tikzcd}$$

   Unit: $\alpha_N(1_N) = 1_B \otimes 1_N$

$$\begin{tikzcd}
N \arrow[rr, "\alpha_N"] \arrow[dr, "\sim"'] & & B \otimes N \\
& K \otimes N \arrow[ur, "\lambda_B \otimes \mathrm{I}_N"'] &
\end{tikzcd}$$

   (b) the algebra operations m_N and λ_N are B-comodule homomorphisms:

   Multiplication: $m_N : N \otimes N \to N$, where N is already a B-comodule, so that we have to endow $N \otimes N$ with a B-comodule structure, ie, we have to define a coaction $\alpha_{N \otimes N}$ of B on $N \otimes N$ such that the diagram commutes:

$$\begin{tikzcd}
N \otimes N \arrow[r, "\alpha_{N\otimes N}"] \arrow[d, "\alpha_N \otimes \alpha_N"'] & B \otimes N \otimes N \\
B \otimes N \otimes B \otimes N \arrow[r, "\mathrm{I}_B \otimes \tau \otimes \mathrm{I}_N"] & B \otimes B \otimes N \otimes N \arrow[u, "m_B \otimes \mathrm{I}_N \otimes \mathrm{I}_N"']
\end{tikzcd}$$

or equivalently, the following condition holds: for every $m, n \in M$,

$$\alpha_{N\otimes N}(m \otimes n) = \sum_{(m,n)} (m_{(0)}n_{(0)}) \otimes m_{(1)} \otimes n_{(1)}$$

Therefore, multiplication m_N satisfies that for every $m, n \in N$,

$$\alpha_N(m_N(m \otimes n)) = (\mathrm{I}_B \otimes m_N)(\alpha_{N\otimes N}(m \otimes n))$$

<u>Unit</u>: $\lambda_N : K \to N$, where N is already a B-comodule, so that we have to endow K with a B-comodule structure, ie, we have to define a coaction α_K of B on K such that the diagram commutes:

$$\begin{tikzcd}
K \arrow[rr, "\alpha_K"] \arrow[dr, "\lambda_B"'] & & B \otimes K \\
& B \arrow[ur, "\sim"'] &
\end{tikzcd}$$

or equivalently, the following condition holds: for every $b \in B$,

$$\alpha_K(1_K) = 1_B \otimes 1_K$$

Therefore, unit λ_N satisfies that for every $b \in B$

$$\alpha_N(\lambda_N(1_K)) = (\mathrm{I}_B \otimes \lambda_N)(\alpha_K(1_K))$$

(c) the coaction α_N is a K-algebra homomorphism:

Since the coaction is defined over algebras and is linear, it remains to impose that it preserves the inner product of N: for every $m, n \in N$,

$$\alpha_N(mn) = \alpha(m)\alpha(n)$$

or equivalently, the following diagram commutes:

$$\begin{tikzcd}
B \otimes N \otimes B \otimes N \arrow[r, "m_{B\otimes N}"] & B \otimes N \\
N \otimes N \arrow[r, "m_N"'] \arrow[u, "\alpha_N \otimes \alpha_N"] & N \arrow[u, "\alpha_N"']
\end{tikzcd}$$

Definition 2.2.15. Let N, N' be left B-comodule K-algebras. A **left B-comodule K-algebra homomorphism** from N to N' is a K-linear map $\phi : N \to N'$ which is both an algebra and a left B-comodule homomorphism.

In a similar way, we define a left comodule coalgebra (with not so many details).

Definition 2.2.16. A **left B-comodule K-coalgebra** is a K-vector space N together with K-linear maps $\Delta_N : N \to N \otimes N$, $\varepsilon_N : N \to K$, and a K-linear coaction $\alpha_N : N \to B \otimes N$ that satisfies:

1. (N, α_N) is a B-comodule,
2. $(N, \Delta_N, \varepsilon_N)$ is a K-coalgebra,
3. Any of these three equivalent conditions:

   (a) The coaction of B on N is compatible with the operations of N as a coalgebra, that is, the following diagrams commute:

   Comultiplication:

$$\begin{tikzcd}
N \arrow[r, "\Delta_N"] \arrow[d, "\alpha_N"'] & N \otimes N \arrow[r, "\alpha_N \otimes \alpha_N"] & B \otimes N \otimes B \otimes N \\
B \otimes N \arrow[rr, "\Delta_B \otimes \Delta_N"'] & & B \otimes B \otimes N \otimes N \arrow[u, "\mathrm{I}_B \otimes \tau \otimes \mathrm{I}_N"']
\end{tikzcd}$$

   Counit:

$$\begin{tikzcd}
N \arrow[r, "\varepsilon_N"] \arrow[d, "\alpha_N"'] & K \arrow[d, "\alpha_K"] \\
B \otimes N \arrow[r, "\mathrm{I}_B \otimes \varepsilon_N"'] & B \otimes K
\end{tikzcd}$$

   (b) the coalgebra operations Δ_N and ε_N are B-comodule homomorphisms.

   (c) the coaction α_N is a K-coalgebra homomorphism.

Definition 2.2.17. Let N, N' be left B-comodule K-coalgebras. A **left B-comodule K-coalgebra homomorphism** from N to N' is a K-linear map $\phi : N \to N'$ which is both a coalgebra and a left B-comodule homomorphism.

Proposition 2.2.18. *Let H be a finite K-Hopf algebra and let S be a K-algebra. If*

$$\begin{array}{rccl} \alpha & : & S & \to & S \otimes H^* \\ & & s & \mapsto & \sum_{(s)} s_{(0)} \otimes s_{(1)} \end{array}$$

is a coaction, then

$$\begin{array}{rccl} \cdot & : & H \otimes S & \to & S \\ & & h \otimes s & \mapsto & \sum_{(s)} s_{(1)}(h) s_{(0)} \end{array}$$

is an action. Moreover

1. *$(S, \cdot)$ is a left H-module K-algebra iff (S, α) is a right H^*-comodule K-algebra.*
2. *If S is a finite commutative K-algebra which is also a left H-module K-algebra, then the map*

$$\begin{array}{rccl} j & : & S \otimes H & \to & \mathrm{End}_K(S) \\ & & s \otimes h & \mapsto & j(s \otimes h)(t) := s(h \cdot t) \end{array}$$

is a K-linear isomorphism if and only if the map

$$\begin{array}{rccl} \gamma & : & S \otimes S & \to & S \otimes H^* \\ & & s \otimes t & \mapsto & m_{S \otimes H^*}((s \otimes \mathrm{I}_{H^*}) \otimes \alpha_S(t)) = (s \otimes \mathrm{I}_{H^*}) \alpha_S(t) = \sum_{(t)} st_{(0)} \otimes t_{(1)} \end{array}$$

is a K-linear isomorphism.

Proof. Sketch of the proof. Firstly, one may check that if α is a coaction, then $\cdot$ satisfies the properties of an action.

1. Moreover, using this fact, one may check that if (S, α) is a right H^*-comodule K-algebra, then $(S, \cdot)$ satisfies the properties of a left H-module K-algebra.

   Now assume $(S, \cdot)$ to be a left H-module K-algebra. Since H is a finite K-Hopf algebra, then H is a finite K-vector space. Let $\{h_1, \ldots, h_n\}$ be a K-basis of H and let $\{f_1, \ldots, f_n\}$ be its dual basis. Recall it satisfies $f_i(h_j) = \delta_{ij}$, for every $i, j \in \{1, \ldots, n\}$.

   Hence, for every $h \in H$, $h = \sum_{i=1}^{n} f_i(h) h_i$. Then one may check that the map defined by

$$\begin{array}{rcl} S & \to & S \otimes H^* \\ s & \mapsto & \sum_{i=1}^{n} (h_i \cdot s) \otimes f_i \end{array}$$

   coincides with α.

   Finally, it remains to check that if $(S, \cdot)$ is a left H-module K-algebra, then (S, α) is a right H^*-comodule K-algebra.

2. It is a consequence of 1: by assumption, S is a left H-module K-algebra, hence by 1 it is a right H^*-comodule K-algebra with coaction α.

   Consider the following diagram:

$$\begin{tikzcd}
S \otimes H \arrow[r, "j"] \arrow[d, "\eta"'] & \mathrm{Hom}_K(S,S) \arrow[d, "\beta"] \\
\mathrm{Hom}_S(S \otimes H^*, S) \arrow[r, "\gamma^*"'] & \mathrm{Hom}_S(S \otimes S, S)
\end{tikzcd}$$

   where:

   - $\eta(s \otimes h)(t \otimes f) = stf(h), \ \forall \ s \otimes h \in S \otimes H, \ t \otimes f \in S \otimes H^*$;
   - $\beta(f)(s \otimes t) = sf(t), \ \forall \ f \in \mathrm{End}_K(S,S), \ s \otimes t \in S \otimes S$;
   - $\gamma^*(f) = f \circ \gamma, \ \forall \ f \in \mathrm{Hom}_S(S \otimes H^*, S)$.

   Let us see that the diagram commutes: indeed, for every $s \otimes h \in S \otimes H$ and $t \otimes u \in S \otimes S$,

$$\begin{aligned}
\gamma^*(\eta(s \otimes h))(t \otimes u) &= \eta(s \otimes h)(\gamma(t \otimes u)) && \text{(def } \gamma^*) \\
&= \eta(s \otimes h)\left(\sum_{(u)} tu_{(0)} \otimes u_{(1)}\right) && \text{(def } \gamma) \\
&= t\sum_{(u)} \eta(s \otimes h)(u_{(0)} \otimes u_{(1)}) && (\eta \text{ linear}) \\
&= ts\sum_{(u)} u_{(0)}u_{(1)}(h) && \text{(def } \eta) \\
&= ts(h \cdot u) && \text{(by 1)} \\
&= tj(s \otimes h)(u) && \text{(def } j) \\
&= \beta(j(s \otimes h))(t \otimes u) && \text{(def } \beta)
\end{aligned}$$

   Now observe that both $S \otimes S$ and $S \otimes H^*$ are S-modules, with the product defined by multiplying the left factor. Thus γ is an S-module homomorphism. Moreover, γ^* is clearly the dual homomorphism of γ. Hence, γ is an isomorphism if and only if γ^* is an isomorphism ([Bo] II §2.1).

   Finally, one can check that η and β are ismorphisms. Then by the commutativity of the diagram, j is an isomorphism if and only if γ^* is an isomorphism. Therefore, by the previous reasoning, we conclude that j is an isomorphism if and only if γ is an isomorphism.

□

2.3 Hopf algebras

In this section, we introduce the notion of Hopf algebra, which are bialgebras with an additional map called coinverse. Moreover we state that coinverse is an algebra and a coalgebra anti-homomorphism. Next we set the main result about duality. And finally we do the scalar extension of a Hopf algebra.

Definition 2.3.1. A K-**Hopf algebra** is a K-bialgebra $H = (H, m_H, \lambda_H, \Delta_H, \varepsilon_H)$ together with a K-linear map $\sigma_H : H \to H$ such that the diagram commutes:

$$\begin{tikzcd}
 & H \otimes H \arrow[rr, "I_H \otimes \sigma_H"] & & H \otimes H \arrow[dr, "m_H"] & \\
H \arrow[ur, "\Delta_H"] \arrow[rr, "\varepsilon_H"] \arrow[dr, "\Delta_H"'] & & K \arrow[rr, "\lambda_H"] & & H \\
 & H \otimes H \arrow[rr, "\sigma_H \otimes I_H"] & & H \otimes H \arrow[ur, "m_H"'] &
\end{tikzcd}$$

The map σ_H is called the **coinverse** or **antipode**.

A K-Hopf algebra H is **commutative** if it is a commutative algebra and is **cocommutative** if it is a cocommutative coalgebra.

Example 2.3.2. The field K is a commutative and cocommutative K-Hopf algebra, called **trivial Hopf algebra**, with coinverse map the identity map on K.

Example 2.3.3. Let G be a finite group. From Example 2.2.4, $K[G]$ has the structure of a cocommutative bialgebra. Moreover it is a cocommutative K-Hopf algebra, called the **group Hopf algebra**, with coinverse map:

$$\begin{array}{rcccc} \sigma_{K[G]} & : & K[G] & \to & K[G] \\ & & g & \to & g^{-1} \end{array}$$

It is commutative if, and only if, G is abelian.

Example 2.3.4. Let $K[x]$ be the polynomial bialgebra with x primitive (Example 2.2.5), which is commutative and cocommutative. Moreover, $K[x]$ is a commutative and cocommutative K-Hopf algebra, called the **polynomial Hopf algebra**, with coinverse map:

$$\begin{array}{rcccc} \sigma_{K[x]} & : & K[x] & \to & K[x] \\ & & x^i & \to & (-x)^i \end{array}$$

Remark 2.3.5. The polynomial bialgebra with x grouplike (Example 2.2.5) can not be endowed with the structure of a K-Hopf algebra.

In many ways, the group ring $K[G]$ of Example 2.3.3 is the canonical example that is generalized to the concept of Hopf algebra.

Proposition 2.3.6. *Let H be a K-Hopf algebra with coinverse map σ_H. Then the coinverse is an algebra and a coalgebra antihomomorphism, that is to say:*

1. $m_H(\sigma_H \otimes \sigma_H)\tau = \sigma_H m_H$, *so that* $\sigma_H(ab) = \sigma_H(b)\sigma_H(a)$, *for all* $a, b \in H$;

2. $\sigma_H \lambda_H = \lambda_H$, *so that* $\sigma_H(1_H) = 1_H$;

3. $\tau(\sigma_H \otimes \sigma_H)\Delta_H = \Delta_H \sigma_H$;

4. $\varepsilon_H \sigma_H = \varepsilon_H$.

Corollary 2.3.7. *Let H be a K-Hopf algebra with coinverse map σ_H. If H is either commutative or cocommutative, then σ_H has order 2 (ie, $\sigma_H^2 = I_H$).*

Definition 2.3.8. Let H, H' be K-Hopf algebras. Since H and H' are bialgebras, $H \otimes H'$ is a bialgebra (Definition 2.2.6). Therefore, the **tensor product of Hopf algebras** $H \otimes H'$ has the structure of a K-Hopf algebra with coinverse map defined as

$$\begin{array}{rrcl} \sigma_{H\otimes H'}: & H \otimes H' & \to & H \otimes H' \\ & a \otimes b & \mapsto & (\sigma_H \otimes \sigma_{H'})(a \otimes b) = \sigma_H(a) \otimes \sigma_{H'}(b) \end{array}$$

Definition 2.3.9. Let H and H' be K-Hopf algebras with coinverse maps σ_H and $\sigma_{H'}$ (resp.). A **K-Hopf algebra homomorphism** from H to H' is a K-linear map $\phi : H \to H'$ that is a K-bialgebra homomorphism and verifies $\phi \circ \sigma_H = \sigma_{H'} \circ \phi$. A K-Hopf algebra homomorphism that is injective and surjective is a **K-Hopf algebra isomorphism**.

Theorem 2.3.10. *Let H be a finite dimensional K-vector space. Then H is a K-Hopf algebra if, and only if, H^* is a K-Hopf algebra.*

Remark 2.3.11. Let H be a K-Hopf algebra. As stated in Remark, page 11 [Ch1], a K-linear map $f : H \to K$ is a K-algebra homomorphism if and only if $f \in H^* = \mathrm{Hom}_K(H, K)$ is grouplike.

Proposition 2.3.12. *Let H be a K-Hopf algebra. The set of grouplike elements of H is a subgroup of the multiplicative group of the units of H.*

Proof. It may be found in Proposition 1.6 [Ch1]. □

Now, we do the scalar extension of a Hopf algebra, which will be useful later on.

Remark 2.3.13. Let $L|K$ be a field extension and let V be a vector space over K. Since L is a K-vector space too, $V \otimes_K L$ is clearly a K-vector space. Moreover, $V \otimes_K L$ is an L-vector space with scalar multiplication defined as $\lambda(v \otimes_K r) = v \otimes_K \lambda r$, for all $\lambda \in L$, $v \otimes_K r \in V \otimes_K L$. Therefore, if $f : V_1 \to V_2$ is a K-linear map, then $f \otimes I_L : V_1 \otimes_K L \to V_2 \otimes_K L$ is an L-linear map.

Proposition 2.3.14. *Let H be a K-Hopf algebra and let L be a field extension of K. Then the scalar extension $L \otimes_K H$ of H is an L-Hopf algebra.*

We close this section with an example: the dual Hopf algebra of the group ring.

Proposition 2.3.15. *Let G be a finite group. There exists a K-Hopf algebra isomorphism between $K[G]^*$ and $\mathcal{O}(G) \coloneqq K^G = \{f : G \to K\}$.*

Proof. Sketch of the proof. We start considering $\mathcal{O}(G)$ with basis $\{e_g : g \in G\}$, where $e_g(h) \coloneqq \delta_{g,h}$. Recall that $\mathcal{O}(G)$ is a K-vector space with operations defined from those of K. The structure maps of $\mathcal{O}(G)$ as a Hopf algebra are defined as:

1. $m_{\mathcal{O}(G)} : \mathcal{O}(G) \otimes \mathcal{O}(G) \to \mathcal{O}(G)$, $m_{\mathcal{O}(G)}(e_g \otimes e_h) = \delta_{g,h} e_g$;
2. $\lambda_{\mathcal{O}(G)} : K \to \mathcal{O}(G)$, $\lambda_{\mathcal{O}(G)}(r) = \sum\limits_{g \in G} r e_g$;
3. $\Delta_{\mathcal{O}(G)} : \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$, $\Delta_{\mathcal{O}(G)}(e_g) = \sum\limits_{uv=g} e_u \otimes e_v$;
4. $\varepsilon_{\mathcal{O}(G)} : \mathcal{O}(G) \to K \cong K^*$, $\varepsilon_{\mathcal{O}(G)}(e_g) = \delta_{g,1_G}$;
5. $\sigma_{\mathcal{O}(G)} : \mathcal{O}(G) \to \mathcal{O}(G)$, $\sigma_{\mathcal{O}(G)}(e_g) = e_{g^{-1}}$.

Now we consider the K-Hopf algebra $K[G]$ (Example 2.3.3). Its canonical basis is $\mathcal{B} = \{g : g \in G\}$. We consider its linear dual $K[G]^* = \mathrm{Hom}_K(K[G], K)$. The dual basis of $\mathcal{B}$ is $\{\omega^g : \omega^g(h) = \delta_{g,h}$, for $g \in G\}$. The map sending e_g to ω^g is a K-vector space isomorphism from $\mathcal{O}(G)$ onto $K[G]^*$. Hence, it remains to show that:

$$\begin{aligned} m^*_{K[G]}(\omega^g) &= \Delta_{\mathcal{O}(G)}(e_g) & \lambda^*_{K[G]}(\omega^g) &= \varepsilon_{\mathcal{O}(G)}(e_g) \\ \Delta^*_{K[G]}(\omega^g \otimes \omega^h) &= m_{\mathcal{O}(G)}(e_g \otimes e_h) & \varepsilon^*_{K[G]} &= \lambda_{\mathcal{O}(G)} \\ \sigma^*_{K[G]}(\omega^g) &= \sigma_{\mathcal{O}(G)}(e_g) & & \end{aligned}$$

□

2.4 Hopf Galois structures

In this section, we see how we move from Galois theory to Hopf Galois theory, whose fathers are Chase and Sweedler [Ch-Sw]. There are two results that leads us to define Hopf Galois structures and to give the fundamental theorem of Hopf Galois theory. Finally we highlight important facts about Hopf Galois structures.

Let L be a finite field extension of K. Let $\mathrm{Aut}_K L$ denote the group of field automorphisms of L that fix K elementwise and let G be a subgroup of $\mathrm{Aut}_K L$. Recall that $K[G]$ is a K-Hopf algebra (Example 2.3.3).

Observe L is a left $K[G]$-module with scalar multiplication given by

$$\left(\sum_{g\in G} a_g g\right)\cdot x = \sum_{g\in G} a_g g(x), \text{ for all } a_g \in K,\ x \in L.$$

Proposition 2.4.1. *Let $L|K$ be a finite extension and let G be a subgroup of $Aut_K L$. Then L is a left $K[G]$-module algebra.*

Proposition 2.4.2. *Let $L|K$ be a finite extension and let G be a subgroup of $Aut_K L$. The following K-linear map is a bijection if and only if L is Galois with group G:*

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

The previous results motivate the notion of Hopf Galois structure by replacing $K[G]$ by any K-Hopf algebra.

Definition 2.4.3. Let $L|K$ be a finite field extension. A **Hopf Galois structure on L|K** is a pair $(H,\cdot)$, where H is a finite cocommutative K-Hopf algebra and $\cdot$ is an action called **Hopf action**, such that the following two conditions are satisfied:

1. L is a left H-module K-algebra,
2. $j : L\otimes_K H \to \mathrm{End}_K L$, $j(x\otimes h)(y) = x(h\cdot y)$, is a K-linear isomorphism.

In this case, we say that $L|K$ is $(H,\cdot)$-Galois, or just H-Galois. Moreover, we say that a finite field extension is a **Hopf Galois extension** if it admits some Hopf Galois structure.

Remark 2.4.4. If $L|K$ is a Hopf Galois extension of degree n, then the K-Hopf algebra H has dimension n: indeed, since j is an isomorphism,

$$\dim_K(L\otimes_K H) = \dim_K(\mathrm{End}_K L) \Rightarrow n\ \dim_K H = n^2 \Rightarrow \dim_K H = n.$$

Remark 2.4.5. Proposition 2.2.18 gives an equivalence definition of Hopf Galois structure.

Definition 2.4.6. We say that two **Hopf Galois structures** are **isomorphic** if the algebras are isomorphic and this isomorphism is compatible with both actions.

The **fundamental theorem of Hopf Galois theory** (see Th 5.1 [Ch-Sw]) in its general form says:

Theorem 2.4.7 (Chase-Sweedler)**.** *Let $(H,\cdot)$ be a Hopf Galois structure on the field extension $L|K$. For a sub-K-Hopf algebra H' of H, we define*

$$L^{H'} := \{x\in L :\ h\cdot x = \varepsilon_H(h)x,\ \forall\ h\in H'\}.$$

Then $L^{H'}$ is a subfield of L containing K, and the map

$$\begin{array}{rcrcl} \mathcal{F}_H & : & \{H' \subseteq H \text{ sub-Hopf algebra}\} & \to & \{E \text{ field } : K \subseteq E \subseteq L\} \\ & & H' & \mapsto & L^{H'} \end{array}$$

is injective and inclusion-reversing.

Observe the fundamental theorem of Galois theory is stronger than this one since it gives a bijective correspondence, whereas the Hopf Galois theorem just gives an injection.

In order to close this section, let us notice some important facts. First of all, Hopf Galois theory is indeed a generalization of classical Galois theory: every Galois extension $L|K$ with Galois group G is Hopf Galois because $K[G]$ together with the following action is a Hopf Galois structure on $L|K$:

$$\underbrace{\left(\sum \lambda_g g\right)}_{\in K[G]} \cdot \underbrace{x}_{\in L} = \sum \lambda_g g(x)$$

But the reciprocal is not true: there are Hopf Galois extensions which are not Galois. For instance: every separable extension of degree 3 or 4 is Hopf Galois.

Finally, whereas a Galois extension determines the Galois group (it is unique), a Hopf Galois extension may have several Hopf Galois structures which are not isomorphic. That is why it is interesting to count them. Unfortunately, the explicit computation of Hopf Galois structures is, in general, very hard. But in the separable case there is a characterization of Hopf Galois structures in terms of groups that allows us to use Magma in order to compute them and determine two important properties of those. We will carefully develop this in the next chapter.

Chapter 3

Greither-Pareigis' theorem

From this chapter on, we will restrict to the case of a separable finite field extension, since under this assumption, there is a characterization of the Hopf Galois character in terms of groups. The fathers of this so-called separable Hopf Galois theory are Greither and Pareigis [G-P]. The proofs of all the results presented here have been enlarged with all details.

3.1 Review on group theory

Let G be a group.

Definition 3.1.1. A subgroup H of G is **normal** in G if for every $g \in G$, $gH = Hg$.

Definition 3.1.2. Let $S \subseteq G$ be a subset. We define the following subgroups of G:

- The **normalizer** of S in G as

$$\mathrm{Norm}_G(S) = \{g \in G : gS = Sg\}.$$

- The **centralizer** of S in G as

$$\mathrm{Cent}_G(S) = \{g \in G : gs = sg,\ \forall\ s \in S\}.$$

Definition 3.1.3. Let H and N be subgroups of G. We say that N is **normalized by** H (or that H **normalizes** N) if for every $h \in H$ and $n \in N$, $hnh^{-1} \in N$.

Remark 3.1.4. Equivalently, N is normalized by H if $H \subseteq \mathrm{Norm}_G(N)$.

Definition 3.1.5. Let S be G-set. We define the **stabilizer** of an element $s \in S$ in G as

$$\mathrm{Stab}_G(s) = \{g \in G : g \cdot s = s\}.$$

Definition 3.1.6. A subgroup N of S_n is **transitive** if the action of N on $\{1, \dots, n\}$ is transitive, that is, for every $i, j \in \{1, \dots, n\}$, there exists $m \in N$ such that $m(i) = j$. N is also called **transitive group of degree** n.

Definition 3.1.7. Let X be a finite set. For a subgroup N of $\mathrm{Perm}(X)$ any two of the following conditions imply the third one:

- $|N| = |X|$,
- N is transitive,
- For every $x \in X$, $\mathrm{Stab}_N(x)$ is trivial.

We say N is **regular** if it satisfies any two of the previous conditions.

Remark 3.1.8. Equivalently, N is regular if it is transitive and the m of Definition 3.1.6 is unique.

Thus we have the following characterizaion of regular subgroups.

Proposition 3.1.9. *A subgroup N of $\mathrm{Perm}(X)$ is regular if and only if there exists $x \in X$ (hence for all $x \in X$) such that the following map is bijective:*

$$\begin{array}{ccc} N & \to & X \\ \eta & \mapsto & \eta(x) \end{array}$$

3.2 Framework

Let $L|K$ be a finite separable field extension of degree g and let $\widetilde{L}$ be its normal closure. Let $G = \mathrm{Gal}(\widetilde{L}|K) = \mathrm{Aut}_K\widetilde{L}$ and $G' = \mathrm{Gal}(\widetilde{L}|L)$. By the primitive element theorem, there exists $\alpha \in L$ such that $L = K(\alpha)$. Let $f = \mathrm{irr}(\alpha, K)$ (it has degree g) and denote $\{\alpha \coloneqq \alpha_1, \dots, \alpha_g\}$ its roots, so that $\widetilde{L} = K(\alpha_1, \dots, \alpha_g)$.

$$\begin{tikzcd}
\widetilde{L} = K(\alpha_1, \dots, \alpha_g) \arrow[d, dash, "G'"] \arrow[dd, dash, bend right=60, "G"'] \\
L = K(\alpha) \arrow[d, dash, "g"'] \\
K
\end{tikzcd}$$

$\widetilde{L}$ normal closure of $L|K$

$G = \mathrm{Gal}(\widetilde{L}|K),\ G' = \mathrm{Gal}(\widetilde{L}|L)$

G/G' left cosets, $|G/G'| = g$

It is easy to check that the action of G on G/G' is equivalent to the Galois action of G on $\{\alpha_1, \dots, \alpha_g\}$. Therefore, since the Galois action is transitive and faithful, G is embedded into S_g as a transitive group via the following injective group homomorphism:

$$\begin{array}{cccc} \lambda_G & : & G & \hookrightarrow & \mathrm{S}_g \cong \mathrm{Perm}(G/G') \\ & & \sigma & \mapsto & [\overline{\tau} \mapsto \overline{\sigma\tau}] \end{array}$$

Hence we can identify G with its image by λ_G. Notice that changing $\lambda_G(G)$ by a conjugated subgroup in S_g is equivalent to renumerate the roots $\{\alpha_1, \dots, \alpha_g\}$. Thus $\lambda_G(G)$ is determined modulo conjugation.

Notice that λ is a left action, but we can also consider the right one, which is an injective group homomorphism as well:

$$\begin{array}{rcccl} \lambda_G & : & G & \hookrightarrow & \mathrm{Perm}(G/G') \\ & & \sigma & \mapsto & \sigma\,\cdot \end{array} \qquad \begin{array}{rcccl} \rho_G & : & G & \hookrightarrow & \mathrm{Perm}(G/G') \\ & & \sigma & \mapsto & \cdot\,\sigma^{-1} \end{array}$$

3.3 Galois descent

Now we consider objects over a field K. The theory of forms states when they become isomorphic by scalar extension to a field E. Afterwards we study the inverse problem: when an E-morphism descends to K.

The first part of this section is a summary of Section 5.1 of my graduate thesis [Sa] and it is based on [Se]. We introduce 1-cocycles, which lead us to define the first cohomology set for the nonabelian case. Then we classify algebra forms.

Let A, G be groups such that A is a left G-module.

Definition 3.3.1. A **1-cocycle of G into A** is a map $p : G \to A$, $\sigma \mapsto p_\sigma$, such that

$$p_{\sigma\tau} = p_\sigma(\sigma p_\tau).$$

Let $C^1(G, A)$ denote the set of 1-cocycles of G into A.

Remark 3.3.2. If the G-action on A is trivial, a 1-cocycle of G into A is a group morphism.

Definition 3.3.3. The **first cohomology set of G with values in A**, $H^1(G, A)$, is defined as the quotient of $C^1(G, A)$ by the equivalence relation $\sim$ defined as

$$p \sim q \Leftrightarrow \text{there exists } a \in A \text{ such that } q_\sigma = a^{-1}\, p_\sigma\, \sigma(a).$$

Now let $E|K$ be a finite Galois extension with group G and let H be a K algebra. Recall that G acts on $E \otimes H$ via the left factor. If $\sigma \in G$, then we also denote by σ the K-algebra automorphism:

$$\begin{array}{rcl} E \otimes H & \to & E \otimes H \\ \lambda \otimes h & \mapsto & \sigma(\lambda) \otimes h \end{array}$$

Moreover, if H_1, H_2 are K-algebras and $f : E \otimes H_1 \to E \otimes H_2$ is an E-algebra morphism, we denote by f^σ the E-algebra morphism $\sigma \circ f \circ \sigma^{-1}$, that is, the morphism making commutative the following diagram:

$$\begin{tikzcd}
E \otimes H_1 \arrow[r, "f"] \arrow[d, "\sigma"'] & E \otimes H_2 \arrow[d, "\sigma"] \\
E \otimes H_1 \arrow[r, "f^\sigma"'] & E \otimes H_2
\end{tikzcd}$$

Definition 3.3.4. We say that a K algebra H' is an $E|K$**-form of** H if there is an E-linear isomorphism $E \otimes H \cong E \otimes H'$.

Let $S_H(E|K)$ denote the set of K-isomorphism classes of forms of H.

Theorem 3.3.5. *The set $S_H(E|K)$ of $E|K$-forms of algebras is in bijection with the set $H^1(G, \mathrm{Aut}_E(E \otimes H))$ of 1-cocycles from G into $\mathrm{Aut}_E(E \otimes H)$.*

Remark 3.3.6. If H' is an $E|K$-form of H, $\phi : E \otimes H' \tilde{\to} E \otimes H$, the above bijection sends H' to the class of the 1-cocycle given by

$$\sigma \longmapsto p_\sigma := \phi \circ \sigma \circ \phi^{-1} \circ \sigma^{-1} = \phi \circ \phi^{-\sigma}$$

From now on, we consider the Galois descent problem. It is based on [G-P].

Definition 3.3.7. Let A_i, B_i be K-algebras such that B_i is an $E|K$-form of A_i, $\phi_i : E \otimes B_i \tilde{\to} E \otimes A_i$, for every $i \in \{1, 2\}$. An E-algebra morphism $f : E \otimes A_1 \to E \otimes A_2$ is called **descendable** if there exists a (unique) morphism $g : B_1 \to B_2$ so that the following diagram commutes:

$$\begin{tikzcd}
E \otimes B_1 \arrow[r, "\mathrm{I}_E \otimes g"] \arrow[d, "\phi_1"'] & E \otimes B_2 \arrow[d, "\phi_2"] \\
E \otimes A_1 \arrow[r, "f"'] & E \otimes A_2
\end{tikzcd}$$

that is, for every $\lambda \in E$, $b \in B_1$,

$$f(\phi_1(\lambda \otimes b)) = \phi_2(\lambda \otimes g(b)).$$

Lemma 3.3.8. *In the previous notation, let $p^{(i)}$ be the associated cocycles to B_i. Then f is descendable if and only if*

$$f \circ p_\sigma^{(1)} = p_\sigma^{(2)} \circ f^\sigma, \quad \forall\ \sigma \in G.$$

Proof. The proof is omitted in [G-P]. Assume f is descendable and let us check that $f \circ p_\sigma^{(1)} = p_\sigma^{(2)} \circ f$, for every $\sigma \in G$. Since f is descendable, by definition, there exists a morphism $g : B_1 \to B_2$ such that

$$f \circ \phi_1 = \phi_2 \circ (\mathrm{I}_E \otimes g)$$

that is,

$$\phi_2^{-1} \circ f \circ \phi_1 = \mathrm{I}_E \otimes g \tag{3.1}$$

Moreover, since G acts via the left factor, we have that for every $\sigma \in G$,

$$(\mathrm{I}_E \otimes g) \circ \sigma = \sigma \circ (\mathrm{I}_E \otimes g) \tag{3.2}$$

Indeed, for every $\lambda \otimes b \in E \otimes B_1$,

- On the one hand,

$$(\mathrm{I}_E \otimes g)(\sigma(\lambda \otimes b)) = (\mathrm{I}_E \otimes g)(\sigma(\lambda) \otimes b) = \sigma(\lambda) \otimes g(b)$$

- On the other hand,

$$\sigma((\mathrm{I}_E \otimes g)(\lambda \otimes b)) = \sigma(\lambda \otimes g(b)) = \sigma(\lambda) \otimes g(b)$$

Now if we combine both identities (3.1) and (3.2), we obtain for every $\sigma \in G$:

$$\phi_2^{-1} \circ f \circ \phi_1 \circ \sigma = \sigma \circ \phi_2^{-1} \circ f \circ \phi_1 \tag{3.3}$$

which is equivalent to the following:

$$\begin{aligned} & \phi_2^{-1} \circ f \circ \phi_1 \circ \sigma = \sigma \circ \phi_2^{-1} \circ f \circ \phi_1 \\ \Leftrightarrow \quad & f \circ \phi_1 \circ \sigma = \phi_2 \circ \sigma \circ \phi_2^{-1} \circ f \circ \phi_1 \\ \Leftrightarrow \quad & f \circ \phi_1 \circ \sigma \circ \phi_1^{-1} = \phi_2 \circ \sigma \circ \phi_2^{-1} \circ f \\ \Leftrightarrow \quad & f \circ (\phi_1 \circ \sigma \circ \phi_1^{-1} \circ \sigma^{-1}) = (\phi_2 \circ \sigma \circ \phi_2^{-1} \circ \sigma^{-1}) \circ (\sigma \circ f \circ \sigma^{-1}) \\ \Leftrightarrow \quad & f \circ p_\sigma^{(1)} = p_\sigma^{(2)} \circ f^\sigma \end{aligned}$$

Reciprocally, assume $f \circ p_\sigma^{(1)} = p_\sigma^{(2)} \circ f^\sigma$ holds for every $\sigma \in G$, and let us see that f is descendable. By the last computation, the assumption is equivalent to (3.3). Now let us define

$$\tilde{g} : E \otimes B_1 \to E \otimes B_2$$

as

$$\tilde{g} = \phi_2^{-1} \circ f \circ \phi_1.$$

Hence by (3.3) $\tilde{g}$ satisfies the following identity for every $\sigma \in G$:

$$\tilde{g} \circ \sigma = \sigma \circ \tilde{g} \tag{3.4}$$

Thus $\tilde{g}$ maps G-invariant elements to G-invariant elements: if x is G-invariant (ie, $\sigma(x) = x, \ \forall \ \sigma \in G$), then $\tilde{g}(x)$ is also G-invariant: for every $\sigma \in G$,

$$\sigma(\tilde{g}(x)) \underset{(3.4)}{=} \tilde{g}(\sigma(x)) \underset{(x \ G\text{-inv})}{=} \tilde{g}(x)$$

Finally, since $G = \mathrm{Aut}_K(E)$, the G-invariant elements in $E \otimes B_i$ are those of $K \otimes B_i \cong B_i$, hence $\tilde{g}$ restricts to a $g : B_1 \to B_2$ such that $\tilde{g} = \mathrm{I}_E \otimes g$, that is, f is descendable. □

3.4 Some auxiliary G-algebras

In this section, we state some previous results that are necessary to prove Greither-Pareigis' theorem. It is based on chapter 2, section 6 [Ch1] and the proofs of the results presented here have been enlarged with all details.

We start generalizing the notion of Hopf Galois structure to rings.

Definition 3.4.1. Let E be a field and S be a finite E-algebra. A **Hopf Galois structure on S|E** is a pair $(H,\cdot)$, where H is a finite cocommutative E-Hopf algebra and $\cdot$ is an action called **Hopf action**, such that the two conditions of the Definition 2.4.3 are satisfied.

Now assume we are under the assumptions of Section 3.2. We see that if we have a Hopf Galois structure $(H,\cdot)$ on $L|K$, then by tensoring with $\widetilde{L}$ over K we obtain another Hopf Galois structure.

Proposition 3.4.2 (Base change)**.** *If $(H,\cdot)$ is a Hopf Galois structure on a finite field extension $L|K$, then $(\widetilde{L}\otimes H,\ast)$ is a Hopf Galois structure on $(\widetilde{L}\otimes L)|\widetilde{L}$, where the action $\ast$ is defined as follows:*

$$\begin{array}{rccl} \ast & : & (\widetilde{L}\otimes H)\otimes_{\widetilde{L}}(\widetilde{L}\otimes L) & \to & \widetilde{L}\otimes L \\ & & (\tilde{s}\otimes h)\otimes(\tilde{t}\otimes x) & \mapsto & (\tilde{s}\tilde{t})\otimes(h\cdot x) \end{array}$$

Proof. Sketch of the proof, which is omitted in [Ch1]. Recall that, by Proposition 2.3.14, $\widetilde{L}\otimes H$ is an $\widetilde{L}$-Hopf algebra. One may check three things:

1. $\widetilde{L}\otimes L$ is a finite $\widetilde{L}$-vector space: if one takes a K-basis $\{e_1,\dots,e_g\}$ of L, then $\{1_{\widetilde{L}}\otimes e_1,\dots,1_{\widetilde{L}}\otimes e_g\}$ is an $\widetilde{L}$-basis of $\widetilde{L}\otimes L$.
2. By tensoring with $\widetilde{L}$ the commutative diagrams giving that L is a left H-module K-algebra (see Definition 2.2.9) we obtain the commutative diagrams giving that $\widetilde{L}\otimes L$ is a left $\widetilde{L}\otimes H$-module $\widetilde{L}$-algebra.
3. $\tilde{j}:(\widetilde{L}\otimes L)\otimes_{\widetilde{L}}(\widetilde{L}\otimes H)\to\mathrm{End}_{\widetilde{L}}(\widetilde{L}\otimes L)$ is an $\widetilde{L}$-linear isomorphism.

   Since $L|K$ is H-Galois by assumption, we have the K-linear isomorphism:

   $$\begin{array}{rccl} j & : & L\otimes H & \to & \mathrm{End}_K(L) \\ & & x\otimes h & \mapsto & j(x\otimes h)(y)=x(h\cdot y) \end{array}$$

   By tensoring with $\widetilde{L}$, we obtain the following $\widetilde{L}$-linear isomorphism (see [Bo] II §3.6):

   $$\widetilde{L}\otimes L\otimes H \xrightarrow{\widetilde{L}\otimes j} \widetilde{L}\otimes\mathrm{End}_K(L).$$

   Now it remains to show that $\widetilde{L}\otimes j=\tilde{j}$, that is:

   $$\widetilde{L}\otimes L\otimes H\cong(\widetilde{L}\otimes L)\otimes_{\widetilde{L}}(\widetilde{L}\otimes H) \qquad\text{and}\qquad \widetilde{L}\otimes\mathrm{End}_K(L)\cong\mathrm{End}_{\widetilde{L}}(\widetilde{L}\otimes L).$$

The first one is clear. Let us check $\widetilde{L} \otimes \mathrm{End}_K(L) \cong \mathrm{End}_{\widetilde{L}}(\widetilde{L} \otimes L)$. As noticed before, if $\{e_1, \dots, e_g\}$ is a K-basis of L, then $\{1_{\widetilde{L}} \otimes e_1, \dots, 1_{\widetilde{L}} \otimes e_g\}$ is an $\widetilde{L}$-basis of $\widetilde{L} \otimes L$. Moreover, a K-basis of $\mathrm{End}_K(L)$ is $\{\varphi_{ij} : i, j \in \{1, \dots, g\}\}$, where:

$$\begin{array}{rccll} \varphi_{ij} & : & L & \longrightarrow & L \\ & & e_i & \longmapsto & e_j \\ & & e_k & \longmapsto & 0 \quad \text{if } k \neq i \end{array}$$

Similarly we define an $\widetilde{L}$-basis $\{\psi_{ij} : i, j \in \{1, \dots, g\}\}$ of $\mathrm{End}_{\widetilde{L}}(\widetilde{L} \otimes L)$, so that there is the following isomorphism:

$$\begin{array}{rcl} \widetilde{L} \otimes \mathrm{End}_K(L) & \to & \mathrm{End}_{\widetilde{L}}(\widetilde{L} \otimes L) \\ 1_{\widetilde{L}} \otimes \varphi_{ij} & \mapsto & \psi_{ij} \end{array}$$

□

Remark 3.4.3. One can recover the action of H on L by identifying H and L with the fixed rings $(\widetilde{L} \otimes H)^G$ and $(\widetilde{L} \otimes L)^G$ resp., where G acts via its action on $\widetilde{L}$:

- H identifies with the K-Hopf subalgebra $(\widetilde{L} \otimes H)^G$ (of $\widetilde{L} \otimes H$):

$$(\widetilde{L} \otimes H)^G = \widetilde{L}^G \otimes H = K \otimes_K H \cong H.$$

- L identifies with the K-subalgebra $(\widetilde{L} \otimes L)^G$ (of $\widetilde{L} \otimes L$):

$$(\widetilde{L} \otimes L)^G = \widetilde{L}^G \otimes L = K \otimes_K L \cong L.$$

Moreover, if $*$ is a Hopf action of $\widetilde{L} \otimes H$ on $\widetilde{L} \otimes L$, then $\cdot$ is a Hopf action of H on L.

This proposition leads to Greither-Pareigis' classification of Hopf Galois structures on $L|K$: the strategy is to classify those Hopf Galois structures on $(\widetilde{L} \otimes L)|\widetilde{L}$ fixing $\widetilde{L}$ on which G acts, and then take the ring of invariants under the G-action. This strategy is facilitated by the special form of $\widetilde{L} \otimes L$, and hence $\widetilde{L} \otimes H$, which permits a complete description of Galois structures on $(\widetilde{L} \otimes L)|\widetilde{L}$.

Proposition 3.4.4. *The map*

$$\begin{array}{rccl} \gamma & : & \widetilde{L} \otimes L & \to & \mathrm{Map}(G/G', \widetilde{L}) \\ & & \tilde{l} \otimes l & \mapsto & \gamma(\tilde{l} \otimes l)(\bar{\sigma}) = \tilde{l}\sigma(l) \end{array}$$

is a $\widetilde{L}$-algebra, G-module isomorphism, where G acts on $\mathrm{Map}(G/G', \widetilde{L})$ as follows:

$$\begin{array}{rcl} G \times \mathrm{Map}(G/G', \widetilde{L}) & \to & \mathrm{Map}(G/G', \widetilde{L}) \\ (\tau, f) & \mapsto & (\tau \cdot f)(\bar{\sigma}) = \tau(f(\overline{\tau^{-1}\sigma})) \end{array}$$

and G and $\widetilde{L}$ act on $\widetilde{L} \otimes L$ via the left factor.

Proof. It is based on the proof given in Lemma 1.2 [G-P]. Set $M := \mathrm{Map}(G/G', \widetilde{L})$.

Claim 1: $\phi : \widetilde{L} \otimes L \to \mathrm{Map}(G/G', \widetilde{L})$, defined as follows, is a K-linear isomorphism.

We have the following K-linear isomorphisms:

$$\begin{array}{rcll}
\widetilde{L} \otimes L & = & \widetilde{L} \otimes K(\alpha) & \text{(Primitive Element Th)} \\
\lambda \otimes s & \mapsto & \lambda \otimes P(\alpha) & \text{(for some } P \in K[x]) \\
 & \cong & \widetilde{L} \otimes \dfrac{K[x]}{\big(\mathrm{irr}(\alpha, K)\big)} & \text{(Isomorphism Th)} \\
 & \mapsto & \lambda \otimes \overline{P(x)} & \\
 & \cong & \dfrac{\widetilde{L}[x]}{\big(\mathrm{irr}(\alpha, K)\big)} & \text{(by (1) below)} \\
 & \mapsto & \overline{\lambda P(x)} & \\
 & = & \dfrac{\widetilde{L}[x]}{\left(\prod_{i=1}^{g} (x - \alpha_i)\right)} & \left(\begin{array}{c} \widetilde{L} \text{ normal closure of} \\ L|K, \text{ hence } \mathrm{irr}(\alpha, K) \\ \text{splits completely} \end{array}\right) \\
 & \mapsto & \overline{\lambda P(x)} & \\
 & \cong & \prod_{i=1}^{g} \dfrac{\widetilde{L}[x]}{(x - \alpha_i)} & \left(\begin{array}{c} \text{Chinese Remainder Th} \\ L|K \text{ separable, thus} \\ (x - \alpha_i) \text{ pairwise prime} \end{array}\right) \\
 & \mapsto & (\lambda P(x) \bmod (x - \alpha_i))_{i=1}^{g} & \\
 & \cong & \prod_{i=1}^{g} \widetilde{L} & \text{(by (2) below)} \\
 & \mapsto & \big(\lambda \sigma(P(\alpha))\big)_{\overline{\sigma} \in G/G'} & \\
 & \cong & \mathrm{Map}(G/G', \widetilde{L}) & \text{(Example 2.1.6)} \\
 & \mapsto & \sum_{\overline{\sigma} \in G/G'} \lambda \sigma(P(\alpha)) e_{\overline{\sigma}} & \left(\begin{array}{c} \{e_{\overline{\sigma}}\}_{\overline{\sigma} \in G/G'} \ \widetilde{L}\text{-basis} \\ \text{of } \mathrm{Map}(G/G', \widetilde{L}) \end{array}\right)
\end{array}$$

where:

(1) On the one hand, by tensoring with $\widetilde{L}$ the projection $\pi : K[x] \twoheadrightarrow K[x]/(\mathrm{irr}(\alpha, K))$, we obtain another surjective morphism:

$$\begin{array}{rcl} \varphi := \mathrm{I}_{\widetilde{L}} \otimes \pi \quad : \quad \widetilde{L} \otimes K[x] & \twoheadrightarrow & \widetilde{L} \otimes \dfrac{K[x]}{\big(\mathrm{irr}(\alpha, K)\big)} \\ \lambda \otimes P & \mapsto & \lambda \otimes \pi(P) \end{array}$$

where $\mathrm{Ker}(\varphi) = (\mathrm{irr}(\alpha, K))$.

On the other hand, we have the following K-linear isomorphism:

$$\begin{array}{rrcl} f \quad : & \widetilde{L}[x] & \to & \widetilde{L} \otimes K[x] \\ & x^j & \mapsto & 1_{\widetilde{L}} \otimes x^j \\ & \sum_j \lambda_j x^j & \mapsto & \sum_j \lambda_j (1_{\widetilde{L}} \otimes x^j) = \sum_j \lambda_j \otimes x^j \end{array}$$

Therefore, $\overline{\varphi} := \varphi \circ f : \widetilde{L}[x] \to \widetilde{L} \otimes K[x]/(\mathrm{irr}(\alpha, K))$ is surjective since f is an isomorphism and $\mathrm{Ker}(\overline{\varphi}) \cong \mathrm{Ker}(\varphi)$, thus we apply the Isomorphism theorem;

(2) For every $i \in \{1, \dots, g\}$, the morphism $f_i : \widetilde{L}[x] \to \widetilde{L}$, defined by $f_i(P) = P(\alpha_i)$, is surjective (given $\beta \in \widetilde{L}$, the constant polynomial $P(x) := \beta \in \widetilde{L}[x]$ satisfies $P(\alpha_i) = \beta$) and $\mathrm{Ker}(f_i) = (x - \alpha_i)$, so that we apply the Isom. theorem and get

$$\begin{array}{ccc} \dfrac{\widetilde{L}[x]}{(x - \alpha_i)} & \longrightarrow & \widetilde{L} \\ \overline{P} & \longmapsto & P(\alpha_i) \end{array}$$

so that:

$$\begin{array}{ccc} \prod_{i=1}^{g} \dfrac{\widetilde{L}[x]}{(x - \alpha_i)} & \longrightarrow & \prod_{i=1}^{g} \widetilde{L} \\ (P(x) \bmod (x - \alpha_i))_{i=1}^{g} & \longmapsto & (P(\alpha_i))_{i=1}^{g} \end{array}$$

Now it remains to check that

$$\big(P(\alpha_i)\big)_{i=1}^{g} = \big(\sigma(P(\alpha))\big)_{\overline{\sigma} \in G/G'}$$

Indeed, observe the Galois action induces a surjective map:

$$\begin{array}{rcl} G & \to & \{\text{roots of } \mathrm{irr}(\alpha, K)\} \\ \sigma & \mapsto & \sigma(\alpha) \end{array}$$

Moreover, for $\sigma, \tau \in G$, we have

$$\sigma(\alpha) = \tau(\alpha) \Leftrightarrow (\tau^{-1}\sigma)(\alpha) = \alpha \Leftrightarrow \tau^{-1}\sigma \in \mathrm{Aut}_{K(\alpha)}(\widetilde{L}) = G' \Leftrightarrow \sigma \in \tau G' = \overline{\tau}.$$

so that the previous map is bijective if we corestrict it to left cosets G/G':

$$\begin{array}{rcl} G/G' & \to & \{\text{roots of } \mathrm{irr}(\alpha, K)\} \\ \overline{\sigma} & \mapsto & \sigma(\alpha) \end{array}$$

Therefore, for every $P \in K[x]$ and $\sigma \in G = \mathrm{Aut}_K(L)$:

$$\big(P(\alpha_i)\big)_{i=1}^{g} = \big(P(\sigma(\alpha))\big)_{\overline{\sigma}\in G/G'} = \big(\sigma(P(\alpha))\big)_{\overline{\sigma}\in G/G'}$$

<u>Claim 2</u>: The previous K-linear isomorphism ϕ is precisely γ.

By definition of γ, for every $\overline{\tau} \in G/G'$, $\lambda \otimes P(\alpha) \in \widetilde{L} \otimes L$,

$$\gamma(\lambda \otimes P(\alpha))(\overline{\tau}) = \lambda\tau(P(\alpha))$$

so that it remains to check that, for every $\overline{\tau} \in G/G'$:

$$\Bigg(\sum_{\overline{\sigma}\in G/G'} \lambda\sigma(P(\alpha))e_{\overline{g}}\Bigg)(\overline{\tau}) = \lambda\tau(P(\alpha)).$$

Indeed, by $\widetilde{L}$-linearity and by definition of $\{e_{\overline{\sigma}}\}_{\overline{\sigma}\in G/G'}$,

$$\Bigg(\sum_{\overline{\sigma}\in G/G'} \lambda\sigma(P(\alpha))e_{\overline{g}}\Bigg)(\overline{\tau}) = \lambda \sum_{\overline{\sigma}\in G/G'} \sigma(P(\alpha))e_{\overline{g}}(\overline{\tau}) = \lambda\tau(P(\alpha)).$$

<u>Claim 3</u>: γ is an $\widetilde{L}$-algebra, G-module isomorphism.

Since we have proved that γ is a K-linear isomorphism, it remains to see that it is an $\widetilde{L}$-algebra, G-module homomorphism.

- $\widetilde{L}$-algebra homomorphism: γ is $\widetilde{L}$-linear by definition.

  Now let us check that γ preserves multiplication: indeed, for every $\overline{\sigma} \in G/G'$, $\tilde{l} \otimes l, \widetilde{m} \otimes m \in \widetilde{L} \otimes L$:

$$\begin{aligned}
\gamma\big((\tilde{l}\otimes l)(\widetilde{m}\otimes m)\big)(\overline{\sigma}) &= \gamma\big((\tilde{l}\widetilde{m})\otimes(lm)\big)(\overline{\sigma}) && \text{(Ex 2.1.7)}\\
&= \tilde{l}\widetilde{m}\ \sigma(lm) && \text{(def }\gamma\text{)}\\
&= \tilde{l}\widetilde{m}\ \sigma(l)\sigma(m) && (\sigma \in G = \mathrm{Aut}_K L)\\
&= (\tilde{l}\sigma(l))(\widetilde{m}\sigma(m)) && \text{(commut. of }\widetilde{L}\text{)}\\
&= \gamma(\tilde{l}\otimes l)(\overline{\sigma})\ \gamma(\widetilde{m}\otimes m)(\overline{\sigma}) && \text{(def }\gamma\text{)}\\
&= \big(\gamma(\tilde{l}\otimes l)\ \gamma(\widetilde{m}\otimes m)\big)(\overline{\sigma}) && \text{(def mult. in }M\text{)}
\end{aligned}$$

- G-module homomorphism: we have to check that the action is compatible with γ. Indeed, for every $\tau \in G$, $\tilde{l}\otimes l \in \widetilde{L}\otimes L$, $\overline{\sigma} \in G/G'$:

$$\begin{aligned}
\big(\tau\cdot\gamma(\tilde{l}\otimes l)\big)(\overline{\sigma}) &= \tau\big(\gamma(\tilde{l}\otimes l)(\overline{\tau^{-1}\sigma})\big) && \text{(def }\cdot\text{)}\\
&= \tau\big(\tilde{l}\ (\tau^{-1}\sigma)(l)\big) && \text{(def }\gamma\text{)}\\
&= \tau(\tilde{l})\ \sigma(l) && (\tau \in G = \mathrm{Aut}_K L)\\
&= \gamma\big((\tau(\tilde{l}))\otimes l\big)(\overline{\sigma}) && \text{(def }\gamma\text{)}\\
&= \gamma\big(\tau(\tilde{l}\otimes l)\big)(\overline{\sigma}) && (G \circlearrowleft \widetilde{L}\otimes L)
\end{aligned}$$

□

Remark 3.4.5. The action of G on the $\widetilde{L}$-basis $\{e_{\overline{\sigma}} : \overline{\sigma} \in G/G'\}$ of $\mathrm{Map}(G/G', \widetilde{L})$ is given by

$$\tau(e_{\overline{\sigma}}) = e_{\overline{\tau\sigma}} \underset{(\text{def } \lambda)}{=} e_{\lambda(\tau)(\overline{\sigma})}$$

so that it corresponds to the action of G on X given by the left translation map $\lambda : G \hookrightarrow \mathrm{Perm}(G/G')$.

Indeed, for every $\tau \in G$ and $\overline{\sigma}, \overline{\rho} \in G/G'$,

$$\begin{array}{rcll} (\tau(e_{\overline{\sigma}}))(\overline{\rho}) & = & \tau(e_{\overline{\sigma}}(\overline{\tau^{-1}\rho})) & (G \circlearrowleft \mathrm{Map}(G/G', \widetilde{L})) \\ & = & \tau(\underbrace{\delta_{\overline{\sigma}, \overline{\tau^{-1}\rho}}}_{\in\{0,1\}\subset K}) & (\text{def } e_{\overline{\sigma}}) \\ & = & \delta_{\overline{\sigma}, \overline{\tau^{-1}\rho}} & (\tau \in G = \mathrm{Aut}_K \widetilde{L}) \\ & = & \delta_{\overline{\tau\sigma}, \overline{\rho}} & (\overline{\sigma} = \overline{\tau^{-1}\rho} \Leftrightarrow \overline{\tau\sigma} = \overline{\rho}) \\ & = & e_{\overline{\tau\sigma}}(\overline{\rho}) & (\text{def } e_{\overline{\sigma}}) \end{array}$$

Remark 3.4.6. Let X be a finite set, E a field and for $x \in X$, let

$$\begin{array}{rcccl} u_x & : & X & \to & E \\ & & y & \mapsto & \delta_{x,y} \end{array}$$

Then $\{u_x : x \in X\}$ is an E-basis of the E-algebra $M := \mathrm{Map}(X, E)$ and is a set of primitive pairwise orthogonal idempotents of $\mathrm{Map}(X, E)$. Indeed,

- Idempotents: for every $x, y \in X$, $u_x^2 = u_x$:

$$\begin{array}{rcll} u_x^2(y) & = & (u_x u_x)(y) & \\ & = & u_x(y)\ u_x(y) & (\text{def mult. in } M) \\ & = & (u_x(y))^2 & \\ & = & \delta_{x,y}^2 & (\text{def } u_x) \\ & = & \delta_{x,y} & (E \text{ field}) \\ & = & u_x(y) & (\text{def } u_x) \end{array}$$

- Pairwise orthogonal: for every $x, x', y \in X$ such that $x \neq x'$, $u_x u_{x'} = 0$:

$$\begin{array}{rcll} (u_x u_{x'})(y) & = & u_x(y)\ u_{x'}(y) & (\text{def mult. in } M) \\ & = & \delta_{x,y}\ \delta_{x',y} & (\text{def } u_x) \\ & = & 0 & (x \neq x') \end{array}$$

- Primitive: recall that a non-zero idempotent is said to be primitive if it cannot be written as a sum of non-zero orthogonal idempotents.

  First of all, observe that every idempotent of M maps any element to 0 or 1: for every $f \in M$ idempotent and every $y \in X$,

$$f^2(y) = f(y) \underset{(E \text{ field})}{\Rightarrow} f(y) \in \{0, 1\}.$$

Finally let us see that $\{u_x : x \in X\}$ are primitive: for every $f, g \in M$ orthogonal idempotents, if $u_x = f + g$, then for every $y \in X$,

$$\delta_{x,y} = u_x(y) = f(y) + g(y) = \begin{cases} 1(= 1 + 0 \text{ or } 0 + 1) & \text{if } x = y \\ 0(= 0 + 0) & \text{if } x \neq y \end{cases}$$

Hence $f = 0$ or $g = 0$.

Lemma 3.4.7. *If $\mathcal{B}$ is a basis of pairwise orthogonal idempotents, then any other idempotent is a sum of elements of $\mathcal{B}$.*

The next result describes the Hopf Galois structures on such "split" algebras $\mathrm{Map}(X, E)$. In order to prove it, we need a previous lemma:

Lemma 3.4.8. *Let X be a finite set of cardinality n. If H is a cocommutative E-Hopf algebra such that $\mathrm{Map}(X, E)|E$ is H-Galois, then there is an E-algebra isomorphism:*

$$E \oplus \overset{n^2}{\ldots} \oplus E \cong H^* \oplus \overset{n}{\ldots} \oplus H^*$$

where $H^* = \mathrm{Hom}_E(H, E)$ is the dual E-Hopf algebra.

Proof. The proof is omitted in [Ch1]. The following are E-algebra isomorphisms:

$$\begin{aligned} E \oplus \overset{n^2}{\ldots} \oplus E &\cong \mathrm{Map}(X \times X, E) && \text{(by (1) below)} \\ &\cong \mathrm{Map}(X, E) \otimes_E \mathrm{Map}(X, E) && \text{(by (2) below)} \\ &\cong \mathrm{Map}(X, E) \otimes_E H^* && \text{(by (3) below)} \\ &\cong H^* \oplus \overset{n}{\ldots} \oplus H^* && \text{(by (4) below)} \end{aligned}$$

where:

(1) Let Y be a finite set. It is already known that the following is an E-linear isomorphism:

$$\mathrm{Map}(Y, E) \cong E \oplus \overset{|Y|}{\ldots} \oplus E.$$

Since the product in $\mathrm{Map}(Y, E)$ is componentwise, it follows that it is moreover an E-algebra isomorphism. Hence we take $Y = X \times X$.

(2) Indeed, by using (1) above and the distributivity of $\otimes$ with respect to $\oplus$:

$$\begin{aligned} \mathrm{Map}(X, E) \otimes_E \mathrm{Map}(X, E) &\cong (E \oplus \overset{n}{\ldots} \oplus E) \otimes_E (E \oplus \overset{n}{\ldots} \oplus E) \\ &\cong (E \otimes_E E) \oplus \overset{n^2}{\ldots} \oplus (E \otimes_E E) \\ &\cong E \oplus \overset{n^2}{\ldots} \oplus E \\ &\cong \mathrm{Map}(X \otimes X, E) \end{aligned}$$

(3) By assumption, $\mathrm{Map}(X,E)|E$ is H-Galois, so that by Definition 2.4.3 we have the following E-linear isomorphism:

$$j : \mathrm{Map}(X,E) \otimes_E H \to \mathrm{End}_E(\mathrm{Map}(X,E))$$

By Proposition 2.2.18 (2) (with $S = \mathrm{Map}(X,E)$), it yields the E-linear isomorphism:

$$\gamma : \mathrm{Map}(X,E) \otimes_E \mathrm{Map}(X,E) \to \mathrm{Map}(X,E) \otimes_E H^*$$

It remains to check that γ is an E-algebra homomorphism in this particular case, which follows from the whole Proposition 2.2.18.

(4) Indeed, by using (1) above and the distributivity of $\otimes$ with respect to $\oplus$:

$$\begin{aligned} \mathrm{Map}(X,E) \otimes_E H^* &\cong (E \oplus \overset{n}{\ldots} \oplus E) \otimes_E H^* \\ &\cong (E \otimes_E H^*) \oplus \overset{n}{\ldots} \oplus (E \otimes_E H^*) \\ &\cong H^* \oplus \overset{n}{\ldots} \oplus H^* \end{aligned}$$

□

Corollary 3.4.9. *In the previous notation, there is an E-algebra isomorphism:*

$$H^* \cong E \oplus \overset{n}{\ldots} \oplus E.$$

Proof. Sketch of the proof, which is omitted in [Ch1]. Recall the following definitions (see [La] XVII): let R be a ring.

1. An *R-module* is *simple* if it has no proper submodules.

2. An *R-module* is *semisimple* if it is a direct sum of simple submodules.

3. The *ring* R is *semisimple* if it is simple as an R-module.

Notice that if we consider the ring R as an R-module, its submodules are its ideals. Therefore a ring is simple if and only if it has no proper ideals. In particular, every field is a simple ring.

By [La] XVII, §2, Proposition 2.2, we know that every submodule of a semisimple module is semisimple. More precisely, the proof shows that if $M = \oplus_{i\in I} M_i$, with M_i simple submodules, and N is a submodule of M, then there exists $J \subseteq I$ such that $N = \oplus_{i\in J} M_i$.

It remains to check that the isomorphism follows from applying both the previous observation and result to Lemma 3.4.8. □

Theorem 3.4.10. *Let X be a finite set and let E be a field. If H is a finite cocommutative E-Hopf algebra such that $\mathrm{Map}(X, E)|E$ is H-Galois, then H is a group ring $E[N]$ for some group N of the same cardinality as X. Moreover, N may be identified as a subgroup of $\mathrm{Perm}(X)$, where the action of N on X is defined by $u_{\eta(x)} = \eta(u_x)$, for every $\eta \in N$, $x \in X$. Hence N is a regular subgroup of $\mathrm{Perm}(X)$. Conversely, if N is a regular subgroup of $\mathrm{Perm}(X)$, then $\mathrm{Map}(X, E)|E$ is $E[N]$-Galois.*

Proof. It is based on the proof given in Th. 6.3 [Ch1]. Set $n := |X|$, $M := \mathrm{Map}(X, E)$. Assume $M|E$ is H-Galois. By Corollary 3.4.9, there is an E-algebra isomorphism:

$$H^* \cong E \oplus \overset{n}{\dots} \oplus E. \tag{3.5}$$

Thus for every $i \in \{1, \dots, n\}$, let us define the i-th coordinate function:

$$\begin{array}{cccl} \eta_i & : & H^* & \to & E \\ & & (e_1, \dots, e_n) & \mapsto & e_i \end{array}$$

Then $N := \{\eta_i : i \in \{1, \dots, n\}\}$ is clearly a basis of $\mathrm{Hom}_E(H^*, E) = H^{**}$. Since H is finite (by assumption), $H^{**} \cong H$ so that N is a basis of H. Moreover, for every $i \in \{1, \dots, n\}$, η_i is clearly an E-algebra isomorphism, hence by Remark 2.3.11, it is grouplike in $H^{**} \cong H$.

All in all, since N is a basis of H and it is made up of grouplike elements, then N consists of all grouplike elements in H ($N = G(H)$ by Proposition 2.1.17). Therefore by Proposition 2.3.12, N is a group, so that H is the group ring $H = E[N]$:

$$E[N] = \{\textstyle\sum \lambda_\eta \eta : \ \eta \in N, \ \lambda_\eta \in E\} = \left\{ \sum_{i=1}^{n} \lambda_i \eta_i : \ \eta_i \in N \right\} = H \tag{3.6}$$

since it is easy to check that the Hopf algebra structure is preserved (by using the definition of the structure maps of a Hopf algebra and that η_i is grouplike).

Claim 1: N acts as a group of permutations of X.

By Remark 3.4.6, let $\mathcal{B} = \{u_x : x \in X\}$ be the basis of primitive pairwise orthogonal idempotents of $\mathrm{Map}(X, E)$, where $u_x(y) = \delta_{x,y}$, for every $x, y \in X$.

Now, the idea is the following: since $\mathrm{Map}(X, E)|E$ is H-Galois (by assumption) and we have seen that $H = E[N]$, we have the Hopf action

$$E[N] \times \mathrm{Map}(X, E) \to \mathrm{Map}(X, E)$$

that restricted to N yields an action

$$N \times \mathrm{Map}(X, E) \to \mathrm{Map}(X, E)$$

Now we will check that we can also restrict to $\mathcal{B}$ to obtain the following action:

$$\begin{array}{ccl} N \times \mathcal{B} & \to & \mathcal{B} \\ (\eta, u_x) & \mapsto & \eta(u_x) = u_y \quad \text{for some } y \in X \end{array}$$

so that since $\mathcal{B}$ is indexed by X, it may be seen as the action

$$\begin{array}{rcl} N \times X & \to & X \\ (\eta, x) & \mapsto & \eta(x) = y \Leftrightarrow \eta(u_x) = u_y \text{ for some } y \in X \end{array}$$

that is equivalent to say that N acts as a group of permutations of X. Hence it remains to show is that the action $N \circlearrowleft \operatorname{Map}(X, E)$ induces the action $N \circlearrowleft \mathcal{B}$ described previously.

Recall that since $M|E$ is H-Galois (by assumption), by definition M is an $E[N]$-module E-algebra. Moreover, let us notice the following facts:

(a) For every $x \in X$ and $\eta \in N$, $\eta(u_x)$ is idempotent:

$$\begin{aligned} \eta(u_x) &= \eta(u_x u_x) && (u_x \text{ idempotent}) \\ &= \eta(u_x)\eta(u_x) && (\text{Rem } 2.2.10) \end{aligned}$$

(b) The set $\{\eta(u_x) : x \in X\}$ are pairwise orthogonal: for every $x \neq y \in X$,

$$\begin{aligned} \eta(u_x)\eta(u_y) &= \eta(u_x u_y) && (\text{Rem } 2.2.10) \\ &= \eta(0) && (\mathcal{B} \text{ pairwise orthog}) \\ &= 0 && (M \ \ E[N]\text{-module}) \end{aligned}$$

(c) For every $x \in X$ and $\eta \in N$, $\eta(u_x) \neq 0$:

$$\begin{aligned} 0 &\neq u_x && (\mathcal{B} \text{ basis of } M) \\ &= 1_N(u_x) && (\text{def action } N \circlearrowleft M) \\ &= (\eta^{-1}\eta)(u_x) && \left(\begin{array}{c} N = G(H) \text{ mult subg} \\ \text{see Prop } 2.3.12 \end{array}\right) \\ &= \eta^{-1}(\eta(u_x)) && (\text{def action } N \circlearrowleft M) \end{aligned}$$

Since the action of N on $\operatorname{Map}(X, E)$ is the scalar product of $\operatorname{Map}(X, E)$ as an $E[N]$-module, we obtain:

$$\eta^{-1}(\eta \cdot u_x) \neq 0 \ \Rightarrow \ \eta(u_x) \neq 0.$$

(d) $1_M = \sum_{x \in X} u_x$: since $1_M : X \to E$ maps any element of X to 1_E, take $y \in X$:

$$\left(\sum_{x \in X} u_x\right)(y) = \sum_{x \in X} u_x(y) = \sum_{x \in X} \delta_{x,y} = \delta_{y,y} = 1_E.$$

(e) $\eta(1_M) = 1_M$:

$$\eta(1_M) \underset{(2.1)}{=} \varepsilon_e(\eta) 1_M \underset{\left(\substack{\text{Prop} \\ 2.1.16}\right)}{=} 1_E 1_M = 1_M.$$

Therefore, we obtain:

$$\sum_{x\in X} u_x \underset{\text{(d)}}{=} 1_M \underset{\text{(c)}}{=} \eta(1_M) \underset{\text{(d)}}{=} \eta\Bigg(\sum_{x\in X} u_x\Bigg) = \sum_{x\in X} \eta(u_x).$$

Now by (a), every $\eta(u_x) \in M$ is idempotent, where $\mathcal{B}$ is a basis of M, so that by Lemma 3.4.7 every $\eta(u_x)$ is a sum of elements of $\mathcal{B}$. Hence by (b), the elements of $\mathcal{B}$ appearing in the decomposition of one $\eta(u_x)$ do not appear in the decomposition of the remaining ones (otherwise, if we multiply them, the repeated element will remain and the product will not be zero). Thus by (c), there is at least one summand in each decomposition. Finally, since $|\mathcal{B}| = |X|$, there is exactly one summand in each decomposition, so that we conclude:

$$\forall\ x \in X,\ \exists\ y \in X \text{ such that } \eta(u_x) = u_y \tag{3.7}$$

and therefore

$$\{u_x :\ x \in X\} = \{\eta(u_x) :\ x \in X\}. \tag{3.8}$$

<u>Claim 2</u>: N is a regular subgroup of $\mathrm{Perm}(X)$.

By definition of regular, we will check that:

- $|N| = |X| = n$:

$$n = \dim_E(E \oplus \overset{n}{\cdots} \oplus E) \underset{(3.5)}{=} \dim_E H^* \underset{(H \text{ finite})}{=} \dim_E H \underset{(3.6)}{=} \dim_E E[N] = |N|.$$

- N acts transitively on X, that is, for every $x, y \in X$, there exists $\eta \in N$ such that $\eta(x) = y$.

  By reduction to absurdity: assume N does not act transitively on X, so that there exists $x \in X$ such that for every $y \in X$, $\eta(x) \neq y$. Hence we define

$$N_{u_x} := \{\eta(u_x) :\ \eta \in N\} \underset{(3.8)}{=} \{u_y :\ y \in X\} \subsetneq \mathcal{B}, \text{ where } Y \subsetneq X. \tag{3.9}$$

  Moreover, by assumption $\mathrm{Map}(X,E)|E$ is $(H,\cdot)$-Galois, so by definition there is an E-linear isomorphism:

$$\begin{array}{rcrcl} j & : & \mathrm{Map}(X,E) \otimes_E H & \to & \mathrm{End}_E(\mathrm{Map}(X,E)) \\ & & s \otimes h & \mapsto & j(s \otimes h)(t) = s(h \cdot t) \end{array}$$

  The contradiction will come by seeing that j is not surjective. Indeed, since $\mathcal{B}$ is a basis of $\mathrm{Map}(X,E)$ and N is a basis of $H = E[N]$ (3.6), then $\mathrm{Map}(X,E)\otimes_E H$ have basis $\{u_z \otimes \eta :\ z \in X,\ \eta \in N\}$, so that for every $\xi \in \mathrm{Map}(X,E) \otimes_E E$,

$$\xi = \sum_{\eta\in N} \sum_{z\in X} \lambda_{z,\eta}\, u_z \otimes \eta.$$

Therefore,

$$\begin{aligned}
j\left(\sum_{\eta\in N}\sum_{z\in X}\lambda_{z,\eta}\ u_z\otimes\eta\right)(u_x) &= \sum_{\eta\in N}\sum_{z\in X}\lambda_{z,\eta}\ j(u_z\otimes\eta)(u_x) && (j \text{ linear})\\
&= \sum_{\eta\in N}\sum_{z\in X}\lambda_{z,\eta}\ u_z\ \eta(u_x) && (\text{def } j)\\
&= \sum_{\eta\in N}\lambda_{y,\eta}\ u_y && (\text{by (1) below})\\
&\in\ <\{u_y:\ y\in Y\}> && (\text{def } <\cdot>)\\
&\notin\ \mathrm{Map}(X,E) && (3.9)
\end{aligned}$$

where (1) holds since for the fixed $x\in X$, there exists $y\in X$ such that $\eta(u_x)=u_y$ (3.7), so that since elements of $\mathcal{B}$ are pairwise orthogonal, we get:

$$u_z\ \eta(u_x)=u_zu_y=\begin{cases}u_y & \text{if } z=y\\ 0 & \text{if } z\neq y\end{cases}$$

Finally, since we can always define an endomorphism by sending the basis $\mathcal{B}$ to any set of vectors, we can find out an endomorphism that sends u_x out of $<\{u_y:\ y\in Y\}>$, so that j is not surjective.

Conversely, assume N is a regular subgroup of $\mathrm{Perm}(X)$ and let us see that $M|E$ is $E[N]$-Galois. First of all, we define the Hopf action. Since $N\leq\mathrm{Perm}(X)$ is regular, then N acts on X, so that N also acts on $\mathcal{B}=\{u_x:\ x\in X\}$ by acting on the indexes. Hence we define the Hopf action as follows:

$$\begin{array}{rcrcl}\mu & : & E[N]\times\mathrm{Map}(X,E) & \to & \mathrm{Map}(X,E)\\ & & (\eta,u_x) & \mapsto & \eta(u_x)=u_{\eta(x)}\end{array}$$

Now we need to see that $\mathrm{Map}(X,E)|E$ is $(E[N],\mu)$-Galois by checking the two conditions of the definition:

- $j:\mathrm{Map}(X,E)\otimes_E E[N]\to\mathrm{End}_E(\mathrm{Map}(X,E))$ is an E-linear isomorphism.

  Notice that both dimensions are equal:

  - On the one hand,

    $$\dim_E\mathrm{Map}(X,E)=\dim_E E^{|X|}=\dim_E E^n=n.$$

    On the other hand, since N is a regular subgroup of $\mathrm{Perm}(X)$, then $|N|=|X|$, so that:

    $$\dim_E E[N]=|N|=|X|=n.$$

All in all, we obtain:

$$\dim_E(\mathrm{Map}(X,E)\otimes_E E[N]) = \dim_E \mathrm{Map}(X,E)\cdot \dim_E E[N] = n^2.$$

- Moreover, it holds that:

$$\dim_E \mathrm{End}_E(\mathrm{Map}(X,E)) = (\dim_E \mathrm{Map}(X,E))^2 = n^2.$$

Thus it remains to show that j is surjective: one may take a basis of $\mathrm{End}_E(M)$ and check that every element of the basis belongs to the image of j.

- $\mathrm{Map}(X,E)$ is a left $E[N]$-module E-algebra: we need to check the three conditions of the definition:
  - $\mathrm{Map}(X,E)$ is an E-algebra (see Definition 2.1.6);
  - $\mathrm{Map}(X,E)$ is an $E[N]$-module (since we have defined the action μ of $E[N]$ on $\mathrm{Map}(X,E)$);
  - It is easy to check that both diagrams of Definition 2.2.9 (a) commute.

□

3.5 Greither-Pareigis' theorem

In this section we finally prove Greither-Pareigis' theorem. We also introduce the definition of the type of a Hopf Galois structure and that of an almost classically Galois structure. In order to close it, we state two important properties of Hopf Galois structures.

We wish to apply this description of Hopf Galois structures (see Theorem 3.4.10) on $\mathrm{Map}(X,E)|E$ to obtain information of Hopf Galois structures on field extensions.

Proposition 3.5.1. *Let $L|K$ be an $(H,\cdot)$-Galois extension with normal closure $\widetilde{L}$, let $G=\mathrm{Gal}(\widetilde{L}|K)$, $G'=\mathrm{Gal}(\widetilde{L}|L)$ and $X=G/G'$. The Hopf action of $\widetilde{L}\otimes H$ on $\widetilde{L}\otimes L$ obtained by base change:*

$$\begin{array}{cccc} \varphi & : & (\widetilde{L}\otimes H)\otimes_{\widetilde{L}}(\widetilde{L}\otimes L) & \to & \widetilde{L}\otimes L \\ & & (\tilde{s}\otimes h)\otimes(\tilde{t}\otimes x) & \mapsto & (\tilde{s}\tilde{t})\otimes(h\cdot x) \end{array}$$

is equivalent to an action

$$\psi : \widetilde{L}[N]\otimes_{\widetilde{L}} \mathrm{Map}(X,\widetilde{L}) \to \mathrm{Map}(X,\widetilde{L})$$

of $\widetilde{L}[N]$ on $\mathrm{Map}(X,\widetilde{L})$, which corresponds to a regular embedding of some group N of order $|X|$ into $\mathrm{Perm}(X)$ with the property that if $\lambda : G \hookrightarrow \mathrm{Perm}(X)$ is the left translation, then $\lambda(G)$ normalizes the image of N in $\mathrm{Perm}(X)$.

Proof. It is based on the argumentation given in pages 50-51 [Ch1].

On the one hand, by definition of $\mathrm{Map}(X,\widetilde{L})$, let $\mathcal{B}=\{u_{\overline{\sigma}} : \overline{\sigma}\in X\}$ be its canonical basis. Then by Proposition 3.4.4, there is a G-module isomorphism:

$$\begin{array}{rccl} \gamma & : & \widetilde{L} \otimes L & \to & \mathrm{Map}(X, \widetilde{L}) \\ & & \tilde{l} \otimes l & \mapsto & \gamma(\tilde{l} \otimes l)(\overline{\sigma}) = \tilde{l}\sigma(l) \end{array}$$

where G acts on $\mathcal{B}$ as follows (see Remark 3.4.5):

$$\begin{array}{ccl} G \times \mathcal{B} & \to & \mathcal{B} \\ (\tau, u_{\overline{\sigma}}) & \mapsto & \tau(u_{\overline{\sigma}}) = u_{\overline{\tau\sigma}} = u_{\lambda(\tau)(\overline{\sigma})} \end{array} \tag{3.10}$$

On the other hand, by Theorem 3.4.10, there is a regular subgroup N of $\mathrm{Perm}(X)$ so that $\widetilde{L} \otimes H = \widetilde{L}[N]$ and the action on N on $\mathcal{B}$ is:

$$\eta(u_{\overline{\sigma}}) = u_{\eta(\overline{\sigma})} \tag{3.11}$$

Hence the action φ becomes isomorphic to an action

$$\begin{array}{rcrcl} \psi & : & \widetilde{L}[N] \otimes_{\widetilde{L}} \mathrm{Map}(X, \widetilde{L}) & \to & \mathrm{Map}(X, \widetilde{L}) \\ & & \eta \otimes u_{\overline{\sigma}} & \mapsto & \psi(\eta \otimes u_{\overline{\sigma}}) = \eta(u_{\overline{\sigma}}) \end{array} \tag{3.12}$$

Now it remains to show that this action is as stated in the proposition.

Claim 1: G acts on N.

Indeed, since $G = \mathrm{Aut}_K(\widetilde{L})$, G acts on $\widetilde{L}$, hence G also acts on $\widetilde{L} \otimes H$ via the left factor and it preserves the Hopf algebra structure (because the Hopf algebra structure of $\widetilde{L} \otimes H$ is obtained by scalar extension). Moreover, since $\widetilde{L} \otimes H = \widetilde{L}[N]$ as Hopf algebras, G acts on $\widetilde{L}[N]$ preserving the Hopf algebra structure.

Recall that the set of grouplike elements of $\widetilde{L}[N]$ is N (see Remark 2.1.15). Furthermore, G maps grouplike elements to grouplike elements: for every $\eta \in N$ (hence it is grouplike), let us check that $\sigma(\eta)$ is also grouplike for every $\sigma \in G$:

$$\begin{array}{rcll} \Delta_{\widetilde{L}[N]}(\sigma(\eta)) & = & \sigma(\Delta_{\widetilde{L}[N]}(\eta)) & (G \text{ preserves struct.}) \\ & = & \sigma(\eta \otimes \eta) & (\text{def } \Delta_{\widetilde{L}[N]}) \\ & = & \sigma(\eta) \otimes \sigma(\eta) & (G \circlearrowleft H \Rightarrow G \circlearrowleft H \otimes H) \end{array}$$

Thus we conclude that G acts on N, as desired.

Claim 2: The previous action of G on N is via conjugation by λ.

First of all, let us see φ is G-equivariant, that is, for every $\sigma \in G$ and every $A \in (\widetilde{L} \otimes H) \otimes_{\widetilde{L}} (\widetilde{L} \otimes L)$:

$$\sigma(\varphi(A)) = \varphi(\sigma(A))$$

Indeed, since $G = \mathrm{Aut}_K(\widetilde{L})$ acts on $\widetilde{L}$, G acts on $\widetilde{L} \otimes L$ and on $(\widetilde{L} \otimes H) \otimes_{\widetilde{L}} (\widetilde{L} \otimes L)$ via the left factor, so that if $A = (\tilde{s} \otimes h) \otimes (\tilde{t} \otimes x)$,

$$\begin{aligned}
\sigma\big(\varphi(A)\big) &= \sigma\big(\varphi((\tilde{s} \otimes h) \otimes (\tilde{t} \otimes x))\big) && (\text{def } A)\\
&= \sigma\big((\tilde{s}\tilde{t}) \otimes (h \cdot x)\big) && (\text{def } \varphi)\\
&= \sigma(\tilde{s}\tilde{t}) \otimes (h \cdot x) && (G \circlearrowright \widetilde{L} \otimes L)\\
&= (\sigma(\tilde{s})\sigma(\tilde{t})) \otimes (h \cdot x) && (\sigma \text{ morphism})\\
&= \varphi\big((\sigma(\tilde{s}) \otimes h) \otimes (\sigma(\tilde{t}) \otimes x)\big) && (\text{def } \varphi)\\
&= \varphi\big(\sigma((\tilde{s} \otimes h) \otimes (\tilde{t} \otimes x))\big) && (G \circlearrowright (\widetilde{L} \otimes H) \otimes_{\widetilde{L}} (\widetilde{L} \otimes L))\\
&= \varphi\big(\sigma(A)\big) && (\text{def } A)
\end{aligned}$$

Therefore ψ is G-equivariant as well, hence it follows that for every $\tau \in G$, $\eta \in N$ and $u_{\overline{\sigma}} \in \mathcal{B}$:

$$\tau(\eta)\big(\tau(u_{\overline{\sigma}})\big) = \tau(\eta(u_{\overline{\sigma}})) \tag{3.13}$$

Indeed,

$$\begin{aligned}
\tau(\eta)\big(\tau(u_{\overline{\sigma}})\big) &= \psi\big(\tau(\eta) \otimes \tau(u_{\overline{\sigma}})\big) && (3.12)\\
&= \psi\big(\tau(\eta \otimes u_{\overline{\sigma}})\big) && (G \circlearrowright N \times \mathcal{B})\\
&= \tau\big(\psi(\eta \otimes u_{\overline{\sigma}})\big) && (\psi\ G - \text{equiv})\\
&= \tau\big(\eta(u_{\overline{\sigma}})\big) && (3.12)
\end{aligned}$$

Finally, let us see that the action of G on N is via conjugation by λ: for every $\tau \in G$, $\eta \in N$ and $u_{\overline{\sigma}} \in \mathcal{B}$,

$$\begin{array}{ccccccc}
\tau(\eta)\big(\tau(u_{\overline{\sigma}})\big) & \underset{(3.13)}{=} & \tau\big(\eta(u_{\overline{\sigma}})\big) & \underset{(3.11)}{=} & \tau\big(u_{\eta(\overline{\sigma})}\big) & \underset{(3.10)}{=} & u_{\lambda(\tau)(\eta(\overline{\sigma}))}\\
\| & & & & & & \\
\tau(\eta)\big(\tau(u_{\overline{\sigma}})\big) & \underset{(3.10)}{=} & \tau(\eta)\big(u_{\lambda(\tau)(\overline{\sigma})}\big) & \underset{(3.11)}{=} & u_{\tau(\eta)(\lambda(\tau)(\overline{\sigma}))} & &
\end{array}$$

All in all, we have obtained:

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

that is, if we define $\overline{\rho} := \lambda(\tau)(\overline{\sigma})$ (and so $\overline{\sigma} = \lambda(\tau^{-1})(\overline{\rho})$), we get:

$$\tau(\eta)(\overline{\rho}) = \big(\lambda(\tau) \circ \eta \circ \lambda(\tau^{-1})\big)(\overline{\rho})$$

Hence we conclude that the action of $\tau \in G$ on $\eta \in N$ is via conjugation by $\lambda(\tau) \in \mathrm{Perm}(X)$:

$$\tau(\eta) = \lambda(\tau) \circ \eta \circ \lambda(\tau^{-1})$$

□

The theorem of Greither and Pareigis asserts that the above proposition has a converse, namely: given $N \subseteq \operatorname{Perm}(X)$ normalized by $\lambda(G)$, there is a unique Hopf Galois structure on $L|K$ which yields N.

Proposition 3.5.2. *Let $L|K$ be a separable field extension with normal closure $\widetilde{L}$, let $G = \operatorname{Gal}(\widetilde{L}|K)$, $G' = \operatorname{Gal}(\widetilde{L}|L)$ and $X = G/G'$. If N is a regular subgroup of* $\operatorname{Perm}(X)$ *normalized by $\lambda(G)$, then $L|K$ is H-Galois, where H is a $\widetilde{L}|K$-form of $K[N]$.*

Proof. Let $N \le \operatorname{Perm}(X)$ be regular and normalized by $\lambda(G)$. Let $\mathcal{B} = \{u_{\overline{\sigma}} : \overline{\sigma} \in X\}$ be the canonical $\widetilde{L}$-basis of $M := \operatorname{Map}(X, \widetilde{L})$. Then by Theorem 3.4.10, $\operatorname{Map}(X, \widetilde{L})|\widetilde{L}$ is $\widetilde{L}[N]$-Galois, so that the Hopf action is defined on the basis as:

$$\begin{array}{rcrcl} \mu & : & \widetilde{L}[N] \otimes_{\widetilde{L}} \operatorname{Map}(X, \widetilde{L}) & \to & \operatorname{Map}(X, \widetilde{L}) \\ & & \eta \otimes u_{\overline{\sigma}} & \mapsto & \eta(u_{\overline{\sigma}}) = u_{\eta(\overline{\sigma})} \end{array}$$

Since N is normalized by $\lambda(G)$, then for every $\sigma \in G$, there is a bijection:

$$\begin{array}{rcrcl} p_\sigma & : & N & \to & N \\ & & \eta & \mapsto & \lambda(\sigma)\eta\lambda(\sigma^{-1}) \end{array}$$

that yields the following group morphism:

$$\begin{array}{rcl} G & \to & \operatorname{Aut}(N) \\ \sigma & \mapsto & p_\sigma \end{array}$$

Indeed, for every $\sigma, \tau \in G$ and $\eta \in N$,

$$\begin{array}{rcll} (p_\sigma \circ p_\tau)(\eta) & = & p_\sigma\big(\lambda(\tau)\eta\lambda(\tau^{-1})\big) & (\text{def } p_\tau) \\ & = & \lambda(\sigma)\ \lambda(\tau)\ \eta\ \lambda(\tau^{-1})\ \lambda(\sigma^{-1}) & (\text{def } p_\sigma) \\ & = & \lambda(\sigma\tau)\ \eta\ \lambda(\tau^{-1}\sigma^{-1}) & (\lambda \text{ group morp}) \\ & = & \lambda(\sigma\tau)\ \eta\ \lambda((\sigma\tau)^{-1}) & ((f \circ g)^{-1} = g^{-1} \circ f^{-1}) \\ & = & p_{\sigma\tau}(\eta) & (\text{def } p_{\sigma\tau}) \end{array}$$

Notice that, for every $\sigma \in G$, $p_\sigma \in \operatorname{Aut}(N) \cong \operatorname{Aut}(\widetilde{L}[N])$ (where an automorphism of N is extended to an automorphism of $\widetilde{L}[N]$ seeing $\widetilde{L}[N]$ as a Hopf algebra). Consider $\widetilde{L}[N]$ and $\operatorname{Aut}(\widetilde{L}[N])$ as trivial G-modules, so that by Remark 3.3.2, p_σ is a 1-cocycle from G into $\operatorname{Aut}(\widetilde{L}[N])$.

Furthermore define $\mu^\sigma := \sigma \circ \mu \circ \sigma^{-1}$, and let us check that the following diagram commutes:

$$\begin{tikzcd} \widetilde{L}[N] \otimes_{\widetilde{L}} \operatorname{Map}(X, \widetilde{L}) \arrow[r, "\mu^\sigma"] \arrow[d, "p_\sigma \otimes \mathrm{I}_M"'] & \operatorname{Map}(X, \widetilde{L}) \arrow[d, "\mathrm{I}_M"] \\ \widetilde{L}[N] \otimes_{\widetilde{L}} \operatorname{Map}(X, \widetilde{L}) \arrow[r, "\mu"'] & \operatorname{Map}(X, \widetilde{L}) \end{tikzcd}$$

Recall that G acts trivially on N and G acts on $\mathrm{Map}(X,\widetilde{L})$ as in Remark 3.4.5:

$$\begin{array}{rcl} G\times \mathrm{Map}(X,\widetilde{L}) & \to & \mathrm{Map}(X,\widetilde{L}) \\ (\tau, u_{\overline{\sigma}}) & \mapsto & u_{\overline{\tau\sigma}} = u_{\lambda(\tau)(\overline{\sigma})} \end{array}$$

Indeed, let us see that the identity $\mu^\sigma = \mu\circ(p_\sigma\otimes \mathrm{I}_M)$ holds.

$$\begin{array}{rcll} \mu^\sigma(\eta\otimes u_{\overline{\rho}}) & = & (\sigma\circ\mu\circ\sigma^{-1})(\eta\otimes u_{\overline{\rho}}) & (\text{def } \mu^\sigma) \\ & = & (\sigma\circ\mu)(\eta\otimes u_{\overline{\sigma^{-1}\rho}}) & (G \circlearrowleft N\otimes M) \\ & = & \sigma(u_{\eta(\overline{\sigma^{-1}\rho})}) & (\text{def } \mu) \\ & = & u_{\overline{\sigma}\,\eta(\overline{\sigma^{-1}\rho})} & (G \circlearrowleft \mathcal{B}) \\ & = & u_{\overline{\sigma}\,\eta\lambda(\sigma^{-1})(\overline{\rho})} & (\text{def } \lambda) \\ & = & u_{(\lambda(\sigma)\eta\lambda(\sigma^{-1}))(\overline{\rho})} & (\text{def } \lambda) \\ & = & \mu\big(\lambda(\sigma)\eta\lambda(\sigma^{-1})\otimes u_{\overline{\rho}}\big) & (\text{def } \mu) \\ & = & \mu(p_\sigma\otimes \mathrm{I}_M)(\eta\otimes u_{\overline{\rho}}) & (\text{def } p_\sigma) \end{array}$$

Now we have the following $\widetilde{L}$-algebra isomorphisms:

$$\underset{\text{(by Prop 3.4.4)}}{\mathrm{Map}(X,\widetilde{L})\cong \widetilde{L}\otimes L} \qquad\qquad \widetilde{L}[N]\cong\widetilde{L}\otimes K[N]$$

Hence the previous commutative diagram induces the commutative diagram:

$$\begin{tikzcd} (\widetilde{L}\otimes K[N])\otimes_{\widetilde{L}}(\widetilde{L}\otimes L) \arrow[r, "\widetilde{\mu}^\sigma"] \arrow[d, "\widetilde{p}_\sigma\otimes \mathrm{I}_{\widetilde{L}\otimes L}"'] & \widetilde{L}\otimes L \arrow[d, "\mathrm{I}_{\widetilde{L}\otimes L}"] \\ (\widetilde{L}\otimes K[N])\otimes_{\widetilde{L}}(\widetilde{L}\otimes L) \arrow[r, "\widetilde{\mu}"'] & \widetilde{L}\otimes L \end{tikzcd}$$

where $\tilde{\mu}$ is a Hopf action since μ is so.

Therefore we can apply Galois descent theory to this situation. In the left part of the diagram we have the 1-cocycle $\tilde{p}_\sigma$ from G into $\mathrm{Aut}(\widetilde{L}\otimes K[N])$, and in the right part, the trivial 1-cocycle.

Then by Theorem 3.3.5, they correspond to $\widetilde{L}|K$-forms of algebras. Clearly, in the right part of the diagram, the $\widetilde{L}|K$-form of L is L. Let H be the $\widetilde{L}|K$-form of $K[N]$ defined by the 1-cocycle $\tilde{p}_\sigma$.

Thus by Lemma 3.3.8, $\tilde{\mu}$ is descendable, so that by definition, there exists a unique K-linear map which, is also a Hopf action:

$$\mu_0 : H\otimes L\to L$$

Finally, by Remark 3.4.3, μ_0 defines an (H,μ_0)-Galois structure on $L|K$. □

Remark 3.5.3. As shown in Section 5.2 [Sa], this theorem allows to obtain explicitly the Hopf Galois structure corresponding to a subgroup N. More precisely, by Galois descent we recover:

- The **Hopf algebra** H corresponding to a regular subgroup N of S_g normalized by $\lambda(G)$ is the Hopf subalgebra $\widetilde{L}[N]^G$ of the group algebra $\widetilde{L}[N]$ fixed under the action of G, where G acts on $\widetilde{L}$ by K-automorphisms and on N by conjugation via λ: for every $\sigma \in G$, $\eta \in N$,

$$\sigma\left(\sum_{x_\eta \in \widetilde{L}} x_\eta \eta\right) = \sum_{x_\eta \in \widetilde{L}} \sigma(x_\eta)\ \underbrace{\lambda(\sigma)\eta\lambda(\sigma)^{-1}}_{\in N},$$

- The **Hopf action** is induced by $\eta \mapsto \eta^{-1}(\overline{1}_G)$, for every $\eta \in N$, where we identify S_g with $\mathrm{Perm}(G/G')$, that is, the K-linear map

$$\begin{array}{rrcl} \psi : & \widetilde{L}[N] & \rightarrow & \mathrm{End}_K \widetilde{L} \\ & \eta \in N & \mapsto & \sigma \text{ such that } \eta^{-1}(\overline{1}_G) = \overline{\sigma} \\ & r \in \widetilde{L} & \mapsto & [f \mapsto rf] \end{array}$$

  induces by restriction to H the Hopf action $\psi_H : H \to \mathrm{End}_K L$.

Finally we can state Greither-Pareigis' theorem as follows:

Theorem 3.5.4 (Greither-Pareigis). *Let $L|K$ be a separable field extension with normal closure $\widetilde{L}$, let $G = \mathrm{Gal}(\widetilde{L}|K)$, $G' = \mathrm{Gal}(\widetilde{L}|L)$ and $X = G/G'$. There is a bijection between regular subgroups N of* $\mathrm{Perm}(X)$ *normalized by $\lambda(G)$ and Hopf Galois structures on $L|K$.*

Moreover, the K-Hopf algebra H is a $\widetilde{L}|K$-form of $K[N]$:

$$\widetilde{L} \otimes H \cong \widetilde{L} \otimes K[N] \cong \widetilde{L}[N].$$

Definition 3.5.5. Let $L|K$ be $(H,\cdot)$-Galois with the corresponding group N. The isomorphism class of N is called the **type** of the Hopf Galois structure $(H,\cdot)$. Moreover, if $\mathrm{Cent}(N) \subseteq \lambda(G)$, we say say that $(H,\cdot)$ is **almost classically Galois**.

Remark 3.5.6. Almost classically Galois structures receive this name since Th. 5.2 [G-P] proves that in such a case the Galois correspondence is bijective.

Finally, we close this chapter with two important properties of Hopf Galois structures, which will be very useful afterwards to determine whether the Galois correspondence is bijective and to give a partition of Hopf algebras in isomorphism classes, respectively. We need the previous definitions:

Definition 3.5.7. Let G and N be subgroups of the symmetric group S_g such that N is normalized by G.

- A **subgroup** M of N is **G-stable** if M is also normalized by G.
- Two **subgroups** N_1, N_2 of S_g are **G-isomorphic** if there is a G-isomophism, that is, there exists an isomorphism F between N_1 and N_2 satisfying that for every $\sigma \in G$,

$$F(\sigma n_1 \sigma^{-1}) = \sigma F(n_1) \sigma^{-1}.$$

Corollary 3.5.8. *Under the notation of Remark 3.5.3, the following properties hold:*

- *Property 1: There is a bijection between the set of K-sub-Hopf algebras of $H = \widetilde{L}[N]^G$ and the set of G-stable subroups of N.*
- *Property 2: Two Hopf algebras $H_1 = \widetilde{L}[N_1]^G$ and $H_2 = \widetilde{L}[N_2]^G$ are isomorphic if and only if N_1 and N_2 are G-isomorphic subgroups of S_g.*

It is a direct consequence of Greither-Pareigis' theorem and the proof may be found in Proposition 2.2 [C-R-V].

Chapter 4

Byott's theorem

This chapter is based on chapter 2, section 7 [Ch1] and the proofs of the results presented here have been enlarged with all details.

One difficulty with Greither-Pareigis criterion is that, applied directly, we need to find out which regular subgroups of $\mathrm{Perm}(G/G')$ are normalized by G, and for n much above 4, $\mathrm{Perm}(G/G')$ has a large number of regular subgroups. Thus it is useful to reverse the relationship between G and N.

4.1 Problem statement

In this section suppose $L|K$ is Galois with group G and $[L : K] = g$. We seek regular subgroups N of $\mathrm{Perm}(G)$ normalized by G. If N is a subgroup of $\mathrm{Perm}(G)$, N acts on G by permutations, and moreover if N is regular, there is a bijection:

$$\begin{array}{ccccc} b & : & N & \to & G \\ & & \eta & \mapsto & \eta \cdot \mathrm{e}_G = \eta(\mathrm{e}_G) \end{array}$$

where e_G is the identity element of G. Indeed,

- Injective: given $\eta_1, \eta_2 \in N$,

$$\begin{array}{rcll} b(\eta_1) = b(\eta_2) & \Rightarrow & \eta_1 \cdot \mathrm{e}_G = \eta_2 \cdot \mathrm{e}_G & (\text{def } b) \\ & \Rightarrow & \eta_1 \cdot \mathrm{e}_G = \sigma \text{ and } \eta_2 \cdot \mathrm{e}_G = \sigma & (\sigma := \eta_i \cdot \mathrm{e}_G \in G) \\ & \Rightarrow & \eta_1 = \eta_2 & (N \text{ reg; Rem } 3.1.8) \end{array}$$

- Bijective: Since N is regular, $|N| = |G| = g$.

The previous bijection induces the following isomorphism:

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

Indeed,

- Group morphism: given $\pi_1, \pi_2 \in \mathrm{Perm}(G)$,

$$\begin{aligned}
\varphi(\pi_1) \circ \varphi(\pi_2) &= (b^{-1} \circ \pi_1 \circ b) \circ (b^{-1} \circ \pi_2 \circ b) && (\text{def } \varphi)\\
&= b^{-1} \circ (\pi_1 \circ \pi_2) \circ b && (b^{-1} \circ b = \mathrm{I}_N)\\
&= \varphi(\pi_1 \circ \pi_2) && (\text{def } \varphi)
\end{aligned}$$

- Injective: given $\pi_1, \pi_2 \in \mathrm{Perm}(G)$,

$$\begin{aligned}
\varphi(\pi_1) = \varphi(\pi_2) &\Rightarrow \forall\ \eta \in N,\ b^{-1}(\pi_1 b(\eta)) = b^{-1}(\pi_2 b(\eta)) && (\text{def } \varphi)\\
&\Rightarrow \forall\ \eta \in N,\ \pi_1(b(\eta)) = \pi_2(b(\eta)) && (b \text{ bij})\\
&\Rightarrow \forall\ \sigma \in G,\ \pi_1(\sigma) = \pi_2(\sigma) && (b(N) = G)\\
&\Rightarrow \pi_1 = \pi_2
\end{aligned}$$

- Bijective: Since N is regular, $|N| = |G|$, so that $|\mathrm{Perm}(G)| = |\mathrm{Perm}(N)|$.

Now, let us notice that under φ:

- N is mapped to $\lambda_N(N)$ in $\mathrm{Perm}(N)$: for every $\mu, \eta \in N$,

$$\begin{aligned}
\varphi(\mu)(\eta) &= b^{-1}(\mu(b(\eta))) && (\text{def } \varphi)\\
&= b^{-1}(\mu(\eta \cdot \mathrm{e}_G)) && (\text{def } b)\\
&= b^{-1}(\mu \cdot (\eta \cdot \mathrm{e}_G)) && (N \circlearrowleft G \text{ by perm})\\
&= b^{-1}((\mu\eta) \cdot \mathrm{e}_G) && (\text{def action})\\
&= \mu\eta && (\text{def } b)\\
&= \lambda_N(\mu)(\eta) && (\text{def } \lambda_N)
\end{aligned}$$

  so that $\lambda_N = \varphi|_N$.

- $\lambda_G(G)$ is mapped to some group $G_0 \cong G$ in $\mathrm{Perm}(N)$:

$$\begin{tikzcd}
\lambda_G : G \arrow[r, hook] & \mathrm{Perm}(G) \arrow[r, "\varphi", "\sim"'] & \mathrm{Perm}(N) \\
G \arrow[r, mapsto] & \lambda_G(G) \arrow[r, mapsto] & G_0 \cong G
\end{tikzcd}$$

Hence, since $\lambda_G(G)$ normalizes N in $\mathrm{Perm}(G)$, G_0 normalizes $\lambda_N(N)$ in $\mathrm{Perm}(N)$:

$$\begin{tikzcd}
\varphi : \mathrm{Perm}(G) \arrow[r, "\sim"] & \mathrm{Perm}(N) \\
\lambda_G(G) \arrow[r, mapsto] \arrow[d, "\text{norma-}\atop\text{lizes}"'] \arrow[dr, phantom, "\Rightarrow"] & G_0 \cong G \arrow[d, "\text{norma-}\atop\text{lizes}"] \\
N \arrow[r, mapsto] & \lambda_N(N)
\end{tikzcd}$$

By this translation, we shall see that to find regular subgroups $N' \cong N$ of $\mathrm{Perm}(G)$ normalized by $\lambda_G(G)$ becomes a question of finding regular embeddings of G into the normalizer $\mathrm{Hol}(N)$ of $\lambda_N(N)$ in $\mathrm{Perm}(N)$, and $\mathrm{Hol}(N)$, the holomorph of N, is far smaller than $\mathrm{Perm}(G)$ and easy to describe.

4.2 Holomorph

Definition 4.2.1. Let N be a group. The **holomorph** of N is the normalizer of $\lambda_N(N)$ in $\mathrm{Perm}(N)$:

$$\mathrm{Hol}(N) = \mathrm{Norm}_{\mathrm{Perm}(N)}(\lambda_N(N)) = \{\pi \in \mathrm{Perm}(N) : \ \pi \text{ normalizes } \lambda_N(N)\}.$$

Proposition 4.2.2. $\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$, *where* $\rho := \rho_N$.

Proof. It is based on the proof given in Prop 7.2, page 56 [Ch1]. Firstly, we check that $\rho(N)\cdot\mathrm{Aut}(N) \subseteq \mathrm{Hol}(N)$. View $\mathrm{Aut}(N) \subseteq \mathrm{Perm}(N)$ in the obvious way and $\lambda(N), \rho(N) \hookrightarrow \mathrm{Perm}(N)$, where $\lambda := \lambda_N$.

Claim 1: $\mathrm{Aut}(N)$ normalizes $\lambda(N)$.

Given $\gamma \in \mathrm{Aut}(N)$, we want to see $\gamma\lambda(N) = \lambda(N)\gamma$ (in $\mathrm{Perm}(N)$). Indeed, for every $\eta, \mu \in N$:

$$\begin{aligned}
(\underset{\in\mathrm{Perm}(N)}{\underbrace{\gamma}\,\underbrace{\lambda(\eta)}})(\mu) &= \gamma(\lambda(\eta)(\mu)) && (\text{def } \circ)\\
&= \gamma(\eta\mu) && (\text{def } \lambda)\\
&= \gamma(\eta)\gamma(\mu) && (\gamma \text{ group morp})\\
&= \lambda(\gamma(\eta))\gamma(\mu) && (\text{def } \lambda)\\
&= (\underset{\in\mathrm{Perm}(N)}{\underbrace{\lambda(\gamma(\eta))}\,\underbrace{\gamma}})(\mu) && (\text{def } \circ)
\end{aligned}$$

so that:

$$\gamma\lambda(\eta) = \lambda(\gamma(\eta))\gamma, \ \forall \ \mu \in N \ \Rightarrow \ \gamma\lambda(N) = \lambda(N)\gamma, \text{ as desired.}$$

Claim 2: $\rho(N)$ centralizes $\lambda(N)$. In particular, $\rho(N)$ normalizes $\lambda(N)$.

Given $\eta, \mu \in N$, we want to see $\rho(\eta)\lambda(\mu) = \lambda(\mu)\rho(\eta)$. Indeed, for every $m \in N$:

$$\begin{aligned}
(\rho(\eta)\lambda(\mu))(m) &= \rho(\eta)(\lambda(\mu)(m)) && (\text{def } \circ)\\
&= \rho(\eta)(\mu m) && (\text{def } \lambda)\\
&= \mu m \eta && (\text{def } \rho)\\
&= \lambda(\mu)(m\eta) && (\text{def } \lambda)\\
&= \lambda(\mu)(\rho(\eta)(m)) && (\text{def } \rho)\\
&= (\lambda(\mu)\rho(\eta))(m) && (\text{def } \circ)
\end{aligned}$$

Therefore, claims 1 and 2 show that both $\mathrm{Aut}(N)$ and $\rho(N)$ are subgroups of $\mathrm{Hol}(N)$. Now, let us show that the product is a subgroup as well.

Claim 3: $\mathrm{Aut}(N)$ normalizes $\rho(N)$.

Given $\gamma \in \mathrm{Aut}(N)$, we want to see that $\gamma\rho(N) = \rho(N)\gamma$ (in $\mathrm{Perm}(N)$). Indeed, for every $\eta, \mu \in N$:

$$\begin{aligned}
(\gamma \circ \rho(\eta))(\mu) &= \gamma(\rho(\eta)(\mu)) && (\text{def } \circ)\\
&= \gamma(\mu\eta^{-1}) && (\text{def } \rho)\\
&= \gamma(\mu)\gamma(\eta^{-1}) && (\rho \text{ group morp})\\
&= \gamma(\mu)(\gamma(\eta))^{-1} && (\gamma \text{ group morp})\\
&= (\rho(\gamma(\eta))\gamma(\mu) && (\text{def } \rho)\\
&= (\rho(\gamma(\eta)) \circ \gamma)(\mu) && (\text{def } \circ)
\end{aligned}$$

so that:

$$\gamma\rho(\eta) = \rho(\gamma(\eta))\gamma, \ \forall\ \mu \in N \ \Rightarrow\ \gamma\rho(N) = \rho(N)\gamma, \text{ as desired.}$$

Therefore, it follows that $\rho(N) \cdot \mathrm{Aut}(N)$ is a subgroup of $\mathrm{Perm}(N)$ which is contained in $\mathrm{Hol}(N)$. Indeed, for every $\eta, \eta' \in \rho(N)$ and $\sigma, \sigma' \in \mathrm{Aut}(N)$:

$$(\eta \cdot \sigma)(\eta' \cdot \sigma') = \eta \underbrace{(\sigma\eta'\sigma^{-1})}_{\in\rho(N)\ [\text{Claim 3}]} (\sigma\sigma') = \underbrace{(\eta\sigma\eta'\sigma^{-1})}_{\in\rho(N)} \underbrace{(\sigma\sigma')}_{\in\mathrm{Aut}(N)} \tag{4.1}$$

Conversely, we check that $\mathrm{Hol}(N) \subseteq \rho(N) \cdot \mathrm{Aut}(N)$. Let $\pi \in \mathrm{Hol}(N)$ and let us see that $\pi \in \rho(N) \cdot \mathrm{Aut}(N)$. If $\pi \in \mathrm{Hol}(N)$, then for every $\eta \in N$, $\pi\lambda(\eta)\pi^{-1} \in \lambda(N)$. Hence for every $\eta \in N$, there exists $\gamma(\eta) \in N$ determined by

$$\pi\lambda(\eta)\pi^{-1} = \lambda(\gamma(\eta)) \tag{4.2}$$

Since λ is injective, this $\gamma(\eta)$ is unique, so that the map $\gamma : N \to N$ can easily be seen to be an automorphism of N. For any $\eta \in N$:

$$\begin{aligned}
\pi(\eta) &= \pi(\eta \mathrm{e}_N) && (\text{def } \mathrm{e}_N)\\
&= \pi(\lambda(\eta)\mathrm{e}_N) && (\text{def } \lambda)\\
&= (\pi\lambda(\eta))(\mathrm{e}_N) && (\text{def } \circ)\\
&= (\lambda(\gamma(\eta))\pi)(\mathrm{e}_N) && (\text{by } (4.2))\\
&= \lambda(\gamma(\eta))(\pi(\mathrm{e}_N)) && (\text{def } \circ)\\
&= \gamma(\eta)\pi(\mathrm{e}_N) && (\text{def } \lambda)\\
&= \rho(\pi(\mathrm{e}_N)^{-1})(\gamma(\eta)) && (\text{def } \rho)\\
&= (\rho(\pi(\mathrm{e}_N)^{-1}) \circ \gamma)(\eta) && (\text{def } \circ)
\end{aligned}$$

Hence $\pi = \rho(\pi(\mathrm{e}_N)^{-1}) \circ \gamma \in \rho(N) \cdot \mathrm{Aut}(N)$.

Finally, it remains to show that $\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$.

On the one hand, since every automorphism is in particular a group morphism, it maps the identity element to itself. Thus $\mathrm{Aut}(N)$ fixes e_N. On the other hand, since the action of ρ is by (right) translation, only the identity leaves fixed elements, so that $\rho(N)$ is a regular subgroup of $\mathrm{Perm}(N)$. Hence the stabilizer of any element of N in $\rho(N)$ is trivial:

$$\forall\ \eta \in N,\ \mathrm{Stab}_{\rho(N)}(\eta) = \{\rho(\mu) \in \rho(N) :\ \eta\rho(\mu) = \eta\} = \{\rho(\mathrm{e}_N)\}.$$

Therefore, $\mathrm{Aut}(N) \cap \rho(N) = \{\mathrm{I}_N\}$, so that every element in $\mathrm{Hol}(N)$ is a product of an element of $\rho(N)$ and an element of $\mathrm{Aut}(N)$ in a unique way. Moreover, since $\mathrm{Aut}(N)$ normalizes $\rho(N)$, the formula of the product (4.1) leads to conclude that the product is, indeed, a semidirect product. □

4.3 Byott's theorem and formula

Here is **Byott's translation theorem**, from [By]. Recall that to count Hopf Galois structures on $L|K$ with normal closure $\widetilde{L}$ and $G = \mathrm{Gal}(\widetilde{L}|K)$, $G' = \mathrm{Gal}(\widetilde{L}|L)$, we seek regular subgroups of $\mathrm{Perm}(G/G')$ normalized by $\lambda_G(G)$.

Theorem 4.3.1 (Byott)**.** *Let $G' \leq G$ be finite groups, let $X = G/G'$ be the left cosets of G' in G and let N be an abstract group of order X. Then there is a bijection between the following sets:*

$$\mathcal{N} = \{\alpha : N \hookrightarrow \mathrm{Perm}(X) \textit{ monomorphism s.t. } \alpha(N) \textit{ is regular}\}$$
$$\mathcal{G} = \{\beta : G \hookrightarrow \mathrm{Perm}(N) \textit{ monomorphism s.t. } \beta(G') = \mathrm{Stab}_{\mathrm{Perm}(N)}(e_N)\}$$

Under this bijection, if $\alpha, \alpha' \in \mathcal{N}$ correspond to $\beta, \beta' \in \mathcal{G}$, respectively, then:

(i) $\alpha(N) = \alpha'(N)$ iff $\beta(G)$ and $\beta'(G)$ are conjugate by an element of $\mathrm{Aut}(N)$*;*

(ii) $\alpha(N)$ is normalized by $\lambda_G(G) \subseteq \mathrm{Perm}(X)$ iff $\beta(G)$ is contained in $\mathrm{Hol}(N)$*.*

Call a monomorphism $\alpha : N \hookrightarrow \mathrm{Perm}(X)$ such that $\alpha(N)$ is regular, a ***regular embedding****.*

Proof. It is based on the proof given in Th 7.3, page 57 [Ch1]. Let $\alpha \in \mathcal{N}$, that is, $\alpha(N)$ is a regular subgroup of $\mathrm{Perm}(X)$. Therefore, by reasoning as in Section 4.1, α induces a bijection:

$$\begin{array}{rcccl} a & : & N & \to & X \\ & & \eta & \mapsto & \alpha(\eta)(\overline{e}) \end{array}$$

where $\overline{e}$ is the left coset in $X = G/G'$ of e_G.

Observe that by definition of a:

$$a(\mathrm{e}_N) = \alpha(\mathrm{e}_N)(\overline{e}) = \mathrm{I}_{\mathrm{Perm}(X)}(\overline{e}) = \overline{e} \tag{4.3}$$

Again, by reasoning as in Section 4.1, the map a in turn yields an isomorphism:

$$\begin{array}{rcrcl} C(a) & : & \mathrm{Perm}(N) & \to & \mathrm{Perm}(X) \\ & & \pi & \mapsto & a \circ \pi \circ a^{-1} \end{array}$$

Let $\lambda_G : G \to \mathrm{Perm}(X)$, $\lambda_N : N \to \mathrm{Perm}(N)$ be the left translation maps. Then

$$C(a)^{-1} \circ \lambda_G : G \to \mathrm{Perm}(N)$$

is an embedding, since it is the composition of an embedding and an isomorphism. We show that it is in $\mathcal{G}$: it remains to show that

$$(C(a)^{-1} \circ \lambda_G)(G') = \mathrm{Stab}_{\mathrm{Perm}(N)}(\mathrm{e}_N).$$

Indeed, for every $\sigma \in G$,

$$\begin{array}{rcll} (C(a)^{-1} \circ \lambda_G)(\sigma)(\mathrm{e}_N) = \mathrm{e}_N & \Leftrightarrow & (C(a)^{-1}(\lambda_G(\sigma)))(\mathrm{e}_N) = \mathrm{e}_N & (\text{def } \circ) \\ & \Leftrightarrow & a^{-1}(\lambda_G(\sigma)(a(\mathrm{e}_N))) = \mathrm{e}_N & (\text{def } C(a)) \\ & \Leftrightarrow & \lambda_G(\sigma)(a(\mathrm{e}_N)) = a(\mathrm{e}_N) & (a \circ a^{-1} = \mathrm{I}_X) \\ & \Leftrightarrow & \lambda_G(\sigma)(\overline{e}) = \overline{e} & (\text{by } (4.3)) \\ & \Leftrightarrow & \overline{\sigma e} = \overline{e} & (\text{def } \lambda_G) \\ & \Leftrightarrow & \overline{\sigma} = \mathrm{e}_G G' & (\text{def } \overline{e}) \\ & \Leftrightarrow & \sigma \in G' & \end{array}$$

so that $C(a)^{-1} \circ \lambda_G \in \mathcal{G}$, as desired.

The bijection we seek from $\mathcal{N}$ to $\mathcal{G}$ is the following:

$$\begin{array}{rcrcl} \Phi & : & \mathcal{N} & \to & \mathcal{G} \\ & & \alpha & \mapsto & C(a)^{-1} \circ \lambda_G \end{array}$$

<u>Claim 1</u>: $C(a)^{-1} \circ \alpha = \lambda_N$, so that $\alpha = C(a) \circ \lambda_N$.

Indeed, for every $\eta, \mu \in N$,

$$\begin{array}{rcll} (C(a)^{-1} \circ \alpha)(\eta)(\mu) & = & (C(a)^{-1}(\alpha(\eta)))(\mu) & (\text{def } \circ) \\ & = & (a^{-1} \circ \alpha(\eta))(a(\mu)) & (\text{def } C(a)) \\ & = & (a^{-1} \circ \alpha(\eta))(\alpha(\mu)(\overline{e})) & (\text{def } a) \\ & = & a^{-1}((\alpha(\eta)\alpha(\mu))(\overline{e})) & (\text{def } \circ) \\ & = & a^{-1}(\alpha(\eta\mu)(\overline{e})) & (\alpha \text{ group morp}) \\ & = & a^{-1}(a(\eta\mu)) & (\text{def } a) \\ & = & \eta\mu & (a^{-1} \circ a = \mathrm{I}_N) \\ & = & \lambda_N(\eta)(\mu) & (\text{def } \lambda_N) \end{array}$$

so that $C(a)^{-1} \circ \alpha = \lambda_N$, as desired.

Now, we define the inverse Ψ of Φ. If $\beta : G \to \mathrm{Perm}(N)$ is in $\mathcal{G}$, then by definition $\beta(G') = \mathrm{Stab}_{\mathrm{Perm}(N)}(\mathrm{e}_N)$. Thus β yields a bijection:

$$\begin{array}{ccccc} b & : & X & \to & N \\ & & \overline{\sigma} & \mapsto & \beta(\sigma)(\mathrm{e}_N) \end{array}$$

Indeed,

- Well-defined: given $\overline{\sigma}, \overline{\tau} \in X$,

$$\begin{array}{rcll} b(\overline{\sigma}) = b(\overline{\tau}) & \Leftrightarrow & \beta(\sigma)(\mathrm{e}_N) = \beta(\tau)(\mathrm{e}_N) & (\text{def } b) \\ & \Leftrightarrow & (\beta(\tau)^{-1} \circ \beta(\sigma))(\mathrm{e}_N) = (\beta(\tau)^{-1} \circ \beta(\tau))(\mathrm{e}_N) & (\text{by (1) below}) \\ & \Leftrightarrow & (\beta(\tau)^{-1} \circ \beta(\sigma))(\mathrm{e}_N) = \mathrm{e}_N & (\text{by (2) below}) \\ & \Leftrightarrow & (\beta(\tau^{-1}) \circ \beta(\sigma))(\mathrm{e}_N) = \mathrm{e}_N & (\text{by (3) below}) \\ & \Leftrightarrow & \beta(\tau^{-1}\sigma)(\mathrm{e}_N) = \mathrm{e}_N & (\text{by (4) below}) \\ & \Leftrightarrow & \tau^{-1}\sigma \in G' & (\beta \in \mathcal{G}, \text{ def } \mathcal{G}) \\ & \Leftrightarrow & \sigma \in \tau G' & (\tau^{-1} \circ \tau = \mathrm{e}_G) \\ & \Leftrightarrow & \overline{\sigma} = \overline{\tau} & (\overline{\tau} = \tau G') \end{array}$$

where:

(1) $\beta(\tau) \in \mathrm{Perm}(N)$,

(2) $\beta(\tau)^{-1} \circ \beta(\tau) = \mathrm{I}_N$,

(3) $\beta(\tau)^{-1} = \beta(\tau^{-1})$,

(4) β is a group morphism.

- Bijective: injectivity follows from the previous computation and since $|X| = |N|$ holds by assumption, it is bijective.

Observe that by definition of b:

$$b(\overline{e}) = \beta(\mathrm{e}_G)(\mathrm{e}_N) = \mathrm{I}_{\mathrm{Perm}(N)}(\mathrm{e}_N) = \mathrm{e}_N \tag{4.4}$$

Hence, by reasoning as in Section 4.1, the map b induces an isomorphism:

$$\begin{array}{ccccc} C(b) & : & \mathrm{Perm}(X) & \to & \mathrm{Perm}(N) \\ & & \pi & \mapsto & b \circ \pi \circ b^{-1} \end{array}$$

Then $C(b)^{-1} \circ \lambda_N : N \to \mathrm{Perm}(X)$ is a regular embedding, since it is the composition of a regular embedding and an isomorphism. Thus it is in $\mathcal{N}$.

The bijection we seek from $\mathcal{G}$ to $\mathcal{N}$ is the following:

$$\begin{array}{ccccc} \Psi & : & \mathcal{G} & \to & \mathcal{N} \\ & & \beta & \mapsto & C(b)^{-1} \circ \lambda_N \end{array}$$

Claim 2: $C(b)^{-1} \circ \beta = \lambda_G$, so that $\beta = C(b) \circ \lambda_G$.

Indeed, for every $\sigma \in G$, $\overline{\tau} \in X$,

$$\begin{aligned}
(C(b)^{-1} \circ \beta)(\sigma)(\overline{\tau}) &= (C(b)^{-1}(\beta(\sigma)))(\overline{\tau}) && (\text{def } \circ)\\
&= (b^{-1} \circ \beta(\sigma))(b(\overline{\tau})) && (\text{def } C(b))\\
&= (b^{-1} \circ \beta(\sigma))(\beta(\tau)(\mathrm{e}_N)) && (\text{def } b)\\
&= b^{-1}((\beta(\sigma)\beta(\tau))(\mathrm{e}_N)) && (\text{def } \circ)\\
&= b^{-1}(\beta(\sigma\tau)(\mathrm{e}_N)) && (\beta \text{ group morp})\\
&= b^{-1}(b(\overline{\sigma\tau})) && (\text{def } b)\\
&= \overline{\sigma\tau} && (b^{-1} \circ b = \mathrm{I}_X)\\
&= \lambda_G(\sigma)(\overline{\tau}) && (\text{def } \lambda_G)
\end{aligned}$$

<u>Claim 3</u>: Ψ and Φ are inverse maps.

- $\Psi \circ \Phi = \mathrm{I}_{\mathcal{N}}$: for a given $\alpha \in \mathcal{N}$, let $\beta := \Phi(\alpha) = C(a)^{-1} \circ \lambda_G$. Then $b = a^{-1}$: for every $\overline{\sigma} \in X$,

$$\begin{aligned}
b(\overline{\sigma}) &= \beta(\sigma)(\mathrm{e}_N) && (\text{def } b)\\
&= (C(a)^{-1}(\lambda_G(\sigma)))(\mathrm{e}_N) && (\text{def } \beta)\\
&= (a^{-1} \circ \lambda_G(\sigma))(a(\mathrm{e}_N)) && (\text{def } C(a))\\
&= (a^{-1} \circ \lambda_G(\sigma))(\overline{e}) && (\text{by } (4.3))\\
&= a^{-1}(\lambda_G(\sigma)(\overline{e})) && (\text{def } \circ)\\
&= a^{-1}(\overline{\sigma e}) && (\text{def } \lambda_G)\\
&= a^{-1}(\overline{\sigma}) && (\text{def } \overline{e})
\end{aligned}$$

Therefore, it follows that $\Psi \circ \Phi = \mathrm{I}_{\mathcal{N}}$:

$$\begin{aligned}
\Psi(\Phi(\alpha)) &= \Psi(\beta) && (\text{def } \beta)\\
&= C(b)^{-1} \circ \lambda_N && (\text{def } \Psi)\\
&= C(b^{-1}) \circ \lambda_N && (C(b)^{-1} = C(b^{-1}))\\
&= C(a) \circ \lambda_N && (b = a^{-1})\\
&= \alpha && (\text{by Claim 1})
\end{aligned}$$

- $\Phi \circ \Psi = \mathrm{I}_{\mathcal{G}}$: for a given $\beta \in \mathcal{G}$, let $\alpha := \Psi(\beta) = C(b)^{-1} \circ \lambda_N$. Then $a = b^{-1}$: for every $\eta \in N$,

$$\begin{aligned}
a(\eta) &= \alpha(\eta)(\overline{e}) && (\text{def } a)\\
&= (C(b)^{-1}(\lambda_N(\eta)))(\overline{e}) && (\text{def } \alpha)\\
&= (b^{-1} \circ \lambda_N(\eta))(b(\overline{e})) && (\text{def } C(b))\\
&= (b^{-1} \circ \lambda_N(\eta))(\mathrm{e}_N) && (\text{by } (4.4))\\
&= b^{-1}(\lambda_N(\eta)(\mathrm{e}_N)) && (\text{def } \circ)\\
&= b^{-1}(\eta \mathrm{e}_N) && (\text{def } \lambda_N)\\
&= b^{-1}(\eta) && (\text{def } \mathrm{e}_N)
\end{aligned}$$

Therefore, it follows that $\Phi \circ \Psi = \mathrm{I}_{\mathcal{G}}$:

$$\begin{aligned}
\Phi(\Psi(\beta)) &= \Phi(\alpha) && (\text{def } \alpha)\\
&= C(a)^{-1} \circ \lambda_G && (\text{def } \Phi)\\
&= C(a^{-1}) \circ \lambda_G && (C(a)^{-1} = C(a^{-1}))\\
&= C(b) \circ \lambda_G && (a = b^{-1})\\
&= \beta && (\text{by Claim 2})
\end{aligned}$$

Now, let us prove (i). We have to see that $\alpha(N) = \alpha'(N)$ if and only if $\beta(G)$ and $\beta'(G)$ are conjugate by an element of $\mathrm{Aut}(N)$.

Notice that by definition of $\mathcal{N}$,

$$\alpha(N) = \alpha'(N) \;\Leftrightarrow\; \gamma := \alpha^{-1} \circ \alpha' \in \mathrm{Aut}(N \;\Leftrightarrow\; \alpha' = \alpha \circ \gamma.$$

We have seen that every $\alpha \in \mathcal{N}$ yields a $\beta = \Phi(\alpha) = C(a)^{-1} \circ \lambda_G \in \mathcal{G}$. So if we replace α by $\alpha' = \alpha\gamma$, with $\gamma \in \mathrm{Aut}(N)$, we obtain:

$$C(a\gamma)^{-1} = C(\gamma)^{-1} C(a)^{-1} : \mathrm{Perm}(X) \to \mathrm{Perm}(N) \tag{4.5}$$

where since $\gamma \in \mathrm{Aut}(N)$, then $C(\gamma)$ is defined as:

$$\begin{aligned}
C(\gamma) \;:\; \mathrm{Perm}(N) &\to \mathrm{Perm}(N)\\
\pi &\mapsto \gamma \circ \pi \circ \gamma^{-1}
\end{aligned}$$

Indeed, for every $\pi \in \mathrm{Perm}(X)$,

$$\begin{aligned}
C(a\gamma)^{-1}(\pi) &= (a\gamma)^{-1} \circ \pi \circ (a\gamma) && (\text{def } C(a\gamma))\\
&= \gamma^{-1} \circ (a^{-1}\pi a) \circ \gamma && ((f \circ g)^{-1} := g^{-1} \circ f^{-1})\\
&= C(\gamma)^{-1}(a^{-1}\pi a) && (\text{def } C(\gamma))\\
&= C(\gamma)^{-1}(C(a)^{-1}(\pi)) && (\text{def } C(a))\\
&= (C(\gamma)^{-1}C(a)^{-1})(\pi) && (\text{def } \circ)
\end{aligned}$$

Thus β and β' are embeddings which are conjugate by an element in $\mathrm{Aut}(N)$:

$$\begin{aligned}
\beta' &= \Phi(\alpha') && (\text{by construction})\\
&= \Phi(\alpha\gamma) && (\text{def } \alpha')\\
&= C(a\gamma)^{-1} \circ \lambda_G && (\text{def } \Phi)\\
&= C(\gamma)^{-1} \circ C(a)^{-1} \circ \lambda_G && (\text{by } (4.5))\\
&= C(\gamma)^{-1} \circ \beta && (\text{def } \beta)
\end{aligned}$$

Finally, let us prove (ii). Let $\alpha(N)$ be normalized by $\lambda_G(G) \subseteq \mathrm{Perm}(X)$ and let us see that $\beta(G) \subseteq \mathrm{Hol}(N)$, that is, $\beta(G)$ normalizes $\lambda_N(N) \subseteq \mathrm{Perm}(N)$:

$$\beta(\sigma)\lambda_N(\eta)\beta(\sigma^{-1}) \in \lambda_N(N).$$

Indeed, if $\alpha(N)$ is normalized by $\lambda_G(G)$, then for every $\sigma \in G$, $\eta \in N$,

$$\lambda_G(\sigma)\alpha(\eta)\lambda_G(\sigma^{-1}) \in \alpha(N) \subseteq \mathrm{Perm}(X).$$

Mapping to $\mathrm{Perm}(N)$ via $C(a)^{-1}$, we have:

$$C(a)^{-1}(\lambda_G(\sigma)\alpha(\eta)\lambda_G(\sigma^{-1})) \in C(a)^{-1}(\alpha(N)) \subseteq \mathrm{Perm}(N).$$

Observe that for every $\sigma \in G$, $\eta \in N$,

$$\begin{aligned}
\underbrace{C(a)^{-1}(\lambda_G(\sigma)\alpha(\eta)\lambda_G(\sigma^{-1}))}_{\in C(a)^{-1}(\alpha(N))} &\underset{(1)}{=} C(a)^{-1}(\lambda_G(\sigma))\ C(a)^{-1}(\alpha(\eta))\ C(a)^{-1}(\lambda_G(\sigma^{-1}))\\
&\underset{(2)}{=} C(a)^{-1}(\lambda_G(\sigma))\ \lambda_N(\eta)\ C(a)^{-1}(\lambda_G(\sigma^{-1}))\\
&\underset{(3)}{=} \underbrace{\beta(\sigma)\ \lambda_N(\eta)\ \beta(\sigma^{-1})}_{\in C(a)^{-1}(\alpha(N))}
\end{aligned}$$

where:

(1) $C(a)^{-1}$ is a group morphism,

(2) by Claim 1,

(3) def β.

Hence, by the previous computation and $\beta = \Phi(\alpha) = C(a)^{-1} \circ \lambda_G$, we conclude that $\beta(G)$ normalizes $\lambda_N(N)$:

$$\beta(\sigma)\lambda_N(\eta)\beta(\sigma^{-1}) \in C(a)^{-1}(\alpha(N)) = \lambda_N(N).$$

Conversely, let $\beta(G)$ be such that it normalizes $\lambda_N(N) \subseteq \mathrm{Perm}(N)$ and let us see that $\alpha(N)$ is normalized by $\lambda_G(G)$, that is:

$$\lambda_G(\sigma)\alpha(\eta)\lambda_G(\sigma^{-1}) \in \alpha(N).$$

Indeed, if $\beta(G)$ normalizes $\lambda_N(N)$, then by definition, for every $\sigma \in G$, $\eta \in N$,

$$\beta(\sigma)\lambda_N(\eta)\beta(\sigma^{-1}) \in \lambda_N(N) \subseteq \mathrm{Perm}(N).$$

Mapping to $\mathrm{Perm}(X)$ via $C(b)^{-1}$, we have:

$$C(b)^{-1}(\beta(\sigma)\lambda_N(\eta)\beta(\sigma^{-1})) \in C(b)^{-1}(\lambda_N(N)) \subseteq \mathrm{Perm}(X).$$

Observe that for every $\sigma \in G$, $\eta \in N$,

$$\begin{aligned}
\underbrace{C(b)^{-1}(\beta(\sigma)\lambda_N(\eta)\beta(\sigma^{-1}))}_{\in C(b)^{-1}(\lambda_N(N))} &\underset{(1)}{=} C(b)^{-1}(\beta(\sigma))\ C(b)^{-1}(\lambda_N(\eta))\ C(b)^{-1}(\beta(\sigma^{-1}))\\
&\underset{(2)}{=} C(b)^{-1}(\beta(\sigma)\ \alpha(\eta)\ C(b)^{-1}(\beta(\sigma^{-1})\\
&\underset{(3)}{=} \underbrace{\lambda_G(\sigma)\ \alpha(\eta)\lambda_G(\sigma^{-1})}_{\in C(b)^{-1}(\lambda_N(N))}
\end{aligned}$$

where:

(1) $C(a)^{-1}$ is a group morphism,

(2) def α,

(3) by Claim 2.

Hence, by the previous computation and $\alpha = \Psi(\beta) = C(b)^{-1} \circ \lambda_N$, we conclude that $\alpha(N)$ is normalized by $\lambda_G(G)$:

$$\lambda_G(\sigma)\alpha(\eta)\lambda_G(\sigma^{-1}) \in C(b)^{-1}(\lambda_N(N)) = \alpha(N).$$

□

As a corollary to the preceding theorem, Byott obtains the following **formula** to count Hopf Galois structures.

Corollary 4.3.2. *Let $L|K$ be a separable field extension of degree g, $\widetilde{L}$ its Galois closure, $G = \mathrm{Gal}(\widetilde{L}|K)$ and $G' = \mathrm{Gal}(\widetilde{L}|L)$. Let N be an abstract group of order g. The number $a(N, L|K)$ of Hopf Galois structures of type N on $L|K$ is given by the following formula:*

$$a(N, L|K) = \frac{|\operatorname{Aut}(G, G')|}{|\operatorname{Aut}(N)|}\, b(N, G, G')$$

where $\operatorname{Aut}(G, G')$ denotes the group of automorphisms of G taking G' to G', $\operatorname{Aut}(N)$ denotes the group of automorphisms of N and $b(N, G, G')$ denotes the number of subgroups G^* of $\operatorname{Hol}(N)$ such that there is an isomorphism from G to G^* taking G' to the stabilizer of e_N in G^*.

Proof. It is based on the proof given in Prop 1, page 3219 [By]. By the previous theorem, there is a bijection between the following sets:

$$\mathcal{N}_0 = \{\alpha : N \hookrightarrow \operatorname{Perm}(X) \text{ s.t. } \alpha(N) \text{ regular and normalized by } \lambda_G(G)\}$$
$$\mathcal{G}_0 = \{\beta : G \hookrightarrow \operatorname{Hol}(N) \subseteq \operatorname{Perm}(N) \text{ s.t. } \beta(G') = \operatorname{Stab}_{\beta(G)}(\mathrm{e}_N)\}$$

Now, if $\alpha \in \mathcal{N}_0$, then $\alpha(N)$ is one of the subgroups N' that gives a Hopf Galois structure counted by $a(N, L|K)$. In fact, all such N' arise this way, and $\alpha, \alpha' \in \mathcal{N}_0$ give the same group N' if and only if $\alpha^{-1} \circ \alpha' \in \operatorname{Aut}(N)$. Thus

$$|\mathcal{N}_0| = |\operatorname{Aut}(N)|\, a(N, L|K).$$

A similar reasoning shows that $|\mathcal{G}_0| = |\operatorname{Aut}(G, G')|\, b(N, G, G')$. Since there is a bijection between $\mathcal{N}_0$ and $\mathcal{G}_0$, that finishes the proof.

□

Chapter 5

Algorithms

In this thesis we present two algorithms I have designed written in the computational algebra system Magma that give all Hopf Galois structures on separable field extensions of degree up to eleven and thirty-one, respectively, and two important properties of those. The code as well as outputs and tables for each degree may be found in our web page [C-S4].

In what follows, let $L|K$, g, $\widetilde{L}$, G and G' be as in Section 3.2. We know there is a monomorphism $\lambda_G : G \to \mathrm{Perm}(G/G')$ that identifies G with $\lambda_G(G)$, where $\lambda_G(G)$ is a transitive subgroup of $\mathrm{Perm}(G/G') \cong S_g$ which is determined up to conjugacy, that is, a transitive group of degree g. Furthermore, if we enumerate the left cosets G/G' starting with the one containing e_G, then $\lambda_G(G')$ is equal to the stabilizer of 1 in G. Therefore the Hopf Galois character of $L|K$ depends only on G and λ_G by Greither-Paregis' theorem.

These transitive groups have been classified in [Hu] up to $g = 31$ and are included in the database of Magma. We shall denote by gTk the k-th transitive group of degree g given by Magma as `TransitiveGroup(g,k)`. Notice that if $|gTk| = g$, then gTk is a regular group. Moreover, if two regular subgroups of S_g are isomorphic, they are conjugate.

5.1 Code structure

Both algorithms share a common code structure, which consists of two functions:

- **Main function**: *HopfGalois(g)*. It computes all the information needed and prints nothing.

  1. Computation of two previous parameters;
  2. Determination of Hopf Galois structures;
  3. Property 1: determine if the Galois correspondence is bijective;
  4. Property 2: give a partition of Hopf algebras in isomorphism classes.

- **Descriptive function**: *HGdescription(g).* It computes nothing important and prints everything with different levels of detail.

There are two main differences between the first and the second algorithm:

1. There is an auxiliary funtion in the second algorithm that determines several sets of automorphisms which are not necessary in the first one.
2. Determination of Hopf Galois structures is performed via Greither-Pareigis' theorem in the first algorithm and via Byott's theorem in the second.

5.2 First algorithm

Input: The degree g of a separable field extension.

Step 1 Given a transitive group G of degree g and a type of regular subgroups N of $\mathrm{Perm}(G/G') \cong \mathrm{S}_g$, run over the conjugacy class of N in S_g and determine whether N is normalized by G. In the affirmative case, check if the centralizer of N in S_g is contained in G. If so, the Hopf Galois structure determined by N is almost classically Galois.

Step 2 For each transitive group G of degree g and $G' = \mathrm{Stab}_G(\mathrm{e}_G)$, determine the number $interfields(G)$ of subgroups of G containing G', that is, by the fundamental theorem of classical Galois theory, the number of intermediate fields of the extension $L|K$.

Step 3 For each pair (G, N) determined in Step 1, compute the number $subGst(N)$ of G-stable subgroups of N, ie, subgroups of N normalized by G. That is to say, compute the cardinality of the image of the map $\mathcal{F}_H$ in Theorem 2.4.7 for the Hopf Galois structure given by N. Check if this number equals $interfields(G)$, that is, if the Galois correspondence is bijective.

Step 4 For each pair (G, N_1), (G, N_2), with $N_1 \cong N_2$ and $subGst(N_1) = subGst(N_2)$, check if N_1 and N_2 are G-isomorphic, ie, if the corresponding Hopf algebras are isomorphic. We obtain the set of all isomorphisms by composing the isomorphism from N_1 to N_2 given by Magma with each automorphism of N_2. We use that for a regular subgroup N of S_g, the automorphism group of N is isomorphic to the stabilizer of 1 in the holomorph of N. We run over this set of isomorphisms and check for each element if it is a G-isomorphism until the answer is affirmative or the set is exhausted.

Output: All regular subgroups N of S_g giving a Hopf Galois structure, hence it determines explicitly all of them up to degree 11. In the vector which collects such N's we have added a numbering variable in order to identify each of them with an integer number. This numeration is respected all allong the program so that, once the $N's$ have been computed in Step 1, we can easily know the properties of the corresponding Hopf Galois structure by searching the assigned number. This greatly simplifies the reading and interpretation of results.

5.3 Second algorithm

The function Automorphisms

Given a pair of integers (g, k), this function returns the group $\mathrm{Aut}(G)$ of automorphisms of the group $G = gTk$ and the group $\mathrm{Aut}(G, G')$ of automorphisms of G sending G' to itself. In order to obtain the latter, the function uses the permutation representation of $\mathrm{Aut}(G)$ to obtain a group P of permutations isomorphic to $\mathrm{Aut}(G)$. It then computes the set `stabims` of images of G' under $\mathrm{Aut}(G)$ and the action of the generators of $\mathrm{Aut}(G)$ on this set. This gives the embedding `act` of P into Sym(`stabims`) and then the preimage of the stabilizer of 1 in Sym(`stabims`) is a subgroup Q of P corresponding to $\mathrm{Aut}(G, G')$ by the permutation representation.

The main function

Input: The degree g of a separable field extension.

Step 0 We order each regular subgroup N of S_g so that $n_j(1) = j$, for $j \in \{1, \dots, g\}$, and compute its embedding $\lambda_N(N)$ in S_g.

Step 1 Given a transitive group G of degree g and a type of regular subgroups N of S_g, we determine the subgroups G^* of $H := \mathrm{Hol}(N)$ which are isomorphic to G and transitive and such that the stabilizer of 1 in G^* is isomorphic to the stabilizer G' of 1 in G.

Step 2 For each G^* obtained in Step 1, we look for an isomorphism from G^* to G sending $\mathrm{Stab}(G^*, 1)$ to G'. Let f be the isomorphism from G^* to G provided by Magma. If $|G| = g$, then G' is trivial and f will do. Otherwise, we compare $f(\mathrm{Stab}(G^*, 1))$ to the images of G' by all automorphisms of G. If, for some $a \in \mathrm{Aut}\, G$, we have $f(\mathrm{Stab}(G^*, 1)) = a(G')$, then $h := f \circ a^{-1}$ is the wanted isomorphism. Then $\beta = h^{-1}$ is the embedding β as in Byott's Theorem 4.3.1.

Step 3 We order $T := G/G'$ so that $t_j(1) = j$, for $j \in \{1, \dots, g\}$.

Step 4 For each pair (G^*, h) obtained in Step 2, we compute the whole set of isomorphisms from G^* to G sending $\mathrm{Stab}(G^*, 1)$ to G' by composing h with each element in $\mathrm{Aut}(G, G')$. We obtain then all β's from G to $\mathrm{Hol}(N)$ as in Byott's Theorem. For each such β we determine the corresponding $\alpha(N)$ as in the proof of Byott's Theorem. Moreover, we compute $\lambda_G(G)$ for those $G's$ for which there is such a β.

Output: All regular subgroups of S_g isomorphic to N and normalized by $\lambda_G(G)$, which correspond with all Hopf Galois structures on a separable field extension up to degree 31.

The functions regarding properties

We further determine those Hopf Galois structures for which the Galois correspondence is bijective and partition the set of Hopf Galois structures of a given type in Hopf algebra isomorphism classes with an optimized version of the first algorithm. We will not describe them with many details since they have already been explained in the previous section and they are essentially the same but with some optimizations.

Previously we compute the embedding $\lambda_G(G)$ in S_g induced by the action of G by left translation on the set T of left cosets of G modulo G' accordingly with the ordering of T in Step 3. Taking into account [C-S1] Proposition 6, we know that an almost classically Galois structure lies alone in its isomorphism class. Hence, we put these apart when performing the partition in Hopf algebra isomorphism classes. Furthermore we determine the Hopf Galois structures for which the Galois correspondence is bijective in a more effective way.

5.4 Main computational and theoretical results

We present a compendium of the computational results of the first and second algorithm in Tables 5.1 and 5.2, respectively. In them, we give for every degree g:

- The two previous parameters, which are: the total number of transitive groups of degree g and the number Max of those whose order does not exceed the order of the holomorphs of all regular subgroups of S_g (ie, the groups of order exactly g). We can ensure that over Max there are no Hopf Galois structures since this just happens whenever G is embedded in $\mathrm{Hol}(N)$ (see the proof of Corollary 4.3.2);

- The number of possible types of Hopf Galois structures;

- The total number of Hopf Galois structures and the number of almost classically Galois ones;

- The number of Hopf Galois structures with bijective Galois correspondence and the number of those which are not almost classically Galois;

- The number of Hopf algebra isomorphism classes in which the Hopf Galois structures are partitioned (which correspond to G-isomorphism classes of the corresponding regular groups N) and the number of those for Galois extensions (ie, when $G' = \mathrm{Gal}(\widetilde{L}|L)$ is trivial);

- And finally, the execution time in seconds and the memory used in megabytes (except for $g = 16$ which could not be computed at once).

We highlight the richness of the results obtained for extensions of degree 8, 16, 24 and 27.

Table 5.1: Main results of the first algorithm

Degree	**Transitive Groups**		**Types**	**HG struct.**		**BC**		***G*-iso**		**Execution time** (s)	**Memory used** (MB)
	Total	Max		Total	a-c	Total	not a-c	Total	Galois		
2	1	1	1	1	1	1	0	1	1	≈ 1	≈ 10
3	2	2	1	2	2	2	0	2	1	≈ 1	≈ 10
4	5	5	2	10	6	7	1	10	6	≈ 1	≈ 11
5	5	3	1	3	3	3	0	3	1	≈ 1	≈ 11
6	16	10	2	15	7	9	2	13	6	≈ 2	≈ 11
7	7	4	1	4	4	4	0	4	1	≈ 1	≈ 11
8	50	48	5	348	74	147	73	262	111	≈ 17	≈ 40
9	34	26	2	38	26	28	2	33	8	≈ 10	≈ 16
10	45	21	2	27	11	17	6	23	6	≈ 160	≈ 45
11	8	4	1	4	4	4	0	4	1	≈ 90	≈ 160

Table 5.2: Main results of the second algorithm

Degree	**Transitive Groups**		**Types**	**HG struct.**		**BC**		***G*-iso**		**Execution**	**Memory**
	Total	Max		Total	a-c	Total	not a-c	Total	Galois	**time** (s)	**used** (MB)
12	301	129	5	249	56	81	25	165	48	≈ 18	≈ 31
13	9	6	1	6	6	6	0	6	1	≈ 1	≈ 18
14	63	25	2	32	14	19	5	26	6	≈ 2	≈ 22
15	104	11	1	8	8	8	0	8	1	≈ 1	≈ 22
16	1954	1906	14	49913	2636	9331	6695	26769	6717	–	–
17	10	5	1	5	5	5	0	5	1	≈ 1	≈ 30
18	983	528	5	881	123	253	130	525	79	≈ 206	≈ 113
19	8	6	1	6	6	6	0	6	1	≈ 1	≈ 26
20	1117	170	5	434	79	156	77	266	55	≈ 57	≈ 48
21	164	26	2	78	22	46	24	42	8	≈ 5	≈ 26
22	59	18	2	36	14	19	5	26	6	≈ 5	≈ 26
23	7	4	1	4	4	4	0	4	1	≈ 1	≈ 18
24	25000	9738	15	14908	844	2682	1838	8353	1896	≈ 9730	≈ 1327
25	211	90	2	106	70	74	4	82	12	≈ 32	≈ 175
26	96	37	2	58	22	35	13	46	6	≈ 12	≈ 27
27	2392	1547	5	6699	766	1100	334	2030	547	≈ 5375	≈ 500
28	1854	214	4	388	84	143	59	256	40	≈ 63	≈ 33
29	8	6	1	6	6	6	0	6	1	≈ 1	≈ 22
30	5712	483	4	479	99	197	98	373	36	≈ 113	≈ 40
31	12	8	1	8	8	8	0	8	1	≈ 1	≈ 22

Finally, we summarize the main theoretical results we have obtained from the collected data. For more details, one may read our three papers [C-S1], [C-S2] and [C-S3].

- **First algorithm**: notice that all integer numbers $g \in \{2, \dots, 11\}$, except $g = 8$, are of one of the forms p, p^2 or $2p$, with p prime.

  - The prime case has been considered by Byott [By], Childs [Ch2] and Pareigis [Pa].
  - We have classified Hopf Galois structures in the cases $2p$ and p^2 [C-S1]. In the case p^2, we prove that a separable extension may have only one type of Hopf Galois structures (either cyclic C_{p^2} or product of cyclics $\mathrm{C}_p \times \mathrm{C}_p$) and determine those of cyclic type. In the case $2p$, we determine all Hopf Galois structures.
  - We also have a property for almost classical structures: they live alone in their Hopf algebra isomorphism class.

- **Second algorithm**: notice that integer numbers $g \in \{12, \dots, 31\}$ are of the form p, $2p$, p^2, p^3, $2p^2$, $4p$... with p an odd prime.

  - The cases $p,\ 2p,\ p^2$ have already been studied.
  - We have classified Hopf Galois structures in the case p^3, and more generally the case p^n in [C-S2]. We prove that if a separable field extension of odd prime power degree has a Hopf Galois structure of cyclic type, then it has no other of noncyclic type, and give a more precise description of those of cyclic type.

    In the case p^3, there are five types: three Abelian ones (C_{p^3}, $\mathrm{C}_{p^2} \times \mathrm{C}_p$, $\mathrm{C}_p \times \mathrm{C}_p \times \mathrm{C}_p$) and two non Abelian (the Heisenberg group H_p and the group G_p defined in Section 3.2 in [C-S2]). Moreover, we give the possible sets of Hopf Galois structure types and determine exactly the number of those of cyclic type.

    There were some previous results by Zenouz (Galois case) in [Ze] and Kohl (radical extensions) in [Ko1].
  - We have also classified those of the case $2p^2$, and more generally the case $2p^n$ in [C-S3]. For separable field extensions of degree $2p^n$, we prove that the occurrence of some type of Hopf Galois structure may either imply or exclude the occurrence of some other type. In particular, for a separable field extensions of degree $2p^2$, we determine exactly the possible sets of Hopf Galois structure types.

    Now, we are working on counting Hopf Galois structures for Galois extensions of degree $2p^2$.
  - The case $4p$ has been studied by Kohl (Galois case) in [Ko2].
  - And there is still a lot of work to do.

5.5 Conclusions

Thanks to this computational approach, we have been able to:

1. **Obtain explicit computations**: our algorithms compute explicitly all Hopf Galois structures on a separable extension of a given degree and determine two important properties.

2. **Develop intuition**: the obtained results provide a very natural way of developing intuition about this topic since we can 'touch' the objects we are studying.

3. **Prove new theoretical results**: we can observe patterns hidden in tables that allow us to obtain new results.

Although the second algorithm goes further in terms of computations, it is worth pointing out the importance of the first one as a:

- **Precursor**: it has been very useful to have the full skeleton of the code together with the properties and the descriptive function. It has involved a great time and effort saving.

- **Reference**: it has been absolutely necessary in order to have something right to compare the new results with.

Moreover, the first algorithm is still relevant now since it is the best one for computing degree 8 with a very significant difference, both in terms of execution time and memory used. This happens because there are some groups of order 8 with many automorphisms (for instance, $\mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$) and the first algorithm does not take them into account (Greither-Pareigis's theorem cares about regular subgroups) but the second does (Byott's theorem needs $\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$).

Bibliography

[Bo] N. Bourbaki, *Algebra I*, Springer, 1989. 19, 30

[By] N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions.* Communications in Algebra 24 (1996), 3217-3228. Corrigendum, ibid., 3705. 53, 59, 67

[Ch-Sw] S. U. Chase and M. Sweedler, *Hopf algebras and Galois Theory.* Lecture Notes in Mathematics, Vol. 97, Springer Verlag, 1969. 22, 23

[Ch1] L. N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory.* American Mathematical Society, 2000. 21, 30, 36, 37, 38, 42, 49, 51, 53

[Ch2] L. N. Childs, *On the Hopf Galois theory for separable field extensions.* Communications in Algebra 17 (1989), 809-825. 67

[C-R-V] T. Crespo, A. Rio and M. Vela, *On the Galois correspondence theorem in separable Hopf Galois theory.* Publicacions Matemàtiques 60 (2016), 221-234. 48

[C-S1] T. Crespo and M. Salguero, *Computation of Hopf Galois structures on low degree separable extensions and classification of those of degree p^2 and $2p$.* To appear in Publicacions Matemàtiques; arXiv:1802.09948. 2, 64, 67

[C-S2] T. Crespo and M. Salguero, *Hopf Galois structures on separable field extensions of odd prime power degree.* Journal of Algebra 519 (2019), 424-439. 2, 67

[C-S3] T. Crespo and M. Salguero, *Computation of Hopf Galois structures on separable extensions and classification of those for degree twice an odd prime power.* Preprint: arXiv:1904.05174. 3, 67

[C-S4] T. Crespo and M. Salguero, web page: *Algorithmic Hopf Galois theory: Magma code, tables and results.* Electronic adress:
https://sites.google.com/view/algorithmichg/ 61

[D-A-N] S. Dăscălescu, C. Năstăsescu and Ş. Raianu, *Hopf algebras: an introduction*, Marcel Dekker, 2001.

[G-P] C. Greither and B. Pareigis, *Hopf Galois theory for separable field extensions*. Journal of Algebra 106 (1987), 239-258. 25, 28, 32, 47

[Hu] A. Hulpke, *Constructing transitive permutation groups*. Journal of Symbolic Computation 39 (2005), 1-30. 61

[Ko1] T. Kohl, *Classification of the Hopf Galois structures on prime power radical extensions*. Journal of Algebra, 207 (1998), 525-546. 67

[Ko2] T. Kohl, *Groups of order* $4p$*, twisted wreath products and Hopf-Galois theory*. Journal of Algebra, 314 (2007), 42-74. 67

[La] S. Lang, *Algebra 3rd edition*, GTM 211, Springer. 37

[Pa] B. Pareigis, *Forms of Hopf algebras and Galois theory* in "Topics in Algebra, Part 1" (Warsaw, 1988), 75-93. Banach Center Publications 26, Part 1, PWN, Warsaw, 1990. 67

[Sa] M. Salguero, *Hopf Galois theory of separable field extensions*, graduate thesis, University of Barcelona, June 2016. Electronic adress:
http://diposit.ub.edu/dspace/bitstream/2445/110365/2/memoria.pdf 2, 5, 27, 47

[Se] Jean-Pierre Serre, *Local Fields*. New York: Springer-Verlag, 1979 (Graduate Texts in Mathematics). 27

[Un] R. G. Underwood, *Fundamentals of Hopf Algebras*. Cham: Springer; 2015 (Universitext). 5

[Ze] K. N. Zenouz, *On Hopf-Galois structures and skew braces of order* p^3, PhD thesis, University of Exeter, January 2018. Electronic adress:
https://ore.exeter.ac.uk/repository/handle/10871/32248 67