UNIVERSITAT DE BARCELONA

Facultat de Matemàtiques
i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

About Hopf-Galois Structures in Magma Computation

Author: Junjie Ji

Advisor: Dr. Maria Teresa Crespo Vicente
Made at: Departament de matemàtiques i informàtica

Barcelona, January 24, 2022

Abstract

Group theory is quite an astonishing field of Mathematics that reminds of a big world of puzzles, starting from the very first definition of a Group to the concept of the Monster Group which is featured in many informational papers and videos. In particular, one of the most interesting approaches is the Galois theory, which was first introduced in the bachelor's degree. We will merge this concept together with algebras to achieve the structures that this work's title is based on, the Hopf Galois structures.

These structures will be the focal point of the present thesis. The goal is to compute them using Magma (short for Magma Computational Algebra System), a software designed for computations in algebra. For that matter, we will start by presenting the preliminaries where we give concepts that might have not been shown in the bachelor's degree. Afterwards we will give the definitions of the types of algebra to be used. It is followed by the Greither-Pareigis theory which gives the background of the Hopf Galois structures. Sought after we have the Byott's Theorem, which has an immediate application that our program will be based on. Finally, to summarize, we will show some other results and continuations about this matter.

2010 Mathematics Subject Classification. 12F10, 16T05, 16T10, 16T15, 20B30, 20B35

Acknowledgements

Ever since I lost the scholarship for the International Baccalaureate in *Aula Escola Europea* I have always felt defeated in terms of studies and mental health. Even considering not starting a University degree at all, but, my math teacher from the institute, Enric Roldán, really inspired me to actually give it a try and, as I am writing this, I am really happy and thankful for everything he has done for me, specially convincing my parents that University was a good route.

This leads to my family, that at the very beginning, were against the idea of me continuing my studies after high school since the scholarship incident, but after the talk with Enric and also me getting a part time job, they allowed me to do keep on with my studies. I feel like, they were really disappointed but, deeply, they just wanted me to become a better person overall.

Also, I want to thank all my friends, without them cheering me up and helping me in the moments I was struggling, I really think I would have dropped out of college.

Finally, I'm really thankful to my advisor, Teresa Crespo. From the very first meeting we had in a Zoom call during lockdown to the very last email, thanks for all the effort, patience and, sometimes, multiple explanations of the same concept that really helped me understand such abstract concepts.

Contents

Introduction

Our journey will start from the preliminaries on a few different aspects of Mathematics, such as regular and transitive subgroups, semidirect product, multilinear maps and tensor product.

Afterwards, on the next chapter, we will introduce the concept of algebra by diagrams as shown in [7] and [5] which is a notion made possible, or one might say simplified, by tensor products. This alternative definition of algebra leads to think of a duality concept which is presented as the coalgebra. Both definitions concatenate into what it is known as bialgebra, which is a vector space with the maps defined in algebras and coalgebras. We also introduce left and right module algebra and to finish the chapter, we have Hopf algebra which is a bialgebra but with an addition of antipode map. Hopf algebras where firstly introduced by Chase-Sweedler in [6].

Subsequently, on the third chapter, we merge the concepts from algebras with group theory and define the group Hopf algebra. Also in this chapter we can find the Greither-Pareigis theory [1] where we define the Hopf Galois structure on a field extension L/K that consists of a Hopf algebra together with an action on the field L. We will see that this action constructs a left module algebra and induces a isomorphism. It also leads to the Greither-Pareigis Theorem.

Theorem 0.1. (Greither-Pareigis) *Let L/K be a separable extension with normal closure E, let $G = Gal(E/K)$, $G' = Gal(E/L)$ and $X = G/G'$. Then there is a bijection between regular subgroups N of $Perm(X)$ normalized by $\lambda(G)$ and Hopf Galois structures on L/K.*

This theorem is crucial for the study of Hopf Galois structures on a field extension, but the research for these regular subgroups N might become really challenging since the amount of regular subgroups grows largely.

On the fourth chapter, we have Byott's Theorem [4], which reverses the roles of the groups G and N and eases permutations.

Theorem 0.2. (Byott) *Let $G' \subset G$ be finite groups, let $X = G/G'$ and let N be an abstract group of order $|X|$. Then there is a bijection between*

$\mathcal{N} = \{\alpha : N \to Perm(X)$ a 1-1 homomorphism $\mid \alpha(N)$ is regular$\}$ and

$\mathcal{G} = \{\beta : G \to Perm(N)$ a 1-1 homomorphism $\mid \beta(G')$ is the stabilitzer of $e_N\}$

where e_N is the identity of N.

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

- $\alpha(N) = \alpha'(N)$ *iff* β *and* β' *are conjugate by an element of Aut(N).*
- $\alpha(N)$ *is normalized by* $\lambda(G) \subset Perm(X)$ *iff* $\beta(G)$ *is contained in* $Hol(N)$*, the normalizer of N in* $Perm(N)$*.*

We also show a proof of this theorem, done by Childs in [3]. This theorem has a immediate result that allows us to properly count Hopf Galois structures.

On the fifth chapter, we have the our program in Magma computation based on the immediate result form Byott's Theorem to compute the amount of Hopf Galois structures for a given $n = [L : K]$.

Lastly, on the last chapter, we have some glimpses of results from works about Hopf algebras and Galois extensions.

Chapter 1

Preliminaries

For the sake of this work, we take into consideration that the reader knows all the concepts introduced in the bachelor's degree of mathematics.

In this chapter regardless the fact that the reader might already know the following concepts from *Estructures i equacions Algebraiques*, due to the variety that the courses might have experienced, we will introduce them anyways.

1.1 Group theory

Definition 1.1. A **symmetric group** S_n of degree n is the group of all permutations on n symbols.

Given a subgroup $G \subset S_n$ we introduce the following definitions.

Definition 1.2. G **is transitive** $\iff \forall i, j \in \{1, \dots, n\}, \exists \sigma \in G : \sigma(i) = j$.

Definition 1.3. G **is regular** $\iff \forall i, j \in \{1, \dots, n\}, \exists! \sigma \in G : \sigma(i) = j$.

Proposition 1.4. *G is regular if and only if G is transitive and $|G| = n$.*

Proof. For the first implication, if G is regular then G is clearly transitive, therefore it suffices to show that $|G| = n$. Clearly $|G| \geq n$ because if we fix i we need at least n different elements from G to map i to all the other elements in $\{1, \dots, n\}$. If $|G| > n$ then by the *Pigeonhole principle* there must be some $j \in \{1, \dots, n\}$ so that there are distincts $\sigma_i, \tau_i \in G$ such that $\sigma_i(i) = \tau_i(i) = j$ for some $i \in \{1, \dots, n\}$ but that is untrue since G is regular.

For the converse, suppose on the contrary, that G is transitive but not regular and $|G| = n$, therefore there is at least one pair of $i, j \in \{1, \dots, n\}$ so there are distincts $\sigma_i, \tau_i \in G$ such that $\sigma_i(i) = \tau_i(i) = j$. Moreover, this i also needs to be

mapped to all the other elements in $\{1,\dots,n\}$, lets say by $\sigma_k, k \in \{1,\dots,n\}, k \neq i$. Hence, there are at least $n-1$ of such permutations σ_k and in addition to σ_i, τ_i we lead to a contradiction. □

Definition 1.5. Let G and H be groups and $\rho\colon H \to Aut(G)$ be a homomorphism. The **semidirect product** $G \rtimes H$ is the group of the cartesian product $G \times H$ with a binary operation defined as

$$(g,h)\,(g',h') = \left(g\rho(h)(g'), hh'\right).$$

The neutral element is (ϵ_g, ϵ_h) and the inverse of (g,h) is $(\rho(h^{-1})(g^{-1}), h^{-1})$.

One can easily verify the fact that $G \rtimes H$ is indeed a group by checking associativity and both neutral and inverse elements.

1.2 Multilinear maps

Recall that another trivial but important concept from *Algebra Lineal* is the fact that we can extend bilinear maps over a ring R to R-n-linear maps by preserving both conditions of linearity and product by a scalar.

Definition 1.6. Let $M_1,\dots,M_n$ be R-modules. A map $f\colon M_1 \times M_2 \times \cdots \times M_n \to A$ is **R-n-linear** if $\forall i, 1 \leq i \leq n$, and all $a_i, a_i' \in M_i, r \in R$,

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

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

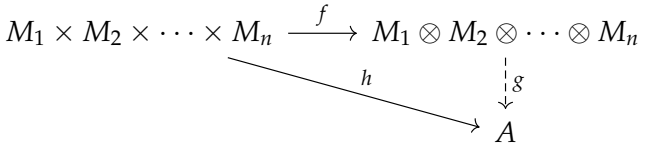
1.3 Tensor product

We will also introduce the tensor product, which will be one of the fundamentals of future concepts.

Definition 1.7. A **tensor product** of $M_1, M_2, \dots, M_n$ over R is an R-module $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ together with an R-n-linear map

$$f\colon M_1 \times M_2 \times \cdots \times M_n \to M_1 \otimes M_2 \otimes \cdots \otimes M_n$$

so that for every R-module A and R-n-linear map $h\colon M_1 \times M_2 \times \cdots \times M_n \to A$ there exists a unique R-module map $g\colon M_1 \otimes M_2 \otimes \cdots \otimes M_n \to A$ such that $gf = h$, which means that the following diagram commutes.



Proposition 1.8. *There is an R-module isomorphism*

$$M_1 \otimes (M_2 \otimes M_3) \cong (M_1 \otimes M_2) \otimes M_3.$$

Proof. The proof of this proposition consists of defining two maps g and h

$$\begin{aligned} g\colon M_1 \times M_2 \times M_3 &\longrightarrow (M_1 \otimes M_2) \otimes M_3 \\ (a_1, a_2, a_3) &\longmapsto (a_1 \otimes a_2) \otimes a_3 \end{aligned}$$

$$\begin{aligned} h\colon M_1 \times M_2 \times M_3 &\longrightarrow M_1 \otimes (M_2 \otimes M_3) \\ (a_1, a_2, a_3) &\longmapsto a_1 \otimes (a_2 \otimes a_3) \end{aligned}$$

and verifying that both maps are R-3-linear. Then since $M_1 \otimes M_2 \otimes M_3$ is a tensor product, there exists a unique map of R-modules for both g and h

$$\begin{aligned} \tilde{g}\colon M_1 \otimes M_2 \otimes M_3 &\longrightarrow (M_1 \otimes M_2) \otimes M_3 \\ a_1 \otimes a_2 \otimes a_3 &\longmapsto (a_1 \otimes a_2) \otimes a_3 \end{aligned}$$

$$\begin{aligned} \tilde{h}\colon M_1 \otimes M_2 \otimes M_3 &\longrightarrow M_1 \otimes (M_2 \otimes M_3) \\ a_1 \otimes a_2 \otimes a_3 &\longmapsto a_1 \otimes (a_2 \otimes a_3) \end{aligned}$$

and finally $\phi := \tilde{g} \circ \tilde{h}^{-1}$ gives us the isomorphism of R-modules.

□

Chapter 2

Types of algebras

In this chapter we will mainly introduce the definitions of all the types of algebras that we will use subsequently. We will consider K as a field, throughout the entire work, unless specifically stated otherwise.

The following definitions are adapted from various works such as [5], [6], and [7].

2.1 Equivalent definitions of algebra

The traditional definition of a K-Algebra that is mainly reminded is the following.

Definition 2.1. A K**-algebra** A is a ring with identity element 1_A together with a ring homomorphism $I : K \to A$ which satisfies $I(r)a = aI(r)$ for $a \in A$, $k \in K$. Then A is a vector space over K with scalar multiplication

$$ka = I(k)a = aI(k)$$

for $k \in K, a \in A$.

The previously defined tensor product, allows us to give another look at the traditional definition of a K-Algebra.

Definition 2.2. A K**-algebra** A is a ring which is also a K-vector space such that always

$$k(a_1a_2) = (ka_1)a_2 = a_1(ka_2),\ k \in K, a_1, a_2 \in A$$

Let 1_A be the identity element of A, then $I : K \to A$ defines a ring homomorphism, with IK in the center of A. The product a_1a_2 is left and right distributive,

so is a K-bilinear function. Therefore $\pi(a_1 \otimes a_2) = a_1 a_2$ describes a K-module homomorphism $\pi : A \otimes A \to A$.
In these terms a K-algebra may be described as a K-module A equipped with two homomorphisms

$$\pi : A \otimes A \to A,\ I : K \to A$$

of K-modules such that the diagrams

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\pi \otimes 1} & A \otimes A \\ {\scriptstyle 1 \otimes \pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ A \otimes A & \xrightarrow{\pi} & A \end{array}$$

and

$$\begin{array}{ccccc} K \otimes A & \xrightarrow{\cong} & A & \xleftarrow{\cong} & A \otimes K \\ {\scriptstyle I \otimes 1}\downarrow & & \| & & \downarrow{\scriptstyle 1 \otimes I} \\ A \otimes A & \xrightarrow{\pi} & A & \xleftarrow[\pi]{} & A \otimes A \end{array}$$

are commutative.

This is true, since the first diagram gives the associativity of the product and the second diagram shows that $I(1_k)$ is a left and right identity element for the product in A and that $\pi(Ik \otimes a) = ka = \pi(a \otimes Ik)$.

The K-algebra A is **commutative** if

$$\pi\tau = \pi$$

where τ denotes the **twist map** defined as $\tau(a \otimes b) = b \otimes a$ for $a, b \in A$

Let A_1 and A_2 be K-algebras. A **K-algebra homomorphism** from A_1 to A_2 is a map of additive groups $\phi : A_1 \to A_2$ for which

- $\phi(1_{A_1}) = 1_{A_2}$
- $\phi(\pi_1(a \otimes b)) = \pi_2(\phi(a) \otimes \phi(b))$
- $\phi(I_1(r)) = I_2(r)$

for $a, b \in A_1, r \in K$. In particular, for A_1 to be a sub-algebra of A_2 (when ϕ is an inclusion) we require that $1_{A_1} = 1_{A_2}$

2.2 Coalgebras

By reversing the arrows from the diagrams in Definition 2.2 we form a dualization of the notion of an algebra.

Definition 2.3. A K**-coalgebra** C is a K-module C with two homomorphisms $\psi : C \to C \otimes C$ and $\epsilon : C \to K$ of K-modules such that the diagrams

$$\begin{array}{ccc} C & \xrightarrow{\psi} & C \otimes C \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle 1\otimes\psi} \\ C \otimes C & \xrightarrow{\psi\otimes 1} & C \otimes C \otimes C \end{array}$$

and

$$\begin{array}{ccccc} C \otimes C & \xleftarrow[\psi]{} & C & \xrightarrow{\psi} & C \otimes C \\ {\scriptstyle\epsilon\otimes 1}\downarrow & & \| & & \downarrow{\scriptstyle 1\otimes\epsilon} \\ K \otimes C & = & C & = & C \otimes K \end{array}$$

are commutative.

The first diagram gives the coassociative law of ψ and the second states that ϵ is a *counit*.

The K-coalgebra C is **cocommutative** if

$$\tau(\psi(c)) = \psi(c)$$

for all $c \in C$

Let C_1 and C_2 be K-coalgebras. A K-linear map $\phi : C_1 \to C_2$ is a K**-coalgebra homomorphism** if

- $(\phi \otimes \phi)\psi_1(c) = \psi_2(\phi(c))$
- $\epsilon_1(c) = \epsilon_2(\phi(c))$

for all $c \in C_1$.

We will use Sweedler's notation in [6] to write

$$\psi(c) = \sum_c c_{(1)} \otimes c_{(2)}$$

2.3 Bialgebras

All together, by merging the maps defined in K-algebras and K-coalgebras, we introduce the concept of bialgebra.

Definition 2.4. A K**-bialgebra** B is a K-vector space with maps π, I, ψ, ϵ that satisfy:

(i) B with multiplication map π and unit map I is a K-algebra

(ii) B with comultiplication map ψ and counit ϵ is a K-coalgebra

(iii) ψ and ϵ are homomorphisms of K-algebras

Remark 2.5. The condition that $\psi\colon B \to B \otimes B$ is an algebra homomorphism implies that

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

for $a, b \in B$.

2.4 Module algebras

Definition 2.6. Let B be a bialgebra, and let A be an algebra and a left B-module with action denoted by "$\cdot$". Then A is a **left** B**-module algebra** if

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

and

$$b \cdot 1_A = \epsilon_b(b)1_A,$$

for all $a, a' \in A, b \in B$.

Let A, A' be K-algebras. A K-linear map $\phi_A\colon A \to A'$ is a **left** B**-module algebra homomorphism** if ϕ_A is both an algebra and a left B-module homomorphism.

Similarly, let C be a coalgebra and a right B-module with action denoted by "$\cdot$". Then C is a **right** B**-module coalgebra** if

$$\psi_c(c \cdot b) = \sum_{(c,b)} c_{(1)}b_{(1)} \otimes c_{(2)}b_{(2)}$$

and

$$\epsilon_C(c \cdot b) = \epsilon_C(c)\epsilon_B(b),$$

for all $c \in C, b \in B$.

Let C, C' be K-coalgebras. A K-linear map $\phi_C \colon C \to C'$ is a **right B-module coalgebra homomorphism** if ϕ_C is both a coalgebra and a right B-module homomorphism.

2.5 Hopf algebras

Definition 2.7. A **K-Hopf algebra** H is a bialgebra with maps π, I, ψ, ϵ together with a K-linear map $\sigma_H : H \to H$ that satisfies

$$\pi(I \otimes \sigma_H)\psi(h) = \epsilon(h)1 = \pi(\sigma_H \otimes I)\psi \tag{2.1}$$

for all $h \in H$. The map σ_H is the **coinverse** (or **antipode**) map and the property (2.1) is the coinverse (or antipode) property.

Chapter 3

Hopf algebras and Galois extensions

The purpose of this chapter is show the concatenation of the previous concepts of algebras and groups to develop the concept of Hopf-Galois structures and the characterization of these structures by Greither and Pareigis.

3.1 Group Hopf algebra

Let G be a group and define

$$KG = \left\{ \sum_{g \in G} r_g g \;\middle|\; rg \in K \right\}.$$

Define aswell a K-bilinear map

$$\begin{aligned} KG \times KG &\longrightarrow KG \\ \left(\sum_{g \in G} r_g g, \sum_{h \in G} r_h h \right) &\longmapsto \left(\sum_{g \in G} r_g g \right) \left(\sum_{h \in G} r_h h \right) = \sum_{g,h \in G} r_g r_h (gh) \end{aligned}$$

by definition of tensor product, there exists a unique K-module map π_{KG}

$$\begin{aligned} \pi_{KG} : KG \otimes KG &\longrightarrow KG \\ a \otimes b &\longmapsto ab \end{aligned}$$

Let I_{KG} be the map

$$\begin{aligned} I_{KG} : K &\longrightarrow KG \\ r &\longmapsto r \cdot 1_G \end{aligned}$$

Then KG is a K-algebra with multiplication map π_{KG} and unit map I_{KG}.

Likewise, let ψ_{KG} be the map

$$\begin{aligned} \psi_{KG} : KG &\longrightarrow KG \otimes KG \\ \sum_{g\in G} r_g g &\longmapsto \sum_{g\in G} r_g (g \otimes g) \end{aligned}$$

and let ϵ_{KG} be the map

$$\begin{aligned} \epsilon_{KG} : KG &\longrightarrow K \\ \sum_{g\in G} r_g g &\longmapsto \sum_{g\in G} r_g \end{aligned}$$

Then KG with comultiplication map ψ_{KG} and counit map ϵ_{KG} is a K-coalgebra. It follows from Remark 2.5 that the maps ψ_{KG} and ϵ_{KG} are also homomorphisms of K-algebras. Hence, $(KG, \pi_{KG}, I_{KG}, \psi_{KG}, \epsilon_{KG})$ is a K-bialgebra.

Define a coinverse map $\sigma_{KG} : KG \to KG$ by $\sigma_{KG}(\tau) = \tau^{-1}$, for $\tau \in G$. Then KG is a K-Hopf algebra.

3.2 Greither-Pareigis theory

Let L be a finite field extension of K. Let $Aut_K(L)$ denote the group of automorphisms of L that fix K. Let G be a subgroup of $Aut_K(L)$.

Define the group action ρ of KG on L as

$$\begin{aligned} \rho\colon KG &\longrightarrow End_K(L) \\ \sum_{g\in G} r_g g &\longmapsto (x \mapsto \sum_{g\in G} r_g g(x)) \end{aligned}$$

Proposition 3.1. *Let L be a finite field extension of K and let G be a subgroup of $Aut_K(L)$. Then L, with the action defined above, is a KG-module algebra.*

Proof. The proof of this proposition consists in checking that L, with action $\rho\colon KG \to End_K(L)$, asserts both conditions in Definition 2.6 so that L is indeed a KG-module algebra. □

Theorem 3.2. *Let L be a finite extension of K, and let G be a subgroup of $Aut_K(L)$. Define the map*

$$\begin{aligned} \varphi\colon L \otimes_K KG &\longrightarrow End_K(L) \\ y \otimes a &\longmapsto \omega_y \circ \rho(a) \end{aligned}$$

where ω_y is the K-linear map

$$\begin{aligned} \omega_y\colon L &\longrightarrow L \\ x &\longmapsto yx \end{aligned}$$

Then φ is a bijection if and only if L is a Galois extension of K with Galois group G.

Proof. The proof of this Theorem can be found in [5] on page 137. □

Therefore, L being a Galois extension of K with group G is equivalent to L being a KG-module algebra for which the map φ is a bijection.

The action ρ defined at the beginning of this section in addition to KG being a K-Hopf algebra as shown at the beginning of this chapter suggests the following notion firstly introduced by Chase and Sweedler in [6].

Definition 3.3. A **Hopf Galois structure** on a finite extension L/K is a pair (H, ρ), where H is a finite cocomuutative K-Hopf algebra and ρ is a Hopf action of H on L. ρ is a K-linear map $\rho\colon H \to End_K(L)$ that gives L a left H-module algebra structure and induces a K-isomorphism $L \otimes_K H \to End_K(L)$.

For the next theorem we introduce the concept of translation maps and the holomorph of a group.

Let $Perm(X)$ denote the group of permutations of the set X.

Definition 3.4. Let L/K be a separable extension with normal closure E, let $G = Gal(E/K)$, $G' = Gal(E/L)$ and $X = G/G'$. The **left translation map**

$$\lambda\colon G \longrightarrow Perm(X)$$

defined as $\lambda(\sigma)(\bar{\tau}) = \sigma\bar{\tau}$.

Likewise, we also introduce **right translation map**

$$\rho\colon G \longrightarrow Perm(X)$$

defined as $\rho(\sigma)(\bar{\tau}) = \bar{\tau}\sigma^{-1}$.

Definition 3.5. Let N be a finite group. The **holomorph** of N, $Hol(N)$, is the normalizer of $\lambda(N)$ in $Perm(N)$:

$$Hol(N) = \{\pi \in Perm(N)\colon \pi \text{ normalizes } \lambda(N)\}$$

Proposition 3.6.

$$Hol(N) = \rho(N) \cdot Aut(N)$$

Proof. To see that $Hol(N) \subset \rho(N) \cdot Aut(N)$, let $\pi \in Hol(N)$. Then for $\eta \in N$, $\pi\lambda(\eta)\pi^{-1} \in \lambda(N)$, hence $\pi\lambda(\eta)\pi^{-1} = \lambda(\gamma(\eta))$ for some $\gamma(\eta) \in N$. The map $\gamma : N \to N$ can be seen as an automorphism of N. Then

$$\begin{aligned}\pi(\eta) = \pi\lambda(\eta)(e) &= (\lambda(\gamma(\eta))\pi)(e) \\ &= \lambda(\gamma(\eta))\pi(e) \\ &= \gamma(\eta)\pi(e) \\ &= (\rho(\pi(e)^{-1})\gamma)(\eta),\end{aligned}$$

hence $\pi = \rho(\pi(e)^{-1})\gamma \in \rho(N) \cdot Aut(N)$.

For the opposite inclusion, view $Aut(N) \subset Perm(N)$ in the obvious way. For $\gamma \in Aut(N), \eta, \mu \in N$ we have

$$\gamma\lambda(\eta)(\mu) = \gamma(\eta\mu) = \gamma(\eta)\gamma(\mu) = (\lambda(\gamma(\eta))\gamma)(\mu),$$

hence $\gamma\lambda(\eta) = \lambda(\gamma(\eta))\gamma$ so $\gamma\lambda(\eta)\gamma^{-1} = \lambda(\gamma(\eta)) \in \lambda(N)$. Therefore $Aut(N)$ normalizes $\lambda(N)$. Also, $\rho(N)$ clearly centralizes $\lambda(N)$ [by definition?], thus both $Aut(N)$ and $\rho(N)$ are subsets of $Hol(N)$.

Now $Aut(N) \cap \rho(N) = \{1\} \in Perm(N)$, since $Aut(N)$ fixes e_N, the identity element of N, and $\rho(N)$ is regular, i.e. the stabilizer in $\rho(N)$ of any element of N is trivial. Also, for $\gamma \in Aut(N), \eta, \mu \in N$,

$$\gamma\rho(\eta)(\mu) = \gamma(\mu\eta^{-1}) = \gamma(\mu)\gamma(\eta^{-1}) = \rho(\gamma(\eta))\gamma(\mu)$$

hence $\gamma\rho(\eta) = \rho(\gamma(\eta))\eta$. Thus $\rho(N) \cdot Aut(N)$ is a subgroup of $Perm(N)$ which is contained in $Hol(N)$. □

Note that we can also think that the following continued equalities, mainly right hand side and left hand side,

$$(\rho(\sigma_1\sigma_2))(\tau) = \tau(\sigma_1\sigma_2)^{-1} = \tau\sigma_2^{-1}\sigma_1^{-1} = \rho(\sigma_1)(\tau\sigma_2^{-1}) = \rho(\sigma_1)(\rho(\sigma_2)(\tau))$$

reminds us of the definition 1.5 of semidirect product, in fact, we have the following corollary.

Corollary 3.7. *$Hol(N)$ as an abstract group,*

$$Hol(N) = N \rtimes Aut(N)$$

Altogether, here's Greither-Pareigis' Theorem from [1].

Theorem 3.8. (Greither-Pareigis) *Let L/K be a separable extension with normal closure E, let $G = Gal(E/K)$, $G' = Gal(E/L)$ and $X = G/G'$. Then there is a bijection between regular subgroups N of $Perm(X)$ normalized by $\lambda(G)$ and Hopf Galois structures on L/K.*

Proof. The proof of this theorem can be found in Chapter 2, Section 6 of [3]. □

Therefore instead of looking for Hopf Galois structures on L/K with normal closure E, and $G = Gal(E/K)$, $G' = Gal(E/L)$, we seek regular subgroups of $Perm(G/G')$ normalized by $\lambda(G)$. For relatively small groups we can specifically find Hopf Galois extensions by finding a regular subgroup N of $Perm(G/G')$ normalized by $\lambda(G)$.

For example, using the same notation as Proposition 3.8, if L/K is not normal, $L \neq E$ and $[L : K] = 3$, we have $G = S_3$ and G' is cyclic of order 2 and $Perm(G/G') \cong S_3$. Therefore $N = A_3$ is a regular subgroup normalized by $\lambda(G)$.

If a Hopf Galois structure corresponds to the regular subgroup N, the isomorphism class of N is referred to as the **type** of the Hopf Galois structure.

To retrieve the Hopf algebra, we see that the Hopf algebra H corresponding to a regular subgroup N of $Perm(X)$ normalized by $\lambda(G)$ is the sub-K-Hopf algebra $E[N]^G$ of the group algebra $E[N]$ fixed under the action of G, where G acts on E by K-automorphisms and on N by conjugation through λ. The Hopf action is given as follows: if $h = \sum_{n\in N} c_n n \in E[N]^G$, then $h(x) = \sum_{n\in N} c_n n^{-1}(\bar{1})(x)$, for $x \in L$, where $\bar{1}$ denotes the class of 1_G in G/G'.

Chapter 4

Byott's theorem

Prior to this chapter, in Greither-Pareigis theory, we would need to find out specifically which regular subgroups of $Perm(X)$ are normalized by G. This task is quite simple for lower degrees but for larger ones we encounter a much more number of regular subgroups. Thus it's useful to reverse the relationship between G and N. This was already done implicitly by Greither and Pareigis, explicitly by L. N. Childs. In this chapter we will show Byott's work about Hopf Galois extensions, which includes how the reversal relationship was precisely done.

Here is Byott's Theorem [4] which is the focal point of this work.

Theorem 4.1. (Byott) *Let $G' \subset G$ be finite groups, let $X = G/G'$ and let N be an abstract group of order $|X|$. Then there is a bijection between*

$\mathcal{N} = \{\alpha : N \to Perm(X)$ *a 1-1 homomorphism* $\mid \alpha(N)$ *is regular*$\}$ *and*

$\mathcal{G} = \{\beta : G \to Perm(N)$ *a 1-1 homomorphism* $\mid \beta(G')$ *is the stabilitzer of* $e_N\}$

where e_N is the identity of N.

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

- *$\alpha(N) = \alpha'(N)$ iff β and β' are conjugate by an element of Aut(N).*
- *$\alpha(N)$ is normalized by $\lambda(G) \subset Perm(X)$ iff $\beta(G)$ is contained in $Hol(N)$, the normalizer of N in $Perm(N)$.*

Definition 4.2. A regular **embedding** is a homomorphism $\alpha\colon N \to Perm(X)$ so that $\alpha(N)$ is regular.

Proof. **(Byott)** (From [3]) Let $\alpha \in \mathcal{N}$, i.e. $\alpha\colon N \to Perm(X)$ is a regular embedding, then $X = \alpha(N)\bar{e}$ where $\bar{e}$ is the coset in X of the identity e of G. Then α induces a bijection $a\colon N \to X$ by $a(\eta) = a(\eta)\bar{e}$. The map a in turn yields an isomorphism

$$C(a)\colon Perm(N) \to Perm(X)$$

by $C(a)(\pi) = a\pi a^{-1}$ for $\pi \in Perm(N)$.

Let $\lambda_X \colon G \to Perm(X)$ be the left transition map, then

$$C(a)^{-1}\lambda_X \colon G \to Perm(N)$$

is an embedding. We show it is in $\mathcal{G}$: for e_N the identity element of N, we have

$$(C(a)^{-1}\lambda_X(\sigma))(e_N) = e_N$$

iff

$$(a^{-1}\lambda_X(\sigma)a)(e_N) = e_N$$

iff

$$\lambda_X(\sigma)(a(e_N)) = a(e_N)$$

iff

$$\lambda_X(\sigma)(\bar{e}) = \bar{e}$$

iff

$$\bar{\sigma} = \bar{e}$$

iff

$$\sigma \in G'.$$

So $C(a)^{-1}\lambda_X \in \mathcal{G}$.

To seek the bijection from $\mathcal{N}$ to $\mathcal{G}$ define

$$\begin{aligned} \Phi : \mathcal{N} &\longrightarrow \mathcal{G} \\ \alpha &\longmapsto C(a)^{-1}\lambda_X \end{aligned}$$

For later in the proof we note that for $C(a)^{-1}\alpha(\eta) = a^{-1}\alpha(\eta)a$ and

$$\begin{aligned} (C(a)^{-1}\alpha(\eta))(\mu) &= (a^{-1}\alpha(\eta)a)(\mu) \\ &= (a^{-1}\alpha(\eta)(\alpha(\mu))\bar{e}) \\ &= a^{-1}((\alpha(\eta)\alpha(\mu))\bar{e}) \\ &= a^{-1}(\alpha(\eta\mu)\bar{e}) \\ &= \eta\mu \\ &= \lambda_N(\eta)\mu. \end{aligned}$$

Therefore we have

$$C(a)^{-1}\alpha = \lambda_N \tag{4.1}$$

About the inverse of Φ. If $\beta\colon G \to Perm(N)$ is in $\mathcal{G}$ then β yields a bijection $b\colon X \to N$ by $b(\bar{\sigma}) = \beta(\sigma)e_N$. Then b is 1-1 and well-defined on cosets because $G' = \{\sigma \in G \mid \beta(\sigma)e_N = e_N\}$, hence b is onto since $|X| = |N|$. Then

$$C(b)\colon Perm(X) \to Perm(N)$$

is an isomorphism, and

$$C(b^{-1})\lambda_N\colon N \to Perm(X)$$

is then a regular embedding of N in $Perm(X)$, hence in $\mathcal{N}$.

Define the inverse Ψ of Φ

$$\begin{aligned} \Psi : \mathcal{G} &\longrightarrow \mathcal{N} \\ \beta &\longmapsto C(b^{-1})\lambda_N \end{aligned}$$

To see that Ψ and Φ are indeed inverse maps, for $\alpha \in \mathcal{N}$, let $\beta = \Phi(\alpha) = C(a)^{-1}\lambda_X$, then $b : X \to N$ is defined by

$$\begin{aligned} b(\bar{\sigma}) &= (C(a)^{-1}\lambda_X(\sigma))(e_N) \\ &= (a^{-1}\lambda_X(\sigma)a)(e_N) \\ &= a^{-1}(\bar{\sigma}) \end{aligned}$$

hence $\Psi(\beta) = C(b)^{-1}\lambda_N = C(a)\lambda_N = \alpha$ by (4.1). Therefore there is a bijection between $\mathcal{N}$ and $\mathcal{G}$ and $\Psi \circ \Phi$ is the identity on $\mathcal{N}$ and $\Phi \circ \Psi$ is the identity on $\mathcal{G}$.

To prove the statements under the bijection, we want to see that if $\alpha(N)$ is normalized by $\lambda_X(G)$ in $Perm(X)$ and $\beta = \Phi(\alpha)$ then $\beta(G)$ normalizes $\lambda_N(N) \subset Perm(N)$.

Let $\lambda_X(\sigma)\alpha(\eta)\lambda(\sigma^{-1}) \in \alpha(N) \subset Perm(X)$ for all $\sigma \in G, \eta \in N$. Mapping over to $Perm(N)$ via $C(a)^{-1}$, we have

$$C(a)^{-1}(\lambda_X(\sigma)\alpha(\eta)\lambda_X(\sigma^{-1})) \in C(a)^{-1}\alpha(N) \subset Perm(N).$$

But again $C(a)^{-1}\alpha(\eta) = a^{-1}\alpha(\eta)a = \lambda_N(\eta)$ by (4.1). Therefore

$$\begin{aligned} C(a)^{-1}(\lambda_X(\sigma)\alpha(\eta)\lambda_X(\sigma^{-1})) &= a^{-1}\lambda_X(\sigma)aa^{-1}\alpha(\eta)aa^{-1}\lambda_X(\sigma^{-1})a \\ &= C(a)^{-1}(\lambda_X(\sigma))\lambda_N(\eta)C(a)^{-1}(\lambda_X(\sigma^{-1})) \\ &= \beta(\sigma)\lambda_N(\eta)\beta(\sigma^{-1}). \end{aligned}$$

So $\beta(G)$ normalizes $\lambda_N(N) \subset Perm(N)$.

Reversing the argument shows that if $\Psi(\alpha) = \beta$, then $\alpha(N)$ is normalized by $\lambda_X(G)$ iff $\beta(G)$ is contained in the normalizer of $\lambda_N(N)$. Finally $\alpha(N) = \alpha'(N)$ iff

$\gamma = \alpha^{-1}\alpha' : N \to N$ is an automorphism of N, hence $\alpha' = \alpha\gamma$. Now α yields $\beta = C(a)^{-1}\lambda_X : G \to Perm(N)$ and $\lambda = C(a)^{-1}\alpha$. If we replace α by $\alpha\gamma$, $\gamma \in Aut(N)$, then

$$C(a\gamma)^{-1} = C(\gamma)^{-1}C(\alpha)^{-1} : Perm(X) \to Perm(N),$$

So if $\Psi(\alpha) = C(a)^{-1}\lambda_X = \beta$, then

$$\beta' = \Psi(\alpha\gamma) = C(\gamma)^{-1}C(a)^{-1}\lambda_X = C(\gamma)^{-1}\beta.$$

So $\beta, \beta' : G \to Perm(N)$ are embeddings which are conjugate by an automorphism of N. That completes the proof.

□

From the theorem we deduce the following corollary.

Corollary 4.3. *Let $a(N, X)$ be the number of regular subgroups in $Perm(X)$ which are normalized by G. Let $b(N, X)$ to be the number of subgroups G^* of $Hol(N)$ such that there is an isomorphism from G^* to G taking the stabiliser in G^* of e_N to G'. We have*

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

where $|Aut(G, G')|$ is the subgroup of $|Aut(G)|$ whose elements send G' to G'.

We will only apply the previous formula when L/K is normal, therefore

$$a(N, G) = \frac{|Aut(G)|}{|Aut(N)|} b(N, G)$$

.

Hence, we can count Hopf Galois structures by computing the right hand side of the formula above.

Chapter 5

Program in Magma computation

In this chapter we will use Magma (short for the software Magma Computational Algebra System [11]) to help us determine every factor in the later formula of the Proposition 4.3

$$a(N,G) = \frac{|Aut(G)|}{|Aut(N)|} b(N,G)$$

- $a(N,G)$ is the number of regular subgroups in $Perm(X)$ normalized by G.
- $b(N,G)$ is the number of subgroups of $Hol(N)$ isomorphic to G.
- $|Aut(G)|$ is the order of the group of automorphisms of G.
- $|Aut(N)|$ is the order of the group of automorphisms of N.

Notice that by Theorem 3.8, $a(N,G)$ corresponds to the number of Hopf Galois structures of a Galois extensions with Galois group G.

The code of the main program is the following

```
HGC:=function(n);
Q:=NumberOfSmallGroups(n);
"The amount of Small groups of order", n ,"is", Q;
for i in [1..Q] do;
"";
"#",i,"small group";
N:=SmallGroup(n,i);
H:=Holomorph(N);
AN:=Order(AutomorphismGroup(N));
G:=SubgroupClasses(H:IsTransitive:=true, OrderEqual:=Order(N));
```

```
AG:=Order(AutomorphismGroup(G[1]‘subgroup));
x:=0;
l:=1;
for j in [1..#G] do;
for k in [1..Q] do;
if IsIsomorphic(G[j]‘subgroup,SmallGroup(n,k)) then ;
x:=x+1;
l:=l*G[j]‘length;
end if;
end for;
end for;
"amount of subgroups isomorphic to the small group: ",x;
"(b(N,G)): ",l;
"|Aut(G)|: ",AG;
"|Aut(N)|: ",AN;
"(a(N,G)): ",AG*l/AN;
"";
end for;
return 1;
end function;
```

This program takes an input n which is the order of the group N. Then calculates the amount of small groups of the same order so we can iterate later on each small group. For every small group N we calculate $Hol(N)$ and $|Aut(N)|$ then, the line

```
S:=SubgroupClasses(H:IsTransitive:=true, OrderEqual:=Order(N));
```

gives us the subgroups G of $Hol(N)$ that are transitive and have order equal to N, therefore regular. Afterwards, we start iterating on the subgroups and look to find isomophisms between said subgroups and small groups of order n, each time we find an isomorphism we concatenate their lengths and print the desired data according to the formula above.

First we will show the number of small groups for every n up to 10:

n	1	2	3	4	5	6	7	8	9	10
Number of small groups (SG)	1	1	1	2	1	2	1	5	2	2

Here are the results for these values of n. Since there are at most 5 small groups of order 8, every column will be representing a small group and its amount of regular subgroups.

HGC (Hopf-Galois counting function), $a(N, G)$					
n	$\mathbf{SG}_1$	$\mathbf{SG}_2$	$\mathbf{SG}_3$	$\mathbf{SG}_4$	$\mathbf{SG}_5$
1	1				
2	1				
3	1				
4	6	4			
5	1				
6	8	6			
7	1				
8	6	588	60	28	232
9	3	9			
10	12	2			

Therefore we have the amount of Hopf Galois structures for n where n is the order of a L/K normal extension. Note that even for small values of n, $(n = 8)$ we already start to see large numbers of structures. In fact, it's known that S_n has $\frac{(n-1)!}{\varphi(n)}$ cyclic subgroups of order n.

Chapter 6

Continuations

In the previous chapter, we have coded a program to count the amount of Hopf Galois structures for a given n, but giving a characterization of whether a separable extension is Hopf Galois or retrieving the Hopf algebra corresponding to a regular subgroup might result a difficult task. In this chapter we will see some results from distinct authors about this matter.

For instance, this first result from Byott [4] is an initial application of Theorem 4.1.

Proposition 6.1. *Let L/K be a extension of prime order with normal closure E. Then L/K is Hopf Galois iff $G = Gal(E/K)$ is solvable.*

From Byott [4] as well we have the following theorem.

Theorem 6.2. (Byott's Uniqueness Theorem) *A Galois extension L/K with galois group G has a unique Hopf Galois structure iff G is a Burnside number.*

A number g is Burnside if $(g, \phi(g)) = 1$, where ϕ is Euler's totient function.

We also have the followings results from [3] and [10].

Corollary 6.3. *There are exactly p^{n-1} Hopf Galois structures on a Galois extension L/K cyclic of order p^n.*

This corollary helps explain some results we got in our program. Every n that is prime has only one Hopf Galois structure.

Theorem 6.4. *Let L/K be a extension of degree p^n, p an odd prime. If $r < n$ there are p^r Hopf Galois structures on L/K.*

Another interesting result is the following proposition from [9]. This result characterizes the type of the structures that we counted in the previous chapter.

Proposition 6.5. *Let L/K be a separable extension of degree p^n, p an odd prime, $n \geq 2$, E its normal closure and $G = Gal(E/K)$. If L/K has a Hopf Galois structure of type C_{p^n}, then it has no structure of noncyclic type.*

Undoubtedly, these results are only a glimpse of the wild amount of other works related to Hopf algebras and Galois extensions...

Postface

One of the things that the bachelor's degree has taught me is the rigor of mathematics. This was made really clear to me while working on this thesis, due to how well written all the academical papers are, how every single detail is taken into account and how every author cite each other for their work purposes.

Another interesting fact that I noticed is about the *Journal of Algebra*. How fascinating is the fact that the paper from Cornelius Greither and Rodo Pareigis is still present nowadays with related works from non other than my thesis advisor, Teresa Crespo, and Marta Salguero.

Furthermore, I also learned how vigorous computation might become with proper mathematical background. I only thought about this matter in the *Aritmetica* subject from the bachelor's where we studied about encryption, but it clearly there's a whole new world behind scientific computation.

Finally I really appreciate how the bachelor's degree helped me grow both intellectually and personally.

Bibliography

[1] Cornelius Greither and Rodo Pareigis, *Hopf Galois Theory for Separable Field Extensions*, Journal of Algebra, **106** (1996).

[2] John J. Cannon and Catherine Playoust, *First Steps in Magma*, (1996).

[3] Lindsay N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, Mathematical Surveys and Monographs, **80**, (2000).

[4] N. P. Byott, *Uniqueness of Hopf Galois Structure for Separable Field Extensions*, Communications in Algebra, **24(10)**, (1996).

[5] Robert G. Underwood, *Fundamentals of Hopf Algebras*, Universitex, (2015).

[6] Stephen U. Chase and Moss E. Sweedler, *Hopf Algebras and Galois Theory*, Lecture Notes in Mathematics, **97** (1969).

[7] Saunders Mac Lane, *Homology*, Classics in Mathematics (1975).

[8] Teresa Crespo, Anna Rio and Montserrat Vela, *From Galois to Hopf Galois: theory and practice*, (2014).

[9] Teresa Crespo and Marta Salguero ,*Hopf Galois structures on separable field extensions of odd prime power degree*, Journal of Algebra, **519** (2019).

[10] T. Kohl, *Classification of Hopf Algebra structures on prime power radical extensions*, Journal of Algebra, **207** (1998).

[11] Magma Computational Algebra System, `http://magma.maths.usyd.edu.au/magma/`