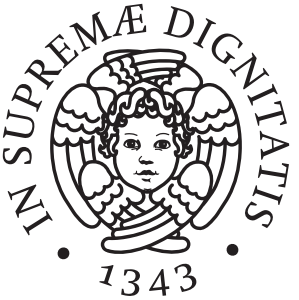
Università di Pisa



Facoltà di Matematica

Hopf Galois theory, tame extensions and integral structures

Tesi di Laurea Magistrale
in Matematica

Candidato
Tommaso Faustini

Relatore
Ilaria Del Corso
Università di Pisa

Anno Accademico 2022 - 2023

Contents

Introduction

After the introduction of Hopf algebras in 1941 due to Heinz Hopf, this objects have proven useful in many areas of mathematics. In particular, they have been used to generalize the classical Galois Theory with the so called Hopf Galois extensions, defined in 1969 by Chase and Sweedler in [CSCS69].

Let L/K be a finite separable extension, then condition of being Galois with group G is equivalent to the bijectivity of the following vector spaces homomorphism: $j : L \otimes KG \to \mathrm{End}_K(L)$ given by $j(l \otimes g)(l') \mapsto lg(l')$. Since the group algebra KG is a Hopf algebra we may say that a Hopf Galois extension is a field extension L/K with an action of an Hopf algebra H on L such that the above condition holds with H instead of KG.

The initial purpose for the introduction of Hopf Galois extensions was to use them with the goal of understanding the automorphisms of purely inseparable field extensions. The idea doesn't work properly and it was recovered only in the eighties by Greither and Pareigis in [PG87] to investigate the separable extensions. They prove a fundamental theorem that reduces the problem of finding all the Hopf Galois structure on a given separable field extension, to a pure group theoretic question. More precisely, let L/K be a finite and separable extension with normal closure E, and Galois groups $G = Gal(E/K)$ and $G' = Gal(E/L)$. Then the theorem states that there is a bijective correspondence between the Hopf Galois structures of L/K and the regular subgroups N of $\mathrm{Perm}(G/G')$ normalized by $\lambda(G)$, where λ is the left multiplication immersion of G in $\mathrm{Perm}(G/G')$. The determination of all regular subgroups of $\mathrm{Perm}(G/G')$ normalized by $\lambda(G)$ becomes really difficult for extension of high degree. In order to solve this problem Byott in [Byo96] reverses the relation between N and G proving that the Hopf Galois structures on L/K correspond to the embedding of G in the holomorph, $Hol(N)$ (that is considerably smaller then $\mathrm{Perm}(G/G')$), where N varies into the set of groups of the same cardinality as G.

In the case of number fields and local fields extensions, the study of the Galois module structure presents very important and long studied questions, especially in relation to the structure of integers. Many of this questions can be generalized to the Hopf Galois context. For example, let L/K be an A-Galois extension of local fields and call S and R the corresponding valuation rings, the notion of associated

order introduced by Leopoldt in [Leo59] extends naturally to the Hopf Galois setting by defining $\mathfrak{A}_G = \{\alpha \in A | \alpha S \subseteq S\}$, while the notion of tameness needs to be reinterpreted to be generalized, as Childs shows in [CH86]. Similarly with the classical case the associated order is the only R-order over which S can be free (as demonstrated in Proposition 3.1.15).

Another important concept is the one of R-Hopf order of a K Hopf algebra A. Essentially, it is an R-order of A equipped with the additional structure of a Hopf algebra. Using this notions, Noether's theorem can be generalized in the Hopf Galois setting and this result is due to Childs (Theorem 3.2.7). The theorem asserts that if we have an R-Hopf order H within A, contained within the associated order, such that S is H-tame, then it follows that S is H-free. Furthermore, in the case where the Hopf algebra is local, these three notions, tame, free, and Galois are equivalent (as shown in Theorem 3.2.13). In this context the notion of Hopf order plays an important role: if the associated order $\mathfrak{A}_A$ is a Hopf order, then S is free over it (as established in Theorem 3.2.9). However, it's crucial to acknowledge that the reverse implication doesn't necessarily hold, as discussed in Remark 4.3.15.

A crucial question that emerges is how to compare the behavior of the valuation ring $\mathcal{O}_L$ within various Hopf–Galois structures over the same field extension L/K. To study this question we restrict to consider a specific family of extensions: the totally ramified, normal extensions L/K of p-adic fields of degree p^2, such that K contains a primitive pth root of unity. Childs in [Chi96] studied the cyclic case, under the hypothesis of p odd and certain restrictions on the ramification numbers, finding a criterion to determine whether $\mathcal{O}_L$ is Hopf Galois with respect to a given Hopf order. A few years later Byott in [Byo02] proved that that criterion remains valid also without the assumption on the ramification number and in the case of elementary abelian extension and $p = 2$. In this case there is an explicit description of both the possible Hopf Galois structure (Theorem 4.2.1) and the Hopf order associated with each structures (Theorem 4.3.12). Studying the question of when is $\mathcal{O}_L$ Hopf Galois, Byott prove that all the extensions L/K such that $\mathcal{O}_L$ is Hopf Galois has to satisfy some arithmetic conditions (Lemma 4.4.2); then after a deep study of the extension with such necessary arithmetic properties (Lemma 4.4.4), finally he finds necessary and sufficient conditions under which $\mathcal{O}_L$ receives a Hopf-Galois structure with respect to a fixed Hopf order in the corresponding Hopf algebra (Proposition 4.4.7).
In the same article, the author specifies all the possibilities for the ramification numbers of L/K under the assumption $\mathcal{O}_L$ is Hopf Galois (Theorem 4.5.3). Finally, Byott arrived at a complete characterisation of the behavior of $\mathcal{O}_L$ in the different Hopf Galois structures, distinguishing the cases of cyclic and elementary abelian extensions, and the cases with p odd and $p = 2$ (Theorems 4.6.4A-D).

In this thesis we present the result of Childs and Byott. Our work is organized as follows.

In Chapter 1 we introduce the basic definitions and results on Hopf algebras and define the Hopf Galois extensions following [Chi00]. In Chapter 2 we present the already mentioned theorem by Greither and Pareigis and the so called Byott's translation. As an application of these results, we count the number of different Hopf Galois structure that a cyclic Galois extension of degree a power of a prime may have. Main sources for this chapter are [Chi00], [PG87] and [Byo96]. In Chapter 3, we introduce the associated order and the concept of tame H-extension; moreover we investigate the relation between being free, Galois and tame. We found that for the associated order being an Hopf order is a sufficient but not necessary condition for being isomorphic to the ring of integers and we prove the generalization of Noether's theorem due to Childs. In the last chapter, we consider a totally ramified normal extension L/K of p-adic fields with degree p^2 and we investigate for which Hopf-Galois structure over L/K we have that $\mathcal{O}_L$ is Hopf-Galois following [Byo02] by Byott described in the previous paragraph. To provide a deeper understanding of these situations, we clarify the results through two illustrative examples.

CHAPTER 1

Basics

In this chapter we will introduce the concepts of Hopf Algebra and Hopf Galois extension. We want to describe many tools that we will use in the following chapter. The result in this section follows mostly [Chi00] and [Und15], with some integration from [Swe69].

1.1 An introduction to Hopf Algebras

1.1.1 Algebras and coalgebras

The usual definition of algebras over a commutative ring with unity R can be formulated in terms of commutative diagrams:

Definition 1.1.1. A *R-algebra* is a triple (A, μ, ι) where A is a R-module, $\mu : A \otimes_R A \to A$ is a linear map, called multiplication, such that the following diagram

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu \otimes id} & A \otimes A \\ {\scriptstyle id \otimes \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow[\mu]{} & A \end{array}$$

commutes and $\iota : R \to A$ is a linear map, called unity, such that the following diagrams

$$\begin{array}{ccc} R \otimes A & \xrightarrow{\iota \otimes id} & A \otimes A \\ & {\scriptstyle s}\searrow & \downarrow{\scriptstyle \mu} \\ & & A \end{array} \qquad \begin{array}{ccc} A \otimes R & \xrightarrow{id \otimes \iota} & A \otimes A \\ & {\scriptstyle s}\searrow & \downarrow{\scriptstyle \mu} \\ & & A \end{array}$$

commute (where s is the scalar multiplication).

The properties of distributivity and compatibility of μ with respect to the sum of A and to s are encoded in linearity. The first diagram illustrates the associativity of μ, while the last two diagrams ensure that $\iota(1_R)$ serves as the unity for μ.
When there is no confusion, we will use A to refer to (A, μ, ι), and we will use ab to represent $\mu(a \otimes b)$. The unadorned tensor $\otimes$ always represents tensors over R.

We prefer this definition of algebras because in this way we can define the coalgebras simply by taking the dual of the diagram, as follows:

Definition 1.1.2. A *R-coalgebra* is a triple (C, Δ, ε) where C is a R-module $\Delta : C \to C \otimes C$ is a linear map, called comultiplication, such that the following diagram

$$\begin{array}{ccc} C \otimes C \otimes C & \xleftarrow{\Delta \otimes id} & C \otimes C \\ {\scriptstyle id \otimes \Delta}\uparrow & & \uparrow{\scriptstyle \Delta} \\ C \otimes C & \xleftarrow[\Delta]{} & C \end{array}$$

commutes and $\varepsilon : C \to R$ is a linear map, called counit, such that the following diagrams

$$\begin{array}{ccc} R \otimes C & \xleftarrow{\varepsilon \otimes id} & C \otimes C \\ & {\scriptstyle t}\nwarrow & \uparrow{\scriptstyle \Delta} \\ & & C \end{array} \qquad \begin{array}{ccc} C \otimes R & \xleftarrow{id \otimes \varepsilon} & C \otimes C \\ & {\scriptstyle t'}\nwarrow & \uparrow{\scriptstyle \Delta} \\ & & C \end{array}$$

commute (where t, t' are respectively the maps $c \mapsto 1 \otimes c, c \mapsto c \otimes 1$).

Notation 1.1.3. *We use the term "coassociativity" referring to the property that the first diagram commutes, while "counitary" describing the property that the last two diagrams commute.*

Same basic example of algebras and coalgebras:

Example 1.1.4. R is clearly an algebra over itself. It is also a coalgebra over itself thanks to the maps: $\Delta_R(r) = 1 \otimes r$ and $\varepsilon_R = id_R$.

Example 1.1.5. $R[x]$ has a structure of R-coalgebra, given by the maps:

$$\Delta(x^n) = \sum_{i=0}^{n} x^i \otimes x^{n-i} \text{ and } \varepsilon(x^n) = \begin{cases} 1 \text{ if } n = 0 \\ 0 \text{ if } n \geq 0 \end{cases} \tag{1.1}$$

extended linearity.

Example 1.1.6. Let S be a set. We denote with RS the free module over R with basis S. If we define

$$\Delta : s \mapsto s \otimes s, \varepsilon : s \mapsto 1 \quad \text{for } s \in S$$

and we extend linearly, we get that RS is a R-coalgebra. This is especially interesting when S is a group, because in this case we have that RS is both an R-algebra and a R-coalgebra.

Example 1.1.7. If A and B are R-algebras, so is $A \otimes B$ equipped with

$$\mu_{A\otimes B} : A \otimes B \otimes A \otimes B \xrightarrow{id_A \otimes \tau \otimes id_B} A \otimes A \otimes B \otimes B \xrightarrow{\mu_A \otimes \mu_B} A \otimes B$$
$$\iota_{A\otimes B} : R \xrightarrow{\Delta_R} R \otimes R \xrightarrow{\iota_A \otimes \iota_B} A \otimes B$$

where τ is the *switch map* that is, the linear extension of the map $a \otimes b \mapsto b \otimes a$. So $\mu_{A\otimes B}$ is the componentwise multiplication.
In the same way, if C and D are R-coalgebras, so is $C \otimes D$ with

$$\Delta_{C\otimes D} : C \otimes D \xrightarrow{\Delta_C \otimes \Delta_D} C \otimes C \otimes D \otimes D \xrightarrow{id_C \otimes \tau \otimes id_D} C \otimes D \otimes C \otimes D$$
$$\varepsilon_{C\otimes D} : C \otimes D \xrightarrow{\varepsilon_A \otimes \varepsilon_B} R \otimes R \xrightarrow{\mu_R} R.$$

Now we introduce a very useful notation, used for the first time by Moss E. Sweedler, for the expression of Δ:

Notation 1.1.8 (Sweedler)**.** *If c is an element of C, we can write:*

$$\Delta(c) = \sum_{i=0}^{n} a_i \otimes b_i,$$

for some $a_i, b_i \in C$. In Sweedler notation we use the symbols $c_{(1)}, c_{(2)}$ to denote the first and second factor of the comultiplication and the indexing is over (c) with the convention that we are summing up all the terms we need for a given c, so it becomes:

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

We can look at the propriety of coalgebras in terms of Sweedler notation:

- Counitary becomes: $c = \sum_{(c)} \varepsilon\left(c_{(1)}\right) c_{(2)} = \sum_{(c)} c_{(1)} \varepsilon\left(c_{(2)}\right)$.
- Coassociativity becomes:

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

  that can be summarized with $\sum_{(c)} c_{(1)} \otimes \left(c_{(2)} \otimes c_{(3)}\right) = \sum_{(c)} \left(c_{(1)} \otimes c_{(2)}\right) \otimes c_{(3)}$.
- Cocommutative becomes: $\sum_{(c)} c_{(1)} \otimes c_{(2)} = \sum_{(c)} c_{(2)} \otimes c_{(1)}$.

Remark 1.1.9. We have seen that if C and D are R-coalgebras, so is $C \otimes D$. Now id we write $\Delta_{C\otimes D}(c \otimes d)$ in Sweedler notation, we get $\sum_{(c\otimes d)} (c \otimes d)_{(1)} \otimes (c \otimes d)_{(2)} = \sum_{(c),(d)} \left(c_{(1)} \otimes d_{(1)}\right) \otimes \left(c_{(2)} \otimes d_{(2)}\right)$.

We have defined the object of our interest, and now we need to define the morphisms between them:

Definition 1.1.10. Let (A, μ_A, ι_A) and (B, μ_B, ι_B) be R-algebras. A R-linear map $f : A \to B$ is an *algebra homomorphism* if the diagrams

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \mu_A}\uparrow & & \uparrow{\scriptstyle \mu_B} \\ A \otimes A & \xrightarrow{f \otimes f} & B \otimes B \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle \iota_A}\nwarrow & \uparrow{\scriptstyle \iota_B} \\ & & R \end{array}$$

commute.

Remark 1.1.11. The commutativity of the diagrams above is equivalent to: for $a, a' \in A$ and $r \in R$

$$f(aa') = f(\mu_A(a \otimes a')) = \mu_B(f(a) \otimes f(a')) = f(a)f(a') \text{ and } f(\iota_A(r)) = \iota_B(r).$$

Definition 1.1.12. Let (A, μ_A, ι_A) and (B, μ_B, ι_B) be R-algebras. A R-linear map $f : A \to B$ is an *algebra antihomomorphism* if the diagrams

$$\begin{array}{ccccc} A & & \xrightarrow{\qquad f \qquad} & & B \\ {\scriptstyle \mu_A}\uparrow & & & & \uparrow{\scriptstyle \mu_B} \\ A \otimes A & \xrightarrow{\tau} & A \otimes A & \xrightarrow{f \otimes f} & B \otimes B \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle \iota_A}\nwarrow & \uparrow{\scriptstyle \iota_B} \\ & & R \end{array}$$

commute.

Definition 1.1.13. Let $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$ be R-coalgebras. A linear map $g : C \to D$ is a coalgebra homomorphism if the diagrams

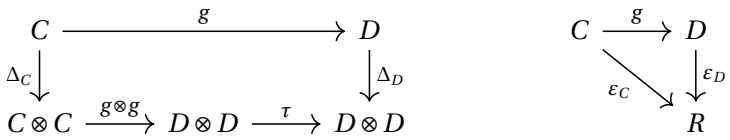
$$\begin{array}{ccc} C & \xrightarrow{g} & D \\ {\scriptstyle \Delta_C}\downarrow & & \downarrow{\scriptstyle \Delta_D} \\ C \otimes C & \xrightarrow{g \otimes g} & D \otimes D \end{array} \qquad \begin{array}{ccc} C & \xrightarrow{g} & D \\ & {\scriptstyle \varepsilon_C}\searrow & \downarrow{\scriptstyle \varepsilon_D} \\ & & R \end{array}$$

commute.

Remark 1.1.14. The commutivity of the diagrams above is equivalent to: for $c \in C$

$$\Delta_D(f(c)) = \sum_{(c)} f(c_{(1)}) \otimes f(c_{(2)}) \text{ and } \varepsilon_D(f(c)) = \varepsilon_C(c).$$

Definition 1.1.15. Let $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$ be R-coalgebras. A linear map $g : C \to D$ is a *coalgebra antihomomorphism* if the diagrams



Definition 1.1.16. A R-bialgebra is a quintuple $(H, \mu, \iota, \Delta, \varepsilon)$ where (H, μ, ι) is a R-algebra, (H, Δ, ε) is a R-coalgebra and either of the following conditions hold:

1. Δ and ε are algebra homomorphisms;
2. μ and ι are coalgebra homomorphisms.

When there is no confusion, we will use H to refer $(H, \mu, \iota, \Delta, \epsilon)$.

Remark 1.1.17. Upon drawing the diagrams for the algebra homomorphism property of Δ and ε, and explicitly writing out the maps $\mu_{H\otimes H}$ and $\iota_{H\otimes H}$ as in Example 1.1.9, we can observe that conditions 1) and 2) are equivalent.

Example 1.1.18. Given any group G, the group algebra RG is a R-bialgebra. As seen in example 1.1.6, RG is a coalgebra and an algebra. So we only have to check that Δ and ε are algebra homomorphisms, i.e.

$$\Delta \circ \mu = \mu_{RG\otimes RG} \circ (\Delta \otimes \Delta), \Delta \circ \iota = \iota_{RG\otimes RG},$$
$$\varepsilon \circ \mu = \mu_R \circ (\varepsilon \otimes \varepsilon), \varepsilon \circ \iota = \iota_R.$$

But for every $\sigma, \tau \in G$ we have $\mu_{RG\otimes RG}(\Delta \otimes \Delta(\sigma \otimes \tau)) = \mu_{RG\otimes RG}(\sigma \otimes \sigma \otimes \tau \otimes \tau) = \sigma\tau \otimes \sigma\tau = \Delta(\mu(\sigma \otimes \tau))$, and by linearity of all maps the property holds for all elements in RG; furthermore $\iota_{RG\otimes RG}(r) = r(\iota(1) \otimes \iota(1)) = \Delta(\iota(r))$, where $r \in R$. The property for ε is straightforward.

Definition 1.1.19. If H, H' are R-bialgebras, $f : H \to H'$ is a bialgebras homomorphism if it is both an algebra and a coalgebra morphism.

1.1.2 Hopf algebras

In this section we introduced the Hopf algebras and we trace a parallel between them and groups, clarifying why they are consider to the a generalization of groups.

Definition 1.1.20. Let H be a R-bialgebra. A linear map $\lambda : H \to H$ is an *antipode* for H if it satisfies the following conditions:

$$\begin{aligned} \mu \circ (id \otimes \lambda) \circ \Delta &= \iota \circ \varepsilon \\ \mu \circ (\lambda \otimes id) \circ \Delta &= \iota \circ \varepsilon \end{aligned} \tag{1.2}$$

A *R-Hopf algebra* is a R-bialgebra with an antipode.

Remark 1.1.21. In the definition of R-Hopf algebra sometimes it is required that the antipode is an R-algebra and R-coalgebra antimorphism. We don't ask that since this request is implied by the condition 1.2, as we will prove later in Proposition 1.1.33.

Example 1.1.22. The R-bialgebra structure on R, together with the antipode $\lambda = id_R$ define a structure of Hopf algebra.

Example 1.1.23. Let K be a field, the polynomial ring $K[x]$ has a structure of free K-algebra, a structure of K-coalgebra with maps that are clearly algebra homomorphism so it is a K-bialgebra. This, together with the map λ defined as linear extension of $x^n \mapsto (-x)^n$, define a structure of Hopf algebra.

Example 1.1.24. Let us consider the bialgebra RG again. We want to define an antipode for RG, for $\sigma \in G$ let $\lambda : \sigma \mapsto \sigma^{-1}$, it extend for linearity to a endomorphism of RG. We check that λ is an antipode, let $\sigma \in G$:

$$\mu((id \otimes \lambda)(\Delta(\sigma))) = \sigma\sigma^{-1} = 1 = \iota(\varepsilon(\sigma)) = \sigma^{-1}\sigma = \mu((\lambda \otimes id)(\Delta(\sigma)))$$

and by linearity of all maps involved the condition holds for all elements in RG. Thus RG is a Hopf algebra.

We have define some new mathematical object, and now we define what does it mean to be a sub-object:

Definition 1.1.25. Let $(H, \mu, \iota, \Delta, \varepsilon)$ be a R-Hopf algebra, we says that H' a R-module of H is a *sub-Hopf algebra of* H if $H' \subseteq H_{Alg}$ is a R-subalgebra, $H' \subseteq H_{CoAlg}$ is a R-subcoalgebra and H' is closed under antipode. In this case $(H', \mu|_{H'}, \iota|_{H'}, \Delta|_{H'}, \varepsilon|_{H'})$ is a Hopf algebra.

Now we define some interesting proprieties that Hopf algebras may have:

Definition 1.1.26. A Hopf algebra H is classified as:

- *commutative* if its algebraic structure $H_{Alg} = (H, \mu, \iota)$ satisfies $\mu \circ \tau = \mu$, making it a commutative algebra .
- *cocommutative* if its co-algebraic structure $H_{CoAlg}(H, \Delta, \varepsilon)$ satisfies $\tau \circ \Delta = \Delta$, making it a cocommutative coalgebra.
- *abelian* if it satisfies both conditions.

Remark 1.1.27. The Hopf algebra RG is always cocommutative:

$$\tau\left(\Delta\left(\sum_{\sigma\in G} r_\sigma \sigma\right)\right) = \tau\left(\sum_{\sigma\in G} r_\sigma(\Delta(\sigma))\right) = \tau\left(\sum_{\sigma\in G} r_\sigma(\sigma \otimes \sigma)\right)$$

using the linearity of τ we obtain that the previous equation is equal to:

$$\sum_{\sigma\in G} r_\sigma \tau(\sigma\otimes\sigma) = \sum_{\sigma\in G} r_\sigma(\sigma\otimes\sigma) = \Delta\left(\sum_{\sigma\in G} r_\sigma\sigma\right)$$

Inspired by the example above we define:

Definition 1.1.28. Given H a Hopf algebra, we define a non-zero element $h \in H$ to be *grouplike* if $\Delta(h) = h \otimes h$.

Proposition 1.1.29. *If R has no idempotents but 0 and 1, and H a Hopf algebra. If $h \in H$ is grouplike, then*

$$\varepsilon(h) = 1.$$

Moreover the set $G(H) = \{h \in H : h \text{ is grouplike}\}$ is a subgroup of the multiplicative group of units of H.

Proof. Let h be grouplike element of H, then it follows easily from counitary that

$$h = \mu(\varepsilon \otimes id)\Delta(h) = h\varepsilon(h),$$

hence $\varepsilon(h) = \varepsilon(h)\varepsilon(h)$. Thus $\varepsilon(h)$ is an idempotent of R; so 0 or 1, and it cannot be zero because ($h \neq 0$ and $h = h\varepsilon(h)$), necessarily $\varepsilon(h) = 1$. We now check that $G(H)$ is a group. Since Δ is an algebra homomorphism, if $h, h' \in G(H)$ we have:

$$\Delta\left(hh'\right) = \Delta(h)\Delta\left(h'\right) = (h\otimes h)\left(h'\otimes h'\right) = hh'\otimes hh',$$

so $G(H)$ is closed under multiplication. Remain to prove that $G(H)$ is closed under antipode. Let $h \in G(H)$, then:

$$\Delta(\lambda(h)) = (\lambda\otimes\lambda)\tau\Delta(h) = (\lambda\otimes\lambda)(h\otimes h) = \lambda(h)\otimes\lambda(h).$$

Finally, for $h \in G(H)$ we have $\lambda(h) = h^{-1}$:

$$1 = \iota\varepsilon(h) = \mu(id\otimes\lambda)\Delta(h) = \mu(id\otimes\lambda)(h\otimes h) = h\lambda(h),$$

and so $G(H)$ is closed under inverse and its elements are units of H.

□

Proposition 1.1.30. *Let K be a field. Distinct grouplike elements are linearly independent over K.*

Proof. Let $h_1, \ldots, h_n$ be grouplike linearly independent elements of H and $h \in H$ a grouplike element such that $h = \sum_{i=1}^n r_i h_i, r_i \in K$. Applying Δ we have:

$$h\otimes h = \sum_i r_i\,(h_i\otimes h_i)$$

thus, replacing h with $\sum_{i=1}^{n} r_i h_i$

$$h \otimes h = \sum_{i,j} r_i r_j \left(h_i \otimes h_j\right).$$

Since $h_1, \ldots, h_n$ on H are linear independent in H, $\{h_i \otimes h_j\}$ are linearly independent in $H \otimes H$. So

$$r_i r_j = 0 \forall\, i \neq j,$$

and

$$r_i^2 = r_i \forall\, i.$$

This two conditions imply that at most one $r_i = 1$ and so either $h = 0$ or $h = h_i$ for that value of i. □

We now introduce the convolution product of function between Hopf Algebras, it is an extension of the usual one for function defined over a group.

Let C be a R-coalgebra and A a R-algebra. We can define an internal multiplication $\star$ on module $\mathrm{Hom}_R(C, A)$, called *convolution* such that for $f, g \in \mathrm{Hom}_R(C, A)$ it is:

$$(f, g) \mapsto f \star g = \mu \circ (f \otimes g) \circ \Delta.$$

Note that $f \star g$ is a map from C to A and is linear because all maps involved in its definition are linear. In Sweedler notation we have $(f \star g)(c) = \sum_{(c)} f(c_1)\, g(c_2)$. Now we can prove the following important proposition:

Proposition 1.1.31. *With the above notation* $(\mathrm{Hom}_R(C, A), \star, \iota \circ \varepsilon)$ *is a R algebra.*

Proof. The product $\star$ is associative, indeed: if $f, g, h \in \mathrm{Hom}_R(C, A)$, by coassociativity of Δ, we have:

$$\begin{aligned}((f \star g) \star h)(c) &= \sum (f \star g)\left(c_{(1)}\right) h\left(c_{(2)}\right) = \sum f\left(c_{(1)}\right) g\left(c_{(2)}\right) h\left(c_{(3)}\right), \\ &= \sum f\left(c_{(1)}\right) (g \star h)\left(c_{(2)}\right) = (f \star (g \star h))(c).\end{aligned}$$

Moreover $\iota \circ \varepsilon \in \mathrm{Hom}_R(C, A)$ is a unity:

$$\begin{aligned}(f \star (\iota \circ \varepsilon))(c) &= \sum f\left(c_{(1)}\right) (\iota \circ \varepsilon)\left(c_{(2)}\right) = \sum f\left(c_{(1)}\right) \varepsilon\left(c_{(2)}\right) \cdot 1_A = f(c), \\ ((\iota \circ \varepsilon) \star f)(c) &= \sum (\iota \circ \varepsilon)\left(c_{(1)}\right) f\left(c_{(2)}\right) = \sum \varepsilon\left(c_{(1)}\right) \cdot 1_A f\left(c_{(2)}\right) = f(c).\end{aligned}$$

□

Now we obtain important result applying the above proposition for H a Hopf algebra, $A = H_{Alg}, C = H_{CoAlg}$:

- we have that $(\mathrm{End}_R(H), \star, \iota\circ\varepsilon)$ is a R-algebra,
- an antipode λ is an inverse for id_H in $(\mathrm{End}_R(H), \star, \iota\circ\varepsilon)$:

$$id \star \lambda = \mu\circ(id\otimes\lambda)\circ\Delta = \iota\circ\varepsilon = \mu\circ(\lambda\otimes id)\circ\Delta = \lambda\star id$$

- the antipode is unique: it is right and left inverse for id in the algebra $(\mathrm{End}_R(H), \star, \iota\circ\varepsilon)$.

We have defined some object so as always we need to define the morphisms between them:

Definition 1.1.32. A *Hopf algebra homomorphism* is a bialgebra homomorphism. If H, H' are Hopf algebras, we denote with $\mathrm{Hom}^R_{Hopf}\left(H, H'\right)$ the set of R-Hopf algebra homomorphisms from H to H'.

Note that we did not require that Hopf algebra homomorphism preserve the antipode. Indeed if $f : H \to H'$ is a bialgebra homomorphism between Hopf algebras with antipode λ, λ' respectively, it follows that $f\circ\lambda = \lambda'\circ f$. In order to prove this, we can show that for any $f \in \mathrm{Hom}_R\left(H, H'\right)$ we have:

$$\begin{aligned} f\star(f\circ\lambda) &= \iota'\circ\varepsilon, \\ \left(\lambda'\circ f\right)\star f &= \iota'\circ\varepsilon. \end{aligned} \tag{1.3}$$

Let us check just the first, for $h \in H$ we have:

$$\begin{aligned} f\star(f\circ\lambda)(h) &= \sum f(h_{(1)})f(\lambda(h_{(2)})) \\ &= \sum f(h_{(1)}\lambda(h_{(2)})) \\ &= f(\varepsilon(h)) \\ &= \iota\circ\varepsilon(h). \end{aligned}$$

This easily imply the thesis:

$$\begin{aligned} f\circ\lambda &= \left(\iota'\circ\varepsilon\right)\star(f\circ\lambda) = \left(\left(\lambda'\circ f\right)\star f\right)\star(f\circ\lambda) = \left(\lambda'\circ(f\star(f\circ\lambda)\right) \\ &= \left(\lambda'\circ f\right)\star\left(\iota'\circ\varepsilon\right) = \left(\lambda'\circ f\right). \end{aligned}$$

Now we can prove that λ is a R-algebra and R-coalgebra antimorphism:

Proposition 1.1.33. *Let H be a Hopf algebra over R; then:*

1. $\lambda\circ\mu = \mu\circ(\lambda\otimes\lambda)\circ\tau$, *meaning that* $\lambda(hh') = \lambda(h')\lambda(h)$ *for every* $h, h' \in H$;
2. $\lambda\circ\iota = \iota$;
3. $\tau\circ(\lambda\otimes\lambda)\circ\Delta = \Delta\circ\lambda$, *meaning that* $\Delta(\lambda(h)) = \sum_{(h)}\lambda\left(h_{(2)}\right)\otimes\lambda\left(h_{(1)}\right)$, *for* $h \in H$;
4. $\varepsilon\circ\lambda = \varepsilon$.

Proof. We start proving 1. From proposition 1.1.31 we know that $\mathrm{Hom}_R(H \otimes H, H)$ is a R-Algebra. Using universal propriety of tensor product we can define two maps $f, g : H \otimes H \to H$ as

$$f(h \otimes h') = \lambda(hh'),$$
$$g(h \otimes h') = \lambda(h')\lambda(h).$$

Since ι is a linear map, for $h, h' \in H$ one has $\iota\varepsilon_{H\otimes H}(h \otimes h') = \varepsilon_{H\otimes H}(h \otimes h')1_H$; so we omit 1_H and write simply $\varepsilon_{H\otimes H}$ for $\iota\varepsilon_{H\otimes H}$. We prove 1) showing that $f \star \mu = \varepsilon_{H\otimes H} = \mu \star g$; in this case $f = f \star \varepsilon_{H\otimes H} = f \star (\mu \star g) = (f \star \mu) \star g = \varepsilon_{H\otimes H} \star g = g$. We have:

$$\begin{aligned}(f \star \mu)(h \otimes h') &= \sum_{(h\otimes h')} f\left((h \otimes h')_{(1)}\right)\mu\left((h \otimes h')_{(2)}\right) \\ &= \sum_{(h),(h')} f\left(h_{(1)} \otimes h'_{(1)}\right)\mu\left(h_{(2)} \otimes h'_{(2)}\right) = \sum_{(hh')} \lambda\left((hh')_{(1)}\right)\left((hh')_{(2)}\right) \\ &= (\lambda \star id)(hh') = \varepsilon(hh') = \varepsilon(h)\varepsilon(h') = \varepsilon_{H\otimes H}(h \otimes h'),\end{aligned}$$

where the third equality holds because Δ is an algebra homomorphism, so $h_{(i)}h'_{(i)} = (hh')_{(i)}$. On the other hand

$$\begin{aligned}(\mu \star g)(h \otimes h') &= \sum_{(h),(h')} \mu\left(h_{(1)} \otimes h'_{(1)}\right) g\left(h_{(2)} \otimes h'_{(2)}\right) \\ &= \sum_{(h),(h')} h_{(1)}h'_{(1)}\lambda\left(h'_{(2)}\right)\lambda\left(h_{(2)}\right) = \sum_{(h)} h_{(1)}\left(\sum_{(h')} h'_{(1)}\lambda\left(h'_{(2)}\right)\right)\lambda\left(h_{(2)}\right) \\ &= \sum_{(h)} h_{(1)}\varepsilon(h')\lambda\left(h_{(2)}\right) = \left(\sum_{(h)} h_{(1)}\lambda\left(h_{(2)}\right)\right)\varepsilon(h') \\ &= \varepsilon(h)\varepsilon(h') = \varepsilon_{H\otimes H}(h \otimes h').\end{aligned}$$

Now we prove 2. Since H is a R-Hopf algebra, ι is a R-coalgebra homomorphism, thus, using equation 1.3 we get $(\lambda \circ \iota) \star \iota = \iota$. But $\iota \circ \varepsilon_R = \iota$ is the identity of the Hopf algebra $Hom_R(R, H)$, so $\iota = (\lambda \circ \iota) \star \iota = (\lambda \circ \iota)$. A similar argument holds for 3) and 4) taking Δ in place of μ, $f = \Delta \circ \lambda$ and $g = \tau \circ (\lambda \otimes \lambda) \circ \Delta$ □

Remark 1.1.34. Remember that in RG we have the antipode map $\lambda = {}^{-1}$, and in $K[x]$ we have the antipode map that is the linear extension of $x^n \mapsto (-x^n)$. In both case the antipode map is such that $\lambda \circ \lambda = id$. This is note a case, as we will show in the following proposition.

Proposition 1.1.35. *Let H be a R-Hopf algebra with antipode λ. If H is commutative or cocommutative, we have $\lambda \circ \lambda = id$.*

Proof. Suppose that H is commutative, the other case is similar. Then λ is a R-algebra homomorphism. So we can use equation 1.3 with $f = \lambda$ obtaining $\lambda \star (\lambda \circ \lambda) = \iota \circ \varepsilon = id \star \lambda$. So:

$$\lambda \circ \lambda = (\iota \circ \varepsilon) \star (\lambda \circ \lambda) = (id \star \lambda) \star (\lambda \circ \lambda) = id \star (\lambda \star (\lambda \circ \lambda)) = id \star (\iota \circ \varepsilon) = id.$$

□

Definition 1.1.36. We say that an R-module M is *finite* if it is finitely generated and projective.

Now we introduce an important class of examples of Hopf algebras, the dual Hopf algebras.
We start with the dual of C a R-coalgebra; if we take $A = R$ in Proposition 1.1.31 , we get that $C^* = \mathrm{Hom}_R(C, R)$ is a R-algebra with multiplication $\mu_{C^*} := \star$ and unit $\iota_{C^*} := \iota_R \circ \varepsilon$. Explicitly, for $f, g \in C^*$, $c \in C, r \in R$ we have:

$$\mu_{C^*}(f \otimes g)(c) = (f \star g)(c) = \sum f\left(c_{(1)}\right) g\left(c_{(2)}\right),$$
$$\iota_{C^*}(r)(c) = \iota_R(\varepsilon(rc)) = r\varepsilon(c).$$

For R-algebras the setting has to be changed a bit, indeed: given A a R-algebra its dual $A^* = \mathrm{Hom}_R(A, R)$ in general is not a R-coalgebra. The problem is that in general is not true that $(A \otimes A)^*$ is isomorphic to $A^* \otimes A^*$. But this become true under the assumption: A finite R-module. In this case we can dualize what we have done for the coalgebra getting:

$$\begin{aligned} \Delta_{A^*} : A^* &\longrightarrow (A \otimes A)^* \simeq A^* \otimes A^* \\ f &\longmapsto f \circ \mu \\ \varepsilon_{A^*} : A^* &\longrightarrow R \\ f &\longmapsto f(1_A). \end{aligned}$$

It is easy to check coassociativity and counitary of the above maps, thus they define a structure of R-coalgebra.

Notation 1.1.37. *If M, N are finite R-module and $f : M \to N$ is a linear map, we write $f^\dagger$ for the transpose map, that is, $f^\dagger : N^* \to M^*$, $f^\dagger(\phi)(m) = \phi(f(m))$.*

Remark 1.1.38. Let (C, Δ, ε) be a R-coalgebra, considering the identification of $(C \otimes C)^*$ with $C^* \otimes C^*$ and of R with R^*, our definition of multiplication and unity on the dual $\left(C^*, \mu^*, \iota^*\right)$ can be re-write as $\mu^* = \Delta^\dagger$ and $\iota^* = \varepsilon^\dagger$.

Now we can note that some property of C (resp. A) pass to the dual:

Remark 1.1.39. If C is cocommutative then C^* is commutative:
the first condition is equivalent to $\sum c_{(1)} \otimes c_{(2)} = \sum c_{(2)} \otimes c_{(1)} \, \forall c \in C$, while the second condition is the same as $\sum f\left(c_{(1)}\right) g\left(c_{(2)}\right) = \sum g\left(c_{(1)}\right) f\left(c_{(2)}\right) \forall f, g \in C^*$ and $\forall c \in C$. Therefore, the implication holds because of commutativity of R.

We have also a dual statement, i.e. if A is commutative then A^* is cocommutative. By definition of Δ^*, for $f \in A^*, a, b \in A$ we have that $\Delta^*(f)(a \otimes b) = f(\mu(a \otimes b)) = f(\mu(b \otimes a)) = \Delta^*(f)(b \otimes a)$; in Sweedler notation $\Delta^*(f)(b \otimes a) = \sum f_{(1)}(b) f_{(2)}(a) = \tau\left(\Delta^*(f)\right)(a \otimes b)$, again by commutativity of R.

Actually in the previous remark the implication could be reverse thanks to the following proposition:

Proposition 1.1.40. *Let C (resp. A) be a finite R-coalgebra (resp. a finite R-algebra). Then $(C, \Delta, \varepsilon) \simeq (C^{**}, \Delta^{**}, \varepsilon^{**})$ as coalgebras (resp. $(A, \mu, \iota) \simeq \left(A^{**}, \mu^{**}, \iota^{**}\right)$ as algebras).*

Proof. We only prove the statement for C (a similar argument holds for A). We already know that there is a module isomorphism

$$\begin{aligned} \varphi : C &\longrightarrow C^{**} \\ c &\longmapsto \varphi_c \end{aligned}$$

where, for $f \in C^*, \varphi_c(f) = f(c)$. We now check that φ is also a coalgebra isomorphism, i.e., for $c \in C, \Delta^{**}(\varphi(c)) = (\varphi \otimes \varphi)\Delta(c)$ and $\varepsilon^{**}(\varphi)(c) = \varepsilon(c)$. Regarding the last equality

$$\varepsilon^{**}(\varphi)(c) = \varepsilon^{**}\left(\varphi_c\right) = \varphi_c(1_{C^*}) = \varphi_c\left(\iota^*(1_R)\right) = \iota^*(1_R)(c) = 1_R \varepsilon(c) = \varepsilon(c),$$

while for the first one we have $\Delta^{**}(\varphi(c)) = \Delta^{**}\left(\varphi_c\right), (\varphi \otimes \varphi)\Delta(c) = \sum \varphi_{c_{(1)}} \otimes \varphi_{c_{(2)}}$ and, for $f, g \in C^*$,

$$\begin{aligned} \Delta^{**}\left(\varphi_c\right)(f \otimes g) = \varphi_c\left(\mu^*(f \otimes g)\right) = \mu^*(f \otimes g)(c) = \sum f\left(c_{(1)}\right) g\left(c_{(2)}\right) \\ = \sum \varphi_{c_{(1)}}(f) \varphi_{c_{(2)}}(g) = \left(\sum \varphi_{c_{(1)}} \otimes \varphi_{c_{(2)}}\right)(f \otimes g). \end{aligned}$$

□

Remark 1.1.41. As already said the above proposition yields the converse implications of the statements in remark 1.1.39, thus C is cocommutative iff C^* is commutative and A is commutative iff A^* is cocommutative.

Proposition 1.1.42. *Let C, D be R-coalgebras and A, B be finite R-algebras. If $f : C \to D$ is a coalgebras homomorphism, then $f^\dagger : D^* \to C^*$ is an algebras homomorphism; in the same way, if $g : A \to B$ is an algebras homomorphism, then $g^\dagger : B^* \to A^*$ is a coalgebras homomorphism.*

Proof. In order to show that $f^\dagger$ is an algebra homomorphism we have to check that $f^\dagger \circ \iota_{D^*} = \iota_{C^*}$ and $f^\dagger \circ \mu_{D^*} = \mu_{C^*} \circ \left(f^\dagger \otimes f^\dagger\right)$. Since f is a coalgebra homomorphism, $\varepsilon_D \circ f = \varepsilon_C$ and for $c \in C$ we have $\Delta_D(f(c)) = \sum_{(c)} f(c_{(1)}) \otimes f(c_{(2)})$. So, for $r \in R, c \in C$ we have:

$$\left(f^\dagger \circ \iota_{D^*}\right)(r)(c) = f^\dagger\left(r\varepsilon_D\right)(c) = r\varepsilon_D(f(c)) = r\varepsilon_C(c) = \iota_{C^*}(r)(c).$$

Furthermore, for $\phi, \psi \in D^*, c \in C$ we have:

$$\begin{aligned}\left(f^\dagger \circ \mu_{D^*}\right)(\phi\circ\psi)(c) &= \left(f^\dagger \circ (\phi \star \psi)\right)(c) = (\phi\star\psi)(f(c)) = \mu(\phi\otimes\psi)\Delta_D(f(c)) \\ &= \mu(\phi\otimes\psi)\left(\sum f\left(c_{(1)}\right)\otimes f\left(c_{(2)}\right)\right) = \sum \varphi f\left(c_{(1)}\right)\psi f\left(c_{(2)}\right) \\ &= ((\phi\circ f)\star(\psi\circ f))(c) = \mu_{C^*}\left(f^\dagger(\phi)\otimes f^\dagger(\psi)\right)(c) \\ &= \mu_{C^*}\left(f^\dagger\otimes f^\dagger\right)(\phi\otimes\psi)(c)\end{aligned}$$

For the second part of the statement we can proceed in a similar way. □

Let $(H, \mu, \iota, \Delta, \varepsilon)$ be a finite R-bialgebra. For what seen above, $\left(H^*, \mu^*, \iota^*, \Delta^*, \varepsilon^*\right)$ is both an R-algebra and a R-coalgebra. Furthermore, thanks to Remark 1.1.38 and Proposition 1.1.42 we can say that Δ_{H^*} and ε_{H^*} are algebra homomorphism so H^* is a R-bialgebra. If we take H to be a Hopf algebra, we have that H^* inherits also the structure of Hopf algebra. Indeed, we can define the antipode to be: $\lambda^* : f \mapsto f\circ\lambda$. Thanks to Remark 1.1.41 we have that H is commutative iff H^* is cocommutative and that H is cocommutative iff H^* is commutative. Moreover, as a corollary of Proposition 1.1.40 we have , $H \simeq H^{**}$ as Hopf algebras. Thanks to this identification we can define the pairing map:

$$\begin{aligned}\langle\cdot,\cdot\rangle : H^* \times H &\longrightarrow R \\ (f,h) &\longmapsto \langle f,h\rangle = f(h).\end{aligned}$$

In order to avoid confusion we will write $\langle f, h\rangle$ in place of $f(h), h(f)$.

Now we see this new construction in the context of group algebras:

Example 1.1.43. Let G be a finite group and H the Hopf algebra RG. Let us study the structure of the dual hops algebra $H^* = \mathrm{Hom}_R(RG, R)$. Let $\{e_\sigma : \sigma \in G\}$ be the dual basis, i.e. $e_\sigma(\tau) = \delta_{\sigma,\tau}$. Every $f \in H^*$ can be written in a unique way as $f = \sum_{\tau\in G} f_\tau e_\tau$. Now we examine the multiplication of element of the dual basis:

$$\left(e_\sigma e_\tau\right)(\rho) = e_\sigma(\rho)e_\tau(\rho) = \delta_{\sigma,\rho}\delta_{\tau,\rho}$$

so for $\sigma = \tau$, we have $e_\sigma^2(\rho) = \delta_{\sigma,\rho} = e_\sigma(\rho)$, while for $\sigma \neq \tau$ we have that e_σ and e_τ are orthogonal. Then $\{e_\sigma : \sigma \in G\}$ are idempotents pairwise orthogonal. The unity is $1_{H^*} = \sum_{\sigma\in G} e_\sigma$, indeed for $f \in H^*$ we have:

$$1\cdot f = \left(\sum_{\sigma\in G} e_\sigma\right)\left(\sum f_\tau e_\tau\right) = \sum_{\sigma,\tau} f_\tau\left(e_\sigma\cdot e_\tau\right) = \sum_\tau f_\tau e_\tau = f,$$

and similarly $f\cdot 1 = f$. Now we examine the comultiplication for element of the dual basis:

$$\Delta(e_\sigma)(\tau\otimes\rho) = e_\sigma(\tau\rho) = \delta_{\sigma,\tau\rho},$$

so since $\{e_\sigma : \sigma \in G\}$ is a basis we have that $\Delta(e_\sigma) = \sum_{\tau\rho=\sigma} e_\tau \otimes e_\rho$. The counit is such that $\varepsilon(e_\sigma) = e_\sigma(1_G) = \delta_{\sigma,1_G}$ and finally the antipode is such that $\lambda(e_\sigma) = e_\sigma \circ \lambda_H = e_{\sigma^{-1}}$.

Furthermore, H^* is always commutative because $H = RG$ is always cocommutative.

Remark 1.1.44. This remark explain why we call abelian the propriety of being commutative and cocommutative:
H^* is cocommutative iff G is an abelian group. Thanks to a precious remark this imply that: H is commutative iff G is an abelian group.
Let us prove the first statement. By linearity of Δ we can reduce ourselves to check cocommutativity only on the element of the dual basis $\{e_\sigma : \sigma \in G\}$. Let us assume that H^* is cocommutative, then for all $\sigma \in G$ we have that $\sum_{\rho\tau=\sigma} e_\tau \otimes e_\rho = \sum_{\rho\tau=\sigma} e_\rho \otimes e_\tau$. Since both sides are sum of elements of the basis $\{e_\mu \otimes e_\nu : \mu, \nu \in G\}$, the equality holds only if each addendum of the LHS appears also on the RHS and vice-versa. So it means that: the set of all τ, ρ such that $\tau\rho = \sigma$ coincides with the set of all τ, ρ such that $\rho\tau = \sigma$. Then for the arbitrariness of $\sigma \in G$ we have that G is abelian. The reverse implication is easy to check.

Now we look at what does it means for an element of H^* to be grouplike:

Remark 1.1.45. Let $f \in H^* = \mathrm{Hom}_R(H, R)$, it is grouplike iff $f : H \to R$ is an algebra homomorphism. Indeed, for $f \in H^*, h, h' \in H$, we have:

$$\Delta^*(f)(h\otimes h') = f(\mu(h\otimes h')) = f(hh'),$$
$$\mu_R(f\otimes f)(h\otimes h') = \mu_R(f(h)\otimes f(h')) = f(h)f(h').$$

Note that, the map $\Delta^*(f)$ has image in R, while the map $f \otimes f$ has image in $R \otimes R$, so we need to identify R and $R \otimes R$ with μ. So for f to be grouplike we require that $\Delta^*(f)$ is the same as $\mu(f \otimes f)$.

1.2 Algebraic structures

1.2.1 Modules and Comodules

Definition 1.2.1. Let A be a R-algebra. A *left module over* A is a couple (M, α) where M is a R-module and $\alpha : A \otimes M \to M$ is a linear map such that the following diagrams

$$\begin{array}{ccc} A\otimes A\otimes M & \xrightarrow{id\otimes\alpha} & A\otimes M \\ {\scriptstyle \mu\otimes id_M}\downarrow & & \downarrow{\scriptstyle \alpha} \\ A\otimes M & \xrightarrow[\alpha]{} & M \end{array} \qquad \begin{array}{ccc} R\otimes M & \xrightarrow{\iota\otimes id_M} & A\otimes M \\ & {\scriptstyle s}\searrow & \downarrow{\scriptstyle \alpha} \\ & & M \end{array}$$

commute, where s is scalar multiplication.

Remark 1.2.2. The commutativity of the diagrams above is equivalent to: $\forall a, b \in A$, $\forall m \in M$ and $\forall r \in R$:

$$(ab) \cdot m = \alpha(\mu(a \otimes b) \otimes m) = \alpha(\alpha \otimes \alpha(b \otimes m)) = a \cdot (b \cdot m),$$
$$r \cdot m = \alpha(\iota(r) \otimes m) = s(r \otimes m) = rm.$$

Definition 1.2.3. Let C be a R-coalgebra. A *right comodule over* C is a couple (N, β) where N is a R-module and $\beta : N \to N \otimes C$ is a linear map such that the following diagrams

$$\begin{array}{ccc} N & \xrightarrow{\beta} & N \otimes C \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\beta\otimes id} \\ N \otimes C & \xrightarrow[id_N \otimes \Delta]{} & N \otimes C \otimes C \end{array} \qquad \begin{array}{ccc} N \otimes C & \xrightarrow{id_N \otimes \varepsilon} & N \otimes R \\ {\scriptstyle\beta}\uparrow & \nearrow_{t'} & \\ N & & \end{array}$$

commute, where t' is the map $n \mapsto n \otimes 1$.

When no confusion may arise we will use M (resp. N) instead of (M, α) (resp. (N, β)), we will call α and β respectively as action and coaction and we will write am or $a \cdot m$ for $\alpha(a \otimes m)$.

Notation 1.2.4. *We adapt the Sweedler notation to coactions in this way: for $n \in N$ we write*

$$\beta(n) = \sum_{(n)} n_{(0)} \otimes n_{(1)},$$

and it should be kept in mind that $n_{(0)} \in N$ and $n_{(1)} \in C$.

Proposition 1.2.5. *Let N be a right comodule over C then it inherits the structure of left module over C^* defined by the map:*

$$\alpha : C^* \otimes N \longrightarrow N$$
$$f \otimes n \longmapsto s_R \circ \tau(id \otimes f) \circ \beta(n) = \sum f\left(n_{(1)}\right) n_{(0)}.$$

where $s_R : N \otimes R \to N$ is the scalar multiplication.

Proof. We need to prove that (N, α) satisfies the properties of a left module over C^*, i.e.:

$$\alpha \circ (id_{C^*} \otimes \alpha) = \alpha \circ \left(\mu^* \otimes id_N\right),$$
$$\alpha \circ \left(\iota^* \otimes id_N\right) = s.$$

First propriety: $f, g \in C^*$ and $n \in N$, we have

$$\begin{aligned}\alpha(id_{C^*}\otimes\alpha)(f\otimes g\otimes n) &= \alpha(f\otimes\alpha(g\otimes n))\\ &= \alpha\left(f\otimes\sum g\left(n_{(1)}\right)n_{(0)}\right)\\ &= \sum g\left(n_{(1)}\right)\alpha\left(f\otimes n_{(0)}\right)\\ &= \sum g\left(n_{(1)}\right)\left(\sum f\left(n_{(0)(1)}\right)n_{(0)(0)}\right)\\ &= \sum g\left(n_{(2)}\right)f\left(n_{(1)}\right)n_{(0)}\\ &= \sum\left(\sum g\left(n_{(1)(0)}\right)f\left(n_{(1)(1)}\right)\right)n_{(0)}\\ &= \sum(f\star g)\left(n_{(1)}\right)n_{(0)}\\ &= \alpha((f\star g)\otimes n) = \alpha\left(\mu^*\otimes id\right)(f\otimes g\otimes n).\end{aligned}$$

Second propriety: for $r\in R, n\in N$:

$$\begin{aligned}\alpha\left(\iota^*\otimes id_N\right)(r\otimes n) &= \alpha\left(\iota_R(r)\varepsilon\otimes n\right) = \sum r\varepsilon\left(n_{(1)}\right)n_{(0)}\\ &= r\sum\varepsilon\left(n_{(1)}\right)n_{(0)} = rn = s(r\otimes n).\end{aligned}$$

□

We now prove a similar result for algebras:

Proposition 1.2.6. *Let A be a finite R-algebra and M is a left module over A. If $\{a_i, a^i\}_{i=1\ldots l}$ let be a projective coordinate system A. Then M inherits the structure of right comodule over A^* defined by the map:*

$$\begin{aligned}\beta : M &\longrightarrow M\otimes A^*\\ m &\longmapsto \sum_{i=1}^{l} a_i m\otimes a^i.\end{aligned}$$

Proof. We need to prove that (M,β) satisfies the properties of a right comodule over A^*, i.e.:

$$\begin{aligned}&\left(\beta\otimes id_{A^*}\right)\circ\beta = \left(id_M\otimes\Delta^*\right)\circ\beta,\\ &\left(id_M\otimes\varepsilon^*\right)\circ\beta = t'.\end{aligned}$$

First propriety: for $m\in M$, the left-hand side equals:

$$\begin{aligned}(\beta\otimes id_{A^*})\beta(m) &= (\beta\otimes id)\left(\sum_i a_i m\otimes a^i\right) = \sum_i\beta(a_i m)\otimes a^i\\ &= \sum_i\left(\sum_j a_j(a_i m)\otimes a^j\right)\otimes a^i = \sum_{i,j} a_j(a_i m)\otimes a^j\otimes a^i,\end{aligned}$$

so evaluating in $b,c\in A$ we obtain:

$$\begin{aligned}(\beta \otimes id_{A^*})\beta(m)(b\otimes c) &= \sum_{i,j} a_j\,(a_i m)\otimes\langle a^j\otimes a^i, b\otimes c\rangle \\ &= \sum_{i,j} a_j\,(a_i m)\,\langle a^j, b\rangle\langle a^i, c\rangle = \sum_j \langle a^j, b\rangle a_j(\sum_i \langle a^i, c\rangle a_i(m)) \\ &= b(cm).\end{aligned}$$

For the right-hand side, instead, we have:

$$\begin{aligned}\left(id_M\otimes\Delta^*\right)\beta(m) &= \left(id\otimes\Delta^*\right)\left(\sum_i a_i m\otimes a^i\right) = \sum_i a_i m\otimes\left(\sum_{(a^i)} a^{i(1)}\otimes a^{i(2)}\right) \\ &= \sum_{i,(a^i)} a_i m\otimes a^{i(1)}\otimes a^{i(2)}\end{aligned}$$

so evaluating in $b, c \in A$ we obtain:

$$\begin{aligned}\left(id_M\otimes\Delta^*\right)\beta(m)(b\otimes c) &= \left(\sum a_i m\otimes\left(a^{i(1)}\otimes a^{i(2)}\right)\right)(b\otimes c) \\ &= \sum a_i m a^i(bc) = (bc)m.\end{aligned}$$

Then the thesis follows from the associativity of the action. The second propriety can be check in a similar way. □

Remark 1.2.7. Based on the preceding discussion, given a left module (M,α) over an algebra A, the action α induces a coaction β, which makes (M,β) a right comodule over A. Similarly, the coaction β induces an action α, making (M,α) a left module over A. It is important to note that A is isomorphic to A, which raises the question of whether α and α^* coincide up to isomorphism. As it turns out, they do coincide, and we can show this by the following equation:

$$\alpha^{**}(a\otimes m) = s_R\left(\tau\left(\sum a_i m\otimes\left\langle a^i, a\right\rangle\right)\right) = \sum\left\langle a^i, a\right\rangle a_i m = am = \alpha(a\otimes m.)$$

A similar conclusion can be drawn when starting with a right module (N,β) over a coalgebra C. In this case, the coaction β induces a module action α on N over C, which in turn induces a comodule coaction β on N over C. This coaction β is the same as the original coaction β up to the isomorphism $C\simeq C^*$, and this can be shown using the following equation:

$$\beta^{**}(n) = \sum a^i\cdot n\otimes a_i = \sum\left(\sum n_{(0)}\left\langle a^i, n_{(1)}\right\rangle\right)\otimes a_i = \sum n_{(0)}\otimes n_{(1)} = \beta(n).$$

As we did before, after introducing new mathematical objects we have to define their morphisms:

Definition 1.2.8. Let (M, α) and $\left(M', \alpha'\right)$ be left modules over an algebra A. A homomorphism of the left modules on A is a linear map $f : M \to M'$ such that the following diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\alpha'} \\ A \otimes M & \xrightarrow[id \otimes f]{} & A \otimes M \end{array}$$

commutes, i.e. for all $a \in A$ and $m \in M$ $f(\alpha(a \otimes m)) = \alpha'(a \otimes f(m))$.

Definition 1.2.9. Let (N, β) and $\left(N', \beta'\right)$ be right comodules over a coalgebra C. A homomorphism of right comodules over C is a linear map $g : N \to N'$ such that the following diagram:

$$\begin{array}{ccc} N & \xrightarrow{g} & N' \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\beta'} \\ N \otimes C & \xrightarrow[g \otimes id]{} & N \otimes C, \end{array}$$

commutes, i.e. for all $n \in N$ $\beta'(g(n) = \sum g(n_{(0)}) \otimes n_{(1)}$.

1.2.2 (Co)Module Algebras

Let H be a Hopf algebra, then we can consider left modules and right comodules over H. For the modules for example we have:

- R is a left H-module via ε: $h \cdot r = \varepsilon(h)r$,
- let M, M' be left modules over H, then we have that $M \otimes M'$ is a left H-module via Δ:
$$h \cdot \left(m \otimes m'\right) = \Delta(h)\left(m \otimes m'\right) = \sum h_{(1)} \cdot m \otimes h_{(2)} \cdot m'$$
So, if α, α' are the actions on M, M', the action on $M \otimes M'$ is the tensor product $\alpha \otimes \alpha'$.

Remark 1.2.10. Notice that if H has only the structure of algebra, $M \otimes M'$ can be enrich with a module structure over H but associated action will not be the tensor product of the actions.

If a left module over H is also a R-algebra, seeing $S \otimes S$ and R as H-modules, we can define an additional structure:

Definition 1.2.11. Let H be a Hopf algebra, and S be both a left module over H and a R-algebra. S is a (left) *H-module algebra* if μ_S and ι_S are H-module homomorphism.

Remark 1.2.12. The condition "μ_S, ι_S are H-module homomorphisms" can be made explicit. For $h \in H$ and $s, t \in S$ we have:

$$\mu_S(\alpha_{S\otimes S}(h \otimes s \otimes t)) = \mu_S\left(\sum_{(h)} h_{(1)} \cdot s \otimes h_{(2)} \cdot t\right) = \sum_{(h)} \left(h_{(1)} \cdot s\right)\left(h_{(2)} \cdot t\right),$$
$$\alpha_S\left(id \otimes \mu_S\right)(h \otimes s \otimes t) = \alpha_S(h \otimes st) = h \cdot st.$$

So μ_S is a H-module homomorphism iff $h \cdot st = \sum_{(h)} \left(h_{(1)} \cdot s\right)\left(h_{(2)} \cdot t\right)$. For $r \in R$ and $h \in H$ we have:

$$\alpha_R(id \otimes \iota_S)(h \otimes r) = \alpha_R(h \otimes \iota_S(r)) = \varepsilon(h)\iota_S(r),$$
$$\iota_S(\alpha_S(h \otimes r)) = \iota_S(h \cdot r).$$

So ι_S is a H-module homomorphism iff $h \cdot r = \varepsilon(h)r$

Now we present our first example of non-trivial H-module algebra, which will bring also the first connection between Hopf algebra theory and Galois theory:

Example 1.2.13 (Galois)**.** Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$ then L is a left module over the Hopf algebra KG. The action $\alpha_{L/K} : KG \otimes L \to L$ is given by the linear extension of the Galois action $G \curvearrowright L$. For $\sigma, \tau \in G$ and $l \in L$ we have $(\sigma\tau)(l) = \sigma(\tau(l))$, so L is a KG-module. Note that L is also a K-algebra. By linearity of the action we can check that L is also a KG-modulo algebra simply proving the properties only for the elements in G: for all $\sigma \in G, l, m \in L$ we have $\sigma(lm) = \sigma(l)\sigma(m)$ and for $k \in K$ we have $\sigma(k) = k$.

Now we notice that module algebras are the generalization of action of groups:

Example 1.2.14. Let G be a finite group and let S be a finite commutative R-algebra, then S is a RG-module algebra if and only if G acts as automorphisms of S. Indeed, if G is a subgroup of the algebra homomorphism group $\mathrm{Aut}(S)$, then for any $\sigma \in G$ and $s, t \in S$, we have $\sigma(st) = \sigma(s)\sigma(t)$. A RG-module action on S can be defined, as in the previous example, by mapping $\sum k_\sigma \sigma \otimes s$ to $\sum k_\sigma \sigma(s)$, and under this action, S becomes a RG-module algebra:

$$\begin{aligned}\left(\sum r_\sigma \sigma\right)(st) &= \sum r_\sigma \sigma(st) = \sum r_\sigma \sigma(s)\sigma(t) \\ &= \sum r_\sigma(\sigma \otimes \sigma)(s \otimes t) = \Delta\left(\sum r_\sigma \sigma\right)(s \otimes t).\end{aligned}$$

The reverse implication can be easily verified.

Now we investigate the corresponding definition for comodules. As for the modules, we have:

- R is a right H-comodule via $\iota : \beta_R(r) = r \otimes \iota(1_R)$

- let N, N' be right comodules over H, then $N \otimes N'$ is a right H-comodule via μ:
$$\beta_{N\otimes N'}\left(n \otimes n'\right) = \sum n_{(0)} \otimes n'_{(0)} \otimes \mu\left(n_{(1)} \otimes n'_{(1)}\right)$$

Seeing now $N \otimes N'$ and R as right H-comodules, we can define an additional structure:

Definition 1.2.15. Let H be a Hopf algebra and S be both a right comodule over H and a R-algebra. S is a (right) H-comodule algebra if μ_S, ι_S are H-comodule homomorphisms.

Remark 1.2.16. The condition "μ_S, ι_S are H-comodule homomorphisms" can be made explicit. For $h \in H$ and $s, t \in S$ we have:

$$\beta\left(\mu_S(s \otimes t)\right) = \beta(st),$$
$$\left(\mu_S \otimes id\right)\left(\sum s_{(0)} \otimes t_{(0)} \otimes \mu\left(s_{(1)} \otimes t_{(1)}\right)\right) = \sum s_{(0)} t_{(0)} \otimes s_{(1)} t_{(1)} = \beta(s)\beta(t),$$

so μ_S is a H-comodule homomorphism iff β is a R-algebra homomorphism. For $r \in R$ we have:

$$\beta\left(\iota_S(r)\right) = \beta\left(r\iota_S\left(1_R\right)\right) = r\beta\left(1_S\right) = r\left(1_S \otimes 1_H\right),$$
$$\left(\iota_S \otimes id\right)\beta_R(r) = \left(\iota_S \otimes id\right)\left(r \otimes \iota\left(1_R\right)\right) = r\left(\iota_S\left(1_R\right) \otimes \iota\left(1_R\right)\right),$$

therefore ι_S is a H-comodule homomorphism iff $\iota_S\left(1_R\right) = 1_S$.

Let S be a H-module algebra, we already know that S has also a structure of H^*-comodule; it is easy to check that S is also a H^*-comodule algebra and that also the reverse holds.

Example 1.2.17 (H^* is a H-module algebra)**.** Let H be a finite-dimensional Hopf algebra. H^* is a H^*-comodule through Δ^*. Furthermore, from remark 1.2.16 to prove that μ_{H^*} and ι_{H^*} are homomorphisms of H^*-comodules we can simply notice that $\beta = \Delta^*$ is a R-algebra homomorphism. So H^* is a H^*-comodule algebra, that is the same as saying that H^* is a H-module algebra.

Now we give a definition that able us to explain that comodule algebras generalize the grading with groups:

Definition 1.2.18. We say that S is a *G-graded R-algebra* if

$$S = \bigoplus_{\sigma \in G} S_\sigma$$

with the properties $R \subseteq S_{id}$ and $S_\sigma \cdot S_\tau \subseteq S_{\sigma\tau}$ for all $\sigma, \tau \in G$.

Example 1.2.19. Let S be a G-graded algebra then the G-grading on S induces a map:

$$\begin{aligned} \beta : S &\longrightarrow S \otimes RG \\ s &\longmapsto s \otimes \sigma; \end{aligned}$$

Where σ is such that $s \in S_\sigma$. β is a R-linear map and it is an algebra homomorphism by the property $S_\sigma \cdot S_\tau \subseteq S_{\sigma\tau}$, so β is a coaction and S is a RG-comodule algebra.

1.3 Hopf-Galois extensions

In this section we want to generalize the definition of Galois extension in the context of Hopf algebra. In order to do this we start showing an equivalent condition for a finite field extension L/K for being a Galois extension with group G.
From now on, we will assume that all extensions of fields are finite and separable.
Let L/K be a Galois extension with Galois group G. In the example 1.2.13, we have seen that the Galois action $G \curvearrowright L$ extends linearly to a module-algebra action $\alpha : KG \to \mathrm{End}_K(L)$. Notice that the map

$$\begin{aligned} id \otimes \alpha : L \otimes KG &\longrightarrow \mathrm{End}_K(L) \\ l \otimes \left(\sum_\sigma k_\sigma \sigma\right) &\longmapsto l\alpha\left(\sum_\sigma k_\sigma \sigma\right) : m \mapsto l\left(\sum_\sigma k_\sigma \sigma(m)\right) \end{aligned}$$

is a bijective homomorphism of vector space. Notice that the two vector space has the same dimension, so we need only to prove the injectivity.

If $(id \otimes \alpha)(l \otimes (\sum k_\sigma \sigma)) = 0$, it means that the map $l(\sum k_\sigma \sigma)$ is the null map in $\mathrm{End}_K(L)$. But Proposition 1.1.30 tell us that grouplike elements are linearly independent so all the coefficients are zero, and therefore $l \otimes (\sum k_\sigma \sigma) = 0$. This implies that $id \otimes \alpha$ is injective.

Remark 1.3.1. Let L be a field and $G < \mathrm{Aut}(L)$ finite, the Example 1.2.14 told us that there is a modulo algebra action α which makes L a KG-modulo algebra. Moreover, by classical Galois theory, L/L^G is a Galois extension with Galois group $G = \mathrm{Aut}\left(L/L^G\right)$. Thus if $id \otimes \alpha$, as defined above, is an isomorphism, we have that $[L : K] = |G|$. Then we have $L^G = K$ and $G = \mathrm{Gal}(L/K)$, indeed:

$$|G| = \left|\mathrm{Aut}\left(L/L^G\right)\right| \leq |\mathrm{Aut}(L/K)| \leq [L : K].$$

The discussion above together with the remark above gives us an equivalent definition of Galois extension:

Definition 1.3.2. Let L/K be a fields extension and $G < \mathrm{Aut}(L)$ finite, we have that L/K is a *Galois extension with group* $G = \mathrm{Aut}(L/K)$ iff $id \otimes \alpha$ is an isomorphism between $L \otimes KG$ and $\mathrm{End}_K(L)$.

The significance of this definition lies in its applicability to Hopf algebras, as it can be extended to this context:

Definition 1.3.3. Let S be a finite commutative R-algebra and H a cocommutative R-Hopf algebra. S is an Hopf Galois extension over R with Hopf algebra H (shortly S/R is H-Galois) if:

- S is a left H-module algebra with action α_S.
- The map

$$\begin{aligned} j : S \otimes H &\longrightarrow \mathrm{End}_R(S) \\ s \otimes h &\longmapsto j(s \otimes h) : t \mapsto s \cdot (ht) := \mu_S(s \otimes \alpha_S(h \otimes t)), \end{aligned}$$

  is an isomorphism.

We consider again a finite Galois extension L/K and dualize the argument above; the action $\alpha : KG \otimes L \to L$ gives us a coaction

$$\begin{aligned} \beta : L &\longrightarrow L \otimes KG^* \\ l &\longmapsto \sum_{\sigma \in G} \sigma(l) \otimes e_\sigma \end{aligned}$$

(where $\{e_\sigma : \sigma \in G\}$ is the dual basis of $\{\sigma : \sigma \in G\}$) that makes L a KG^* comodule algebra. As for the case above we have that the vector spaces homomorphism:

$$\begin{aligned} \gamma : L \otimes L &\longrightarrow L \otimes KG^* \\ l \otimes m &\longmapsto \sum_{\sigma} l\sigma(m) \otimes e_\sigma \end{aligned}$$

is a bijection. As already observed above, for dimensional reason we just need to prove the injectivity of the map. Let $\{m_1, \ldots, m_n\}$ be a K-basis for L. We can express any element in $L \otimes L$ as $\sum_i l_i \otimes m_i$. Suppose $\gamma\left(\sum_\sigma l_i \otimes m_i\right) = 0$, meaning $\sum_\sigma \sum_i l_i \sigma(m_i) \otimes e_\sigma = 0$. Since $\sum_i l_i \sigma(m_i) = \sum k_i^\sigma m_i$ where $k_i^\sigma \in K$, we have $\sum_{i,\sigma} k_i^\sigma m_i \otimes e_\sigma = 0$, which implies $k_i^\sigma = 0$ for all i, σ. Hence, $\sum_i l_i \sigma(m_i) = 0$ for all σ, and so $l_i = 0$ for all i. Therefore, γ is injective.
Also in this case the discussion gives us an equivalent definition of Galois extension:

Definition 1.3.4. Let L/K be a fields extension and G a finite subgroup of $\mathrm{Aut}(L)$, L/K is Galois with group $G = \mathrm{Aut}(L/K)$ iff $L \otimes L \simeq L \otimes KG^*$ via γ.

Hence we have a generalization also for the dual structure:

Definition 1.3.5. Let S be a finite commutative R-algebra and H a finite cocommutative R-Hopf algebra with finite and commutative dual Hopf algebra H^*. S is a *H^*-Galois object* (shortly S/R is H^*-Galois) if

- S is a right H^*-comodule algebra with coaction β_S.

- The map:
$$\gamma : S \otimes S \longrightarrow S \otimes H^*$$
$$s \otimes t \longmapsto (s \otimes 1)\beta(t)$$
is an isomorphism

The term "H-Galois object" originates from the common use of referring to H-comodules as H-object.

As we could expect, these definitions are equivalent.

Proposition 1.3.6. *Let H be a finite R-Hopf algebra and S a finite commutative R-algebra which is also a left H-module algebra. We have that j is an isomorphism iff γ is an isomorphism.*

Proof. Consider

$$\begin{array}{ccc} S \otimes H & \xrightarrow{\quad j \quad} & Hom_R(S,S) \\ \eta \downarrow & & \downarrow \nu \\ Hom_S(S \otimes H^*, S) & \xrightarrow[\gamma^\dagger]{} & Hom_S(S \otimes S, S) \end{array}$$

where $\eta(s \otimes h)(t \otimes f) = s \cdot (tf(h))$, $\nu(g)(s \otimes t) = s \cdot g(t)$ and $\gamma^\dagger$ is the transpose map $\gamma^\dagger(f)(s \otimes t) = f(\gamma(s \otimes t)) = f((s \otimes 1)\beta(t)) = f\left(\sum_{(t)} st_{(0)} \otimes t_{(1)}\right)$. Notice that the previous diagram is commutative, indeed:

$$\begin{aligned} \nu(j(s \otimes h))(t \otimes u) &= t(j(s \otimes h))(n) = t \cdot s \cdot (hu); \\ \gamma^\dagger(\eta(s \otimes h))(t \otimes u) &= \eta(s \otimes h)\left(\sum_{(u)} tu_{(0)} \otimes u_{(1)}\right) \\ &= s \cdot t \cdot \left(\sum_{(u)} u_{(0)} \langle h, u_{(1)} \rangle\right) \\ &= s \cdot t \cdot (hu). \end{aligned}$$

Notice that thanks to the assumption H and S finite we have that η and ν are isomorphisms, so γ is an isomorphism iff $\gamma^\dagger$ is an isomorphism. This conclude simply noticing that $\gamma^\dagger$ is an isomorphism iff γ is an isomorphism. □

Corollary 1.3.7. *Let S be a finite commutative R-algebra that is also a H module algebra, with H^* a finite cocommutative R-Hopf algebra. We have that S is H-Galois iff S is a H^*-Galois object.*

Remark 1.3.8. The R-module $\mathrm{End}_R(S)$ is also a R-algebra endowed with composition. Furthermore, we have already seen that the tensor product of algebras is also an algebra.

If S is H-Galois then we have that γ is an isomorphism, so we can "pullback" the structure of algebra for $S \otimes H^*$ to $S \otimes H$. In this case we simply obtain the componentwise multiplication:

Remark 1.3.9. Let S be a finite commutative R-algebra, H a finite cocommutative R-algebra and suppose that S is a H^*-comodule algebra; the vector spaces $S \otimes S$ and $S \otimes H^*$ equipped with the componentwise multiplication are R algebras. We have that $\gamma : S \otimes S \to S \otimes H^*$ is an algebras homomorphism; for $s, t, s', t' \in S$

$$\begin{aligned}\gamma((s \otimes t)(a \otimes b)) &= (sa \otimes 1)\beta(tb) = (sa \otimes 1)\beta(t)\beta(b) \\ &= \left(\sum_{(t)} sat_{(0)} \otimes t_{(1)}\right)\left(\sum_{(b)} b_{(0)} \otimes b_{(1)}\right),\end{aligned}$$

where the second equality holds because S is a H^*-comodule algebra, thus β is an algebras homomorphism. Recalling that on $S \otimes H^*$ we have componentwise multiplication, by commutativity of S the last quantity equals

$$\left(\sum_{(t)} st_{(0)} \otimes t_{(1)}\right)\left(\sum_{(b)} ab_{(0)} b_{(1)}\right) = \gamma(s \otimes t)\gamma(a \otimes b).$$

If S is H-Galois then we have that j is an isomorphism, so we can "pullback" the structure of algebra of $\mathrm{End}_R(S)$ to $S \otimes H$. In order to investigate this structure we consider:

Definition 1.3.10. Let S be a H-module algebra. The *smash product* $\sharp$ on the R-module $S \otimes H$ is given by: for $s, t \in S$ and $h, g \in H$:

$$(s \otimes h)\sharp(t \otimes g) = \sum_{(h)} sh_{(1)}(t) \otimes h_{(2)}g,$$

$$\iota_\# := r \otimes 1 = \iota_S(r) \otimes \iota_H(1).$$

The following proposition explain the importance of the newly introduced product:

Proposition 1.3.11. *The map $j : (S \otimes H, \sharp) \to (\mathrm{End}_R(S), \circ)$ is a R-algebras homomorphism.*

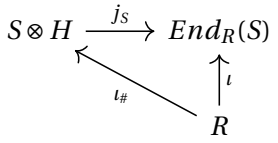
Proof. We need to prove the commutativity of the following diagram:

$$\begin{array}{ccc} S \otimes H & \xrightarrow{\quad j_S \quad} & End_R(S) \\ {\scriptstyle \mu_\#}\uparrow & & \uparrow{\scriptstyle \circ} \\ (S \otimes H) \otimes (S \otimes H) & \xrightarrow[j_S \otimes j_S]{} & End_R(S) \otimes End_R(S) \end{array}$$

For $s,t,u \in S$ and $h,g \in H$:

$$\begin{aligned} j((s\otimes h)\sharp(t\otimes g))(u) &= j\left(\sum s_{(1)}(t)\otimes h_{(2)}g\right)(u) = \sum \mathrm{sh}_{(1)}(t)h_{(2)}(g(u)) \\ &= \mathrm{sh}(tg(u)) = (j(s\otimes h))(tg(u)) \\ &= j(s\otimes h)(j(t\otimes g)(u)) = (j(s\otimes h)\circ j(t\otimes g))(u). \end{aligned}$$

Finally, we need to prove the commutativity of the following diagram:



For all $s \in S$ and for all $r \in R$, we have:

$$j(\iota_\#(r))(s) = j(\iota_S(r)\otimes \iota_H(1))(s) = \iota_S(r)((\iota_H(1))(s)) = rs$$

□

Definition 1.3.12. Let S be a H-module algebra, the *ring of the invariants of the H-action* is $S^H = \{s \in S : h(s) = \varepsilon(h)s \ \forall h \in H\}$.
Let S be a H-comodule algebra the *ring of the coinvariants of the H-coaction* is $S^{coH} = \left\{s \in S : \beta(s) = s\otimes 1_H\right\}$.

Now we prove a theorem that extend what we know about invariant in the usual Galois extension:

Proposition 1.3.13. *Let H be a R-Hopf algebra and S a H-Galois, then $S^H = R$.*

Proof. Form the definition of H-module algebra follows that for all $r \in R$ $h(r) = \varepsilon(h)r$ for all $h \in H$, so $R \subseteq S^H$. Now, we suppose $s \in S^H$; for $t \in S, h \in H$ we have:

$$\begin{aligned} (t\otimes h)\sharp(s\otimes 1) &= \sum th_{(1)}(s)\otimes h_{(2)} = \sum t\varepsilon\left(h_{(1)}\right)s\otimes h_{(2)} \\ &= ts\left(\sum \varepsilon\left(h_{(1)}\right)\otimes h_{(2)}\right) = ts\left(1_S\otimes \sum \varepsilon\left(h_{(1)}\right)h_{(2)}\right) \\ &= ts\otimes h = (s\otimes 1)\sharp(t\otimes h). \end{aligned}$$

Therefore $s\otimes 1$ commutes with all elements $t\otimes h$ and, since j is an isomorphism, also $j(s\otimes 1)$ commutes with all elements $j(t\otimes h)$. So $j(s\otimes 1)$ commutes with all maps in $\mathrm{End}_R(S)$, moreover $j(s\otimes 1) = s\cdot 1_H$ is the multiplication by s, so it must be in R.

□

1.3.1 Base change and Galois descent

In this last paragraph we introduce the concepts of Base change and Galois descent. Although totally general, we restrict ourselves to presenting them for Hopf algebras over fields, this will greatly simplify the exposition.
We want to extend the concept of base change that we have in usual Galois theory, i.e. extending the base field to a larger field while preserving the underlying Hopf-Galois structure. The following theorem will be the pillar on which the Greither-Pareigis's Theorem will be based.

Theorem 1.3.14 (Base Change)**.** *1. Let L/K be a H-Galois fields extension and F a finite fields extension of K; then $(F\otimes L)/F$ is an $(F\otimes H)$-Galois extension.*

2. Let L be a field which is also a H-module algebra over K and F a finite extension of fields of K. If $(F\otimes L)/F$ is $(F\otimes H)$-Galois with action induced by $H\curvearrowright L$, then L/K is H-Galois.

Proof. 1. It is easy to check that $F\otimes H$ is a F-Hopf algebra; we have also that $F\otimes L$ is a F-algebra with component-wise product, and the action induced by $H\curvearrowright L$ makes $F\otimes L$ a $(F\otimes H)$-module algebra: for $f,f',f''\in F, h\in H$ and $l,m\in L$,

$$\begin{aligned}(f\otimes h)((f'\otimes l)(f''\otimes m)) &= (f\otimes h)(f'f''\otimes lm) = ff'f''\otimes h(lm)\\ &= ff'f''\otimes\left(\sum_{(h)} h_{(1)}(l)h_{(2)}(m)\right)\\ &= f\left(\sum_{(h)}\left(f'\otimes h_{(1)}(l)\right)\left(f''\otimes h_{(2)}(m)\right)\right)\\ &= f\left(\sum_{(1\otimes h)}\left(1\otimes h_{(1)}\right)(f'\otimes l)\left(1\otimes h_{(2)}\right)(f''\otimes m)\right),\end{aligned}$$

$$(f\otimes h)(1\otimes 1) = f\otimes h(1) = f\otimes 1\cdot\varepsilon_H(h) = f\varepsilon_H(h)\otimes 1 = \varepsilon(f\otimes h)\otimes 1.$$

It remains to check that the Galois map $j' : (F\otimes L)\otimes_F(F\otimes H)\to \mathrm{End}_F(F\otimes L)$ is an isomorphism. But, recalling that j is an isomorphism, the thesis follows from the commutativity of:

$$\begin{array}{ccc}(F\otimes L)\otimes_F(F\otimes H) & \xrightarrow{j'} & End_F(F\otimes L)\\ \cong\downarrow & & \downarrow\cong\\ F\otimes(L\otimes H) & \xrightarrow[id\otimes j]{} & F\otimes End_K(L)\end{array}$$

2. Here we have only to check that j is an isomorphism. Looking at the above diagram we have that $id \otimes j$ is an isomorphism, therefore, by flatness of F, so is j.

□

Form usual Galois theory we know that if L/K is a finite Galois extension, we know the following:

- let A be a K-vector space, then $A \otimes L$ is a L-vector space;
- let $f : A \to B$ be a homomorphism of K-vector spaces, then:

$$(id \otimes f) : L \otimes A \to L \otimes B,$$
$$(l \otimes a) \mapsto l f(a)$$

  is a homomorphism of L-vector spaces.

More generally, that the same holds with algebras or Hopf algebras instead of vector spaces.
Galois descent, on the other hand, is the inverse process of base change. It involves descending a Galois extension to a smaller field while preserving essential properties and structures. By applying Galois descent, one can explore the Galois theory of the original field using tools and techniques from a smaller field, which often leads to simplifications. So Descent theory provide criteria that determine when one can assert one of the following:

- let A be a L-vector space, then $A \simeq L \otimes A_0$ as L-vector spaces, with A_0 K-vector space,
- if $f : L \otimes A_0 \to L \otimes B_0$ is a L-vector spaces homomorphism, then $f = id_L \otimes f_0$ with $f_0 : A_0 \to B_0 K$-vector spaces homomorphism, (and make analogous assertions for algebras or Hopf algebras).

Now we want to prove the Morita Theorem, because it will be useful in the development of the descent theory. In order to do that we introduce some basic concept in module theory:

Notation 1.3.15. *Let A be a ring, we write ${}_A\mathfrak{M}$ for the category of left A-modules.*

Definition 1.3.16. Let A be a ring, we call *progenerator* a $P \in {}_A\mathfrak{M}$ that satisfy:

1. P is projective and finitely generated,
2. for all $M \in \mathfrak{M}$, exist a set I such that exist $\pi : P^{\oplus I} \twoheadrightarrow M$ epimorphism.

Example 1.3.17. For example $M = A$ is always a progenerator.

Theorem 1.3.18 (Morita)**.** *Let A, B be two rings, then ${}_A\mathfrak{M}$ and ${}_B\mathfrak{M}$ are equivalent iff there is a progenerator $P \in {}_B\mathfrak{M}$ such that* $\mathrm{End}_B(P) = A$

Proof. For the sufficient part: let $F : {}_A\mathfrak{M} \to {}_B\mathfrak{M}$ equivalence of categories and let $P = F(A) \in {}_B\mathfrak{M}$. Now we check that P is a progenerator:

1. Being projective and finitely generated is preserved by the equivalence of category. (Notice that the definition of projective involves only arrows.)

2. Let $M \in {}_B\mathfrak{M}$ and let G be the quasi-inverse equivalence of F. For Example 1.3.17 exist a set I such that exist an epimorphism $\pi : A^{\oplus I} \to G(M)$. Then since F and G are adjoint we have the existence of an epimorphism $\pi' : F(A^{\oplus I}) = P^{\oplus I} \to M$.

In order to conclude notice that:

$$\mathrm{End}_B(P) = \mathrm{End}_A(F(A)) \cong \mathrm{End}_A(A) \cong A.$$

For the necessity part: Let us suppose we have a progenerator $P \in {}_B\mathfrak{M}$ such that $A = \mathrm{End}_B(P)$. We may look at P as a left $A-B$-bimodule thanks to the following product:

$$\begin{aligned} A \times P &\longrightarrow P \\ (f, p) &\longmapsto f(p) \end{aligned}$$

Now we consider the two following functor:

$$\begin{aligned} F = \mathrm{Hom}_B(P, \_) : {}_B\mathfrak{M} &\longrightarrow {}_A\mathfrak{M}, \\ G = \_ \otimes_A P : {}_A\mathfrak{M} &\longrightarrow {}_B\mathfrak{M}. \end{aligned}$$

For a famous result of category theory we know that G is left adjoints to F, sometimes this adjunction is called “tensor-hom adjunction".
In order to show that F and G are inverse of each other we may consider :

$$\begin{aligned} \mathrm{Nat}(F, F) &\xrightarrow{\cong} \mathrm{Nat}(GF, Id) \\ Id_F &\longmapsto \varepsilon \end{aligned}$$

$$\begin{aligned} \mathrm{Nat}(G, G) &\xrightarrow{\cong} \mathrm{Nat}(FG, Id) \\ Id_G &\longmapsto \eta \end{aligned}$$

where, for any $Y \in {}_B\mathfrak{M}$ and $X \in {}_A\mathfrak{M}$:

$$\begin{aligned} \varepsilon_Y : \mathrm{Hom}_B(P, Y) \otimes P &\longrightarrow Y \\ \varphi \otimes p &\longmapsto \varphi(p) \end{aligned}$$

$$\begin{aligned} \eta_X : X &\longrightarrow \mathrm{Hom}_B(P, X \otimes P) \\ x &\mapsto (p \longmapsto x \otimes p) \end{aligned}$$

are the counite and unite. The goal is to check that ε_Y and η_X are isomophism. We do it for ε_Y, the other case is similar. We start noticing that for $Y = P$ ε_P is an isomorphism:

$$\begin{aligned} \varepsilon_P : \mathrm{Hom}_B(P,P) \otimes P &\longrightarrow P \\ \varphi \otimes p &\longmapsto \varphi(p) = \varphi \cdot p. \end{aligned}$$

where we use $A = \mathrm{End}_B(P)$ and the structure of P as an A-module. Now using the fact that P is a progenerator we have that, for any $Y \in {}_B\mathfrak{M}$, exists I_1, I_2 such that there is an exact sequence:

$$\begin{array}{ccccccc} P^{\oplus I_2} & \longrightarrow & P^{\oplus I_1} & \twoheadrightarrow & Y & \longrightarrow & 0 \\ \downarrow & \nearrow & & & & & \\ \mathrm{Ker}(\pi) & & & & & & \end{array}$$

Since P is projective we know that F is an exact functor and commute with direct sum. On the other hand G is right exact and commutes with coproduct. So we get the following commutative diagram:

$$\begin{array}{ccccccc} GF(P)^{\oplus I_2} & \longrightarrow & GF(P)^{\oplus I_1} & \longrightarrow & GF(Y) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varepsilon_P^{\oplus I_2}} & & \downarrow{\scriptstyle \varepsilon_P^{\oplus I_1}} & & \downarrow{\scriptstyle \varepsilon_Y} & & \\ P^{\oplus I_2} & \longrightarrow & P^{\oplus I_1} & \longrightarrow & Y & \longrightarrow & 0. \end{array}$$

Thus, being ε_P an isomorphism we conclude that ε_Y is an isomorphism using the snake lemma. □

Remark 1.3.19. Let S be a finite K-algebra and M a left E-module, then $\mathrm{Hom}_E(S,E) \otimes_E M \simeq \mathrm{Hom}_E(S,M)$. Indeed, if we fix M, the equality holds for $S = E$, hence for a free E-module, hence for a projective E-module. Then it holds for S.

Then from Morita Theorem and the previous remark, it follows:

Corollary 1.3.20. *Let K be a field, S a finite K-algebra and $E \coloneqq \mathrm{End}_K(S)$. Then the covariant functors*

$$\begin{aligned} S \otimes_K \_ : {}_K\mathfrak{M} &\longrightarrow {}_E\mathfrak{M} \\ \mathrm{Hom}_E(S,E) \otimes_E \_ : {}_E\mathfrak{M} &\longrightarrow {}_K\mathfrak{M} \end{aligned}$$

define an equivalence of categories between ${}_K\mathfrak{M}$ and ${}_E\mathfrak{M}$.

This theorem immediately tell us something about descended modules:

Corollary 1.3.21. *Let S be a finite K-algebra, then a S-module M descends iff the S-action on M can be extended to an action on $\mathrm{End}_K(S)$ on M.*

Now if L/K is a Galois extension with Galois group G (i.e. $j : L \otimes KG \to \mathrm{End}_K(L)$ is an isomorphism), then a left $\mathrm{End}_K(L)$-module is simply a L-vector space with a compatible action of G (i.e. so that for all $m \in M$, $\sigma \in G$ and $s \in S$ $\sigma(sm) =$

$\sigma(s)\sigma(m)$.). In this case we see that the inverse of the base change functor is given by the functor: $M \to M^G$. This can be generalized for Hopf-Galois as shown by the following:

Proposition 1.3.22. *Let S be a finite commutative K-algebra and a H-Galois. We find that for any $M \in {}_E\mathfrak{M}$, M is isomorphic to $S \otimes M^H$ via the map $s \otimes m \mapsto ms$.*

Proof. By Corollary 1.3.20 we have:

$$M \cong S \otimes_K \mathrm{Hom}_E(S, E) \otimes_E M.$$

Furthermore, using $(E, \circ) \simeq (S \otimes H, \#)$ as algebras, we get $\mathrm{Hom}_E(S, M) \simeq \mathrm{Hom}_{S\otimes H}(S, M)$ and so:

$$M \simeq S \otimes_K \mathrm{Hom}_{S\otimes H}(S, M).$$

We claim that $\mathrm{Hom}_{S\otimes H}(S, M) \cong M^H$ via the map:

$$\begin{aligned} \varphi : \mathrm{Hom}_{S\otimes H}(S, M) &\longrightarrow M^H \\ \phi &\longmapsto \varphi(1). \end{aligned}$$

For any $s \in S$ we have $(s \otimes 1)1 = s$ and so $\varphi(s) = \phi((s \otimes 1)1) = (s \otimes 1)\varphi(1)$. This imply that phi is completely determined by the value in 1. Now, for $h \in H$, we have:

$$h\varphi(1) = (1 \otimes h)\varphi(1) = \varphi((1 \otimes h)1) = \varphi(\varepsilon(h)1) = \varepsilon(h)\varphi(1)$$

so $\phi(1) \in M^H$. We have that φ is well defined and injective. The surjectivity follows from the fact that for $m \in M^H$, m is the image of $\phi : s \mapsto sm$. □

The above proposition tell us that the functor $(\_)^H$ is the inverse of the base change module. Then, there is an equivalence of categories:

$$\begin{aligned} {}_R\mathcal{M} &\longrightarrow {}_E\mathcal{M} \\ N &\longmapsto S \otimes_R N \end{aligned}$$

$$\begin{aligned} {}_E\mathcal{M} &\longrightarrow {}_R\mathcal{M} \\ M &\longmapsto M^H. \end{aligned}$$

Definition 1.3.23. Let L/K be a Galois extension with group G and A is a L-vector space, we say that A is a *G-compatible L-vector space* if it is a KG-module and the structure map of A is G-equivariant, i.e. $s \circ (g\cdot) = (g\cdot) \circ s$ for every $g \in G$, where $s : L \otimes A \to A$ is the scalar multiplication and G acts on $L \otimes A$ diagonally.

This definition is justified by:

Proposition 1.3.24. *We have the following equivalences:*

1. *A is a $(L\otimes KG)$-module iff A is a G-compatible L-vector space;*

2. *$f : A \to B$ is a $(L\otimes KG)$-modules homomorphism iff f is a L-linear map G-equivariant.*

Proof. 1. Suppose that A is a $(L\otimes KG)$-module, so

$$\begin{aligned}\phi : L\otimes KG &\longrightarrow \mathrm{End}(A)\\ l\otimes\sigma &\longmapsto \varphi_{l\sigma} : a \mapsto l\sigma(a)\end{aligned}$$

is a rings homomorphism. Restricting this module action to $\{l\otimes 1\}_{l\in L}$ and $\{1\otimes\sigma\}_{\sigma\in G}$ we get a L-module structure and a KG-module structure on A given by $\phi(l\otimes 1)=\varphi_l$ and $\phi(1\otimes\sigma)=\varphi_\sigma$, respectively. Since $\phi((1\otimes\sigma)\sharp(l\otimes 1)) = \phi(1\otimes\sigma)\circ\varphi(l\otimes 1)$, i.e. $\varphi_{\sigma(l)\sigma}=\varphi_\sigma\circ\varphi_l$, for all $a\in A$

$$\sigma(la)=\varphi_\sigma\left(\varphi_l(a)\right)=\varphi_{\sigma(l)\sigma}(a)=\sigma(l)\sigma(a).$$

Note that the above condition is exactly the G-equivariance of the scalar multiplication of A, so A is a G-compatible L-vector space. On the contrary, let A be a G-compatible L-vector space, so that we have the modules actions $\phi_L : L\to\mathrm{End}(A), \varphi_L(l)(a)=\varphi_l(a)=la$ and $\phi_G : KG\to\mathrm{End}(A)$, $\phi_G(\sigma)(a)=\varphi_\sigma(a)=\sigma(a)$. As we now show, the diagonal G-action on $L\otimes A$ allows us to extend the L-module action over A to a $(L\otimes KG)$-module action over A. Firstly we note that any $l\otimes\sigma\in L\otimes KG$ can be written as $l\otimes\sigma=(1\otimes\sigma)\sharp\left(\sigma^{-1}(l)\otimes 1\right)$; thus we define

$$\begin{aligned}\phi : L\otimes KG &\longrightarrow \mathrm{End}(A)\\ l\otimes 1 &\longmapsto \varphi_l\\ 1\otimes\sigma &\longmapsto \varphi_\sigma\\ l\otimes\sigma &\longmapsto \varphi_{l\sigma}:=\varphi_\sigma\circ\varphi_{\sigma^{-1}(l)},\end{aligned}$$

so that $\varphi_{l\sigma}(a)=\varphi_\sigma\left(\varphi_{\sigma^{-1}(l)}(a)\right)=\sigma\left(\sigma^{-1}(l)a\right)=l\sigma(a)$. We now check that ϕ is a ring homomorphism: for $l,m\in L,\sigma,\tau\in G, a\in A$ we have

$$\begin{aligned}\phi((l\otimes\sigma)\sharp(m\otimes\tau))(a)&=\phi(l\sigma(m)\otimes\sigma\tau)(a)=\varphi_{l\sigma(m)\sigma\tau}(a)=l\sigma(m)\sigma\tau(a)\\ (\phi(l\otimes\sigma)\circ\varphi(m\otimes\tau))(a)&=\left(\phi_{l\sigma}\circ\varphi_{m\tau}\right)(a)=\phi_{l\sigma}(m\tau(a))=l\sigma(m\tau(a)),\end{aligned}$$

and, by compatibility of the G-action, $l\sigma(m)\sigma\tau(a)=l\sigma(m\tau(a))$. Thus ϕ is a rings homomorphism.

2. Let f be a $(L \otimes KG)$-modules homomorphism between A and B. A and B, endowed with the structure defined in the proof of 1), are G-compatible L-vector spaces. Therefore f is an homomorphism of G-compatible L-vector spaces iff it is both L-linear and G-equivariant.

□

Since a $(L \otimes KG)$-module is a G-compatible L-vector space, for A a L-vector space we have:

A descends $\Leftrightarrow$ the L-action on A extends to a $(L \otimes KG)$-action on $A \Leftrightarrow G$ acts on A compatibly with the L-vector space structure.

In this case, by Morita's theorem and Proposition 1.3.22 we have $A \simeq L \otimes A^G$, where A^G is a K-vector space. The functors of Morita's theorem can be applied also to maps; for A, B two $(L \otimes KG)$-modules and $f : A \to B$ a L-linear map, we have

$$\begin{aligned} f \text{ descends } &\Leftrightarrow f \text{ is a } (L \otimes KG)\text{-modules homomorphism} \\ &\Leftrightarrow f \text{ is } G\text{-equivariant,} \end{aligned}$$

and in this case $f = id_L \otimes f_0$, where $f_0 : A^G \to B^G$ is a K-linear map.

Thus, if A is a $(L \otimes KG)$-module and we have a commutative diagram involving only $(L \otimes KG)$-modules and $(L \otimes KG)$-modules homomorphisms and which defines a property for A, then we have the same commutative diagram for fixed spaces through the functor $(*)^G$ and so the property holds also for fixed space A^G.

Definition 1.3.25. Let A be a L-algebra (or a L-Hopf algebra), we say that A is a *G-compatible* L-algebra (resp. L-Hopf algebra) if A is a KG-module and the structure maps of A are G-equivariant (here G acts diagonally on $A \otimes A$).

Let A be a G-compatible (Hopf) algebra over a field L then for the structure maps we have the diagram:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu \otimes id} & A \otimes A \\ {\scriptstyle id \otimes \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow[\mu]{} & A \end{array}$$

then applying the functor $(\_)^G$ we have the following commutative diagram:

$$\begin{array}{ccc} (A \otimes A \otimes A)^G & \xrightarrow{\mu \otimes id} & (A \otimes A)^G \\ {\scriptstyle id \otimes \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ (A \otimes A)^G & \xrightarrow[\mu]{} & A^G \end{array}$$

Remember that $A^G \otimes A^G \otimes A^G$ embeds in $(A \otimes A \otimes A)^G$, so this last diagram enrich A^G with a structure of (Hopf) algebra over L.

Now, let H be a Hopf algebra over L and A a L-algebra which is also a H module algebra, i.e. the properties $h(ab) = \mu(\Delta(h)(a \otimes b))$ and $h(1) = \varepsilon(h) \cdot 1$ hold. Both this properties can be expressed by commutative diagrams, so working as before we have that if H and A are a G-compatible (Hopf) algebras and that the module algebra action is G-equivariant, then we can enrich A^G with a structure of H^G-module algebra.

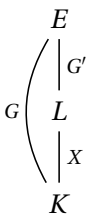
CHAPTER 2

Hopf Galois Theory

In the previous chapter we have generalized the concept of Galois extension, this new extension has some difference with classic Galois theory, for example a fields extension can be Hopf Galois for different Hopf algebras H. In this chapter we want to determinate all possible Hopf Galois structures for a given fields extension. In order to do this we will follow the path lined by the fathers of the so-called separable Hopf-Galois theory, Greither and Pareigis in [PG87]. Remember that we always consider finite and separable extension.

Framework

We want to characterize the Hopf Galois structures H for a fields extension, L/K, of degree n. We will refer to the following setup as $(\star)$:



L/K fields extension
E normal closure of L/K
$G = Gal(E/K)$
$G' = Gal(E/L)$
$X = G/G'$ set of coset

By Primitive Element theorem, there exist $\alpha \in L$ such that $L = K(\alpha)$, and a polynomial μ_α that is the minimal polynomial of α over K. If we call $\alpha_1, ..., \alpha_n$ the roots of μ_α we have that $E = K(\alpha_1, ..., \alpha_n)$. We will use the left translation map:

$$\begin{aligned} \lambda : G &\longrightarrow \mathrm{Perm}(X) \\ \sigma &\longmapsto \lambda_\sigma : \bar{\tau} \mapsto \overline{\sigma\tau}, \end{aligned}$$

which allows us to think of G as a subgroup of $\mathrm{Perm}(X)$.

Lemma 2.0.1. *The translation map λ is injective.*

Proof. We have

$$\begin{aligned}&\mathrm{Ker}(\lambda) = \{\sigma \in G : \lambda_\sigma = id_X\} = \{\sigma \in G : \lambda_\sigma(\bar{\tau}) = \bar{\tau} \forall \bar{\tau} \in X\}\\ &\subseteq \left\{\sigma \in G : \lambda_\sigma(\overline{1}) = \overline{1}\right\} = \{\sigma \in G : \bar{\sigma} = \overline{1}\} = G'.\end{aligned}$$

Moreover $M = \mathrm{Ker}(\lambda) \lhd G$, so E^M/K is a normal extension; since $M \subseteq G' \subseteq G$, $E^G = K \subseteq E^{G'} = L \subseteq E^M$. The latter inclusion, together with E^M/K being a normal extension, implies, since E is the normal closure of L/K, that $E = E^M$, and so M is trivial. □

We have defined λ using the left action, but we can also consider the right one, which define an injective group homomorphism as well:

$$\begin{aligned}\rho : G &\longrightarrow \mathrm{Perm}(X)\\ \sigma &\longmapsto \lambda_\sigma : \bar{\tau} \mapsto \overline{\tau\sigma},\end{aligned}$$

2.1 Special case

We start with a characterization of the Hopf Galois structures for a special type of extensions. This section is based on section 6 of [Chi00].

We start giving some definition of group theory:

Definition 2.1.1. Let X be a finite set and $\mathrm{Perm}(X)$ its permutation group. A subgroup $N < \mathrm{Perm}(X)$ is regular if two of the following conditions hold:

- $|N| = |X|$
- the action $N \curvearrowright X$ is transitive;
- $\mathrm{Stab}_N(x) = id_N$ for all $x \in X$.

The action $N \curvearrowright X$ and a fixed $x \in X$ yields a map $\cdot x : N \to X$. It is easy to note that N is regular iff the map $\cdot x$ is a bijection for every x.

Notation 2.1.2. *Let E be a field, X a finite set. We will write XE for the E-vector space* $\mathrm{Map}(X, E) = \{f : X \to E\}$.

An orthogonal basis for XE is given by $\{u_x : x \in X\}$, where:

$$\begin{aligned}u_x : X &\longrightarrow E\\ y &\longmapsto \delta_{x,y}.\end{aligned}$$

Since E is a field we can see XE as E-algebra with componentwise multiplication; in this way we have that all u_x are idempotents.

Definition 2.1.3. For any $x \in X$ we call u_x *primitive idempotents.*

The name is justified by the following:

Remark 2.1.4. Note that if $f \in XE$ is idempotent, $f = \sum_{x\in X} a_x u_x$ and we have

$$\sum_{x\in X} a_x u_x = f = f^2 = \sum_{x,y\in X} a_x a_y u_x u_y = \sum_{x\in X} a_x^2 u_x$$

that is, each $a_x \in E$ must be idempotent, i.e. $a_x = 0$ or $a_x = 1$, and so $f = \sum_{y\in Y} u_y$ for $Y \subseteq X$

Theorem 2.1.5. *Let E be a field, X a finite set. We have:*

1. *if XE/E is Hopf Galois with Hopf-algebra H, then H is a group ring EN, where N is (identified with) a regular subgroup of* $\mathrm{Perm}(X)$*;*
2. *if N is a regular subgroup of* $\mathrm{Perm}(X)$*, then XE/E is EN-Galois.*

Proof. □

1. Recalling that an extension is H-Galois iff is an H^*-Galois object, we have the following E-vector spaces isomorphisms (where $n = |X|$):

   $$\underbrace{E \times \cdots \times E}_{n^2 \text{ times}} \simeq \mathrm{Map}(X \times X, E) \simeq XE \otimes_E XE \simeq XE \otimes_E H^* \simeq \underbrace{H^* \times \cdots \times H^*}_{n \text{ times}}$$

   It is easy to check that they are all isomorphisms of E-algebras as well. Thanks to the finite-dimensional assumption the decomposition of a semisimple algebra in simple algebras is unique, thus we get that $H^* \simeq E \times \cdots \times E$ as algebras. Since a basis for $(E \times \cdots \times E)^*$ is given by π_i for $i = 1, \ldots, n$ (where π_i is the projection on the i-th coordinate), a basis for H^{**} is given by: for $i = 1, \ldots, n$

   $$\nu_i : H^* \xrightarrow{\simeq} E \times \cdots \times E \xrightarrow{\pi_i} E.$$

   We know that the ν_i are algebras homomorphisms and so, by 1.1.45, they are grouplike elements of H^{**}. We also know that $H^{**} \simeq H$, therefore we can identify $N = \{\nu_i : i = 1, \ldots, n\}$ with a basis for H made by grouplike elements. All in all, since N is a basis of H and it is made up of grouplike elements, that are independent by proposition 1.1.30 N consists of all grouplike elements in H. For Proposition 1.1.29 N is a group, so H is the group algebra EN.

   Claim 1. (N is a a subgroup of $\mathrm{Perm}(X)$) Since XE/E is H-Galois we have that $H = EN$ acts on XE as a modulo algebra. We will show that this action restrict to $\mathscr{B} = \{u_x : x \in X\}$ obtaining:

   $$N \times \mathscr{B} \longrightarrow \mathscr{B}$$
   $$(\nu, u_x) \longmapsto \nu(u_x) = u_y \text{ for some } y \in X.$$

Now, since $\mathscr{B}$ is indexed by X, we rewrite this action as the injective homomorphism:

$$\begin{aligned} N &\longrightarrow \mathrm{Perm}(X) \\ \nu &\longmapsto : x \mapsto y \text{ if } \nu(u_x) = u_y, \end{aligned}$$

We start looking at action of N on $\mathscr{B}$:

$$\begin{aligned} &\nu(u_x)\,\nu(u_x) = \mu((\Delta(\nu))(u_x \otimes u_x)) = \nu(u_x u_x) = \nu(u_x) \\ &\nu(u_x)\,\nu\left(u_y\right) = \nu\left(u_x u_y\right) = 0 \text{ for } x \neq y. \end{aligned}$$

So ν maps primitive idempotents of XE in orthogonal idempotents of XE. We want to show that for every x there exists y such that $\nu(u_x) = u_y$, in order to do that we prove that $\nu(u_x)$ are primitive. It is easy to check that $1_{XE} = \sum_x u_x$, moreover $\nu(1_{XE}) = \varepsilon(\nu)1_{XE} = 1_{XE}$ (where we have used the Proposition 1.1.29); combining these two equalities:

$$1_{XE} = \nu(1_{XE}) = \nu\left(\sum_{x\in X} u_x\right) = \sum_{x\in X} \nu(u_x)$$

Notice that this imply that each $\nu(u_x)$ is not zero, because $u_x = 1_N(u_x) = \nu\nu^{-1}(u_x)$.
So, $\nu(u_x) \neq 0$) and idempotent, therefore exist some $Y \subseteq X$ such that $\nu(u_x) = \sum_{y\in Y} u_y$. Since $\nu(u_x)$ are orthogonal we have that an element of $\mathscr{B}$ can appear in one and only one of the $\{\nu(u_x)\}_{x\in X}$. So $|Y| = 1$ and for any $x \in X$ exist a $y \in X$ such that $\nu(u_x) = u_y$.

Claim 2: (N is regular) By definition of regular we have to prove that $|N| = |X|$ and $N \curvearrowright X$ is transitive. The first follows from $\dim_E(EN) = \dim_E(XE)$.
For the second statement we suppose, on the contrary, that the action is not transitive, i.e. $Nu_x = \left\{u_y : y \in Y\right\}$ for $Y \subsetneq X$. By assumption the Galois map:

$$\begin{aligned} j : XE \otimes EN &\longrightarrow \mathrm{End}_E(XE) \\ u_t \otimes \nu_i &\longmapsto j(u_t \otimes \nu_i) : u_x \mapsto u_t \nu_i(u_x) \end{aligned}$$

is bijective. The contradiction will come by seeing that j is not surjective. Let z be an element in $X \setminus Y$; we definite the elements e_{xz} in $\mathrm{End}_E(XE)$ to be $e_{xz}(u_x) = u_z$ and $e_{xz}\left(u_y\right) = 0$ for $y \neq x$. By bejectivity of j it must exist an element $\alpha = \sum_{z,\nu} \alpha_{z,\nu} u_z \otimes \nu \in XE \otimes EN$ such that $j(\alpha) = e_{xz}$. For a general α we have:

$$\begin{aligned} j(\alpha) &= j\left(\sum_{z,\nu} \alpha_{z,\nu} u_z \otimes \nu\right) \\ &= \sum_{z,\nu} \alpha_{z,\nu} u_z \nu(u_x) \\ &= \sum_{y\in Y} \alpha_y u_y \end{aligned}$$

We conclude noticing that $e_{xz}(u_x) = u_z \notin \langle \{u_y : y \in Y\} \rangle$.

2. Let $x, z \in X$ and e_{xz} defined as above, then we have that $\mathfrak{B} = \{e_{xz} : x, z \in X\}$ is an E-basis for $\mathrm{End}_E(XE)$. Moreover, by regularity of N we know that exist $\nu \in N$ such that $\nu(x) = z$. We want to prove that the Galois map j is surjective, this will be sufficient since $|N| = |X|$ by regularity and so $dim_E(XE \otimes EN) = dim_E(End_E(XE))$. For the surjectivity is sufficient to notice that $\mathfrak{B} \subset \mathrm{Im}(j)$, but we know that for a $\nu \in N$ as above we have $j(u_z \otimes \nu) = e_{xz}$.

2.2 Greither-Pareigis's Theorem

In This section we finally prove Greither-Pareigis's Theorem in the setting $(\star)$.

Notation 2.2.1. *We will simply say G-module for KG-module.*

Example 2.2.2. $(E \otimes L)$ is a G-module by G-action on the first component. Note that $XE = \mathrm{Map}(X, E) = \mathrm{Hom}_E(EX, E)$, and G acts both on E and EX, so G acts on $\mathrm{Hom}_E(EX, E) = XE$:

$$\sigma(f)(y) = \sigma\left(f\left(\sigma^{-1}(y)\right)\right)$$

for $\sigma \in G, f \in \mathrm{Hom}_E(EX, E)$ and $y \in EX$.

The idea of Greither and Pareigis is based on the used of Base change: the strategy is to classify those Hopf Galois structures on $(E \otimes L)/E$ on which G acts, and then take the ring of invariants under the G-action. This strategy is facilitated by the special form of $E \otimes L$, and $E \otimes H$.

Proposition 2.2.3. *Suppose to be in the setup $(\star)$, then we have that:*

$$\begin{aligned} \varphi : E \otimes L &\longrightarrow XE \\ e \otimes l &\longmapsto \varphi(e \otimes l) : \bar{\sigma} \mapsto e\sigma(l) \end{aligned}$$

is a E-algebras and G-modules isomorphism.

Proof. The map φ is well-defined: if $\bar{\sigma} = \bar{\tau}$, then $\sigma = \tau\rho'$ for some $\rho' \in G'$ and, since $L = E^{G'}$, we have $\sigma(l) = \tau\left(\rho'(l)\right) = \tau(l)$. Now we prove that φ:

- is a E-algebras homomorphism: φ is E-linear by definition. We need to check that it preserves the multiplication: $\forall \overline{\sigma} \in G/G'$, $e \otimes l, e' \otimes l'$

$$\begin{aligned} \varphi((e \otimes l)(e' \otimes l'))(\overline{\sigma}) &= \varphi((ee') \otimes (ll'))(\overline{\sigma}) = (ee')\sigma(ll') \\ &= (ee')\sigma(l)\sigma(l') = (e\sigma(l))(e'\sigma(l')) \\ &= (\varphi(e \otimes l)(\overline{\sigma})\varphi(e' \otimes l')(\overline{\sigma}) = (\varphi(e \otimes l)\varphi(e' \otimes l'))(\overline{\sigma}) \end{aligned}$$

- is a G-module homomorphism: for every $\tau \in G$ we have:

$$\begin{aligned}\tau \cdot (\varphi(e \otimes l))(\bar{\sigma}) &= \tau\left(\varphi(e \otimes l)(\overline{\tau^{-1}\sigma})\right) = \tau\left(e(\tau^{-1}\sigma)(l)\right) \\ &= \tau(e)\tau\left(\tau^{-1}(\sigma(l))\right) = \tau(e)\sigma(l) \\ &= \varphi(\tau(e) \otimes l)(\bar{\sigma}) = \varphi(\tau \cdot (e \otimes l))(\bar{\sigma}).\end{aligned}$$

- is bijective: Let $\{l_i\}_{i=1,\dots,n}$ be a K-basis for L; thus $\{1 \otimes l_i\}_{i=1,\dots,n}$ is a E-basis for $E \otimes L$ and so we can write $\alpha = \sum e_i \otimes l_i$ for every $\alpha \in E \otimes L$. If $\alpha \in \mathrm{Ker}(\varphi)$, then $\varphi(\alpha) = 0$, that is, $\sum_i e_i \sigma(l_i) = 0$ for all $\sigma \in G$. Therefore e_i is zero for every i and φ is injective. For dimensional reasons it has to be bijective.

□

Notation 2.2.4. *Let L/K be a H-Hopf Galois extension we will sometimes refer to the module algebra action $H \otimes L \to L$ as Hopf action.*

We are now ready to state the following fundamental result:

Proposition 2.2.5. *Suppose to be in the setup $(\star)$ and that L/K is H-Galois; the base change action*

$$\alpha : (E \otimes H) \otimes_E (E \otimes L) \longrightarrow E \otimes L$$

is equivalent to an action

$$\alpha' : EN \otimes_E XE \longrightarrow XE$$

which corresponds to a regular embedding $N \hookrightarrow \mathrm{Perm}(X)$ such that the image of N in $\mathrm{Perm}(X)$ is normalized by $\lambda(G)$, where λ is the left translation.

Proof. Notice that we know two actions on XE. On one hand, we have the action of G over XE as described in Remark 2.2.2. Let us look at the action of G on the elements of the basis $\{u_{\bar{\sigma}} : \bar{\sigma} \in G/G'\}$:

$$\sigma(u_{\bar{\tau}})(\bar{\rho}) = \sigma\left(u_{\bar{\tau}}(\overline{\sigma^{-1}\rho})\right) = u_{\bar{\tau}}(\overline{\sigma^{-1}\rho}) = u_{\overline{\sigma\tau}}(\bar{\rho}) = u_{\lambda_\sigma(\bar{\tau})}(\bar{\rho}).$$

Since $\sigma(u_{\bar{\tau}}) = u_{\lambda_\sigma(\bar{\tau})}$, the G-action on $\{u_{\bar{\sigma}}\}_{\bar{\sigma} \in G/G'}$ corresponds to the left translation. On the other hand, as described in the proof of Theorem 2.1.5, N acts on the basis $\{u_{\bar{\sigma}} : \bar{\sigma} \in G/G'\}$ by

$$\nu(u_{\bar{\sigma}}) = u_{\nu(\bar{\sigma})}.$$

This N-action on $\{u_{\bar{\sigma}}\}_{\bar{\sigma} \in G/G'}$ corresponds to an embedding $N \hookrightarrow \mathrm{Perm}(X)$.

Claim 1: G acts on N

The Galois action $G \curvearrowright E$ gives a G-modules structure on $E \otimes L$ and $E \otimes H$ acting on first components. It is immediate to check that $E \otimes L$ is a G-compatible E-algebra, $E \otimes H$ is a G-compatible E-Hopf algebra and using that the action is componentwise, that the action α is G-equivariant. Theorem 2.1.5 imply that $E \otimes H \simeq EN$ and Proposition 2.2.3 imply that $E \otimes L \simeq XE$ via φ so the Hopf action α is isomorphic to a G-equivariant Hopf action:

$$\alpha' : EN \otimes_E XE \to XE.$$

Moreover, since $E \otimes H \simeq EN$ as Hopf algebras, G acts on EN with a G-compatible action. So, if Δ is the comultiplication of EN we have:

$$\sigma(\Delta(\nu)) = \Delta(\sigma(\nu))$$

Recall that N is the set of grouplike elements of EN, thus $\sigma(\nu) \otimes \sigma(\nu) = \Delta(\sigma(\nu))$ and G acts on N.

Claim 2: The cation of G over N is via conjugation by λ

Let us look now at the action defined above; by G-equivariance we have:

$$\sigma\left(\nu\left(u_{\bar{\tau}}\right)\right) = \sigma(\nu)\sigma\left(u_{\bar{\tau}}\right),$$

and writing explicitly the actions of N and G on the $\{u_{\bar{\sigma}}\}_{\bar{\sigma} \in G/G'}$, we get:

$$\begin{aligned} \sigma\left(\nu\left(u_{\bar{\tau}}\right)\right) &= \sigma\left(u_{\nu(\bar{\tau})}\right) = u_{\lambda_\sigma(\nu(\bar{\tau}))}, \\ \sigma(\nu)\sigma\left(u_{\bar{\tau}}\right) &= (\sigma(\nu))\left(u_{\lambda_\sigma(\bar{\tau})}\right) = u_{(\sigma(\nu))\left(u_{\lambda_\sigma(\bar{\tau})}\right)}. \end{aligned}$$

Hence $\lambda_\sigma(\nu(\bar{\tau})) = (\sigma(\nu))\left(u_{\lambda_\sigma(\bar{\tau})}\right)$, that is, $(\sigma(\nu))(\bar{\tau}) = \left(\lambda_\sigma \nu \lambda_{\sigma^{-1}}\right)(\bar{\tau})$, and $\sigma(\nu) = \lambda_\sigma \nu \lambda_{\sigma^{-1}}$, as desired. □

The theorem of Greither and Pareigis asserts that the above proposition has converse:

Theorem (Greither-Pareigis)**.** *Suppose to be in the setup* $(\star)$*, then there is a bijective correspondence between Hopf Galois structures on* L/K *and regular subgroups of* $\mathrm{Perm}(X)$ *normalized by* $\lambda(G)$*. The bijection is given by:*

$$\begin{aligned} \{H \text{ Hopf Galois strucure on } L/K\} &\longleftrightarrow \{N < Perm(X) \mid N \text{ is normalized by } \lambda(G)\} \\ H &\longmapsto N \simeq G(E \otimes H) \\ E[N]^G &\longleftarrow N. \end{aligned}$$

Proof. By Proposition 2.2.5, to prove the statement we have only to check that if we have a regular subgroup N of $\mathrm{Perm}(X)$ normalized by $\lambda(G)$, we can find a unique Hopf Galois structure H on L/K.

Claim 1: The base change action is G-equivariant.

Since N is regular, by Theorem 2.1.5, XE/E is EN-Galois, so that the Hopf action is defined on the basis as:

$$\begin{aligned} \alpha : EN \otimes_E XE &\longrightarrow XE \\ \nu \otimes u_{\overline{\sigma}} &\longmapsto \nu(u_{\overline{\sigma}}) = u_{\nu(\overline{\sigma})}. \end{aligned}$$

We want to show that XE and EN are G-compatible E-vector spaces and α is G-equivariant. Notice that XE, with the action of G defined in example 2.2.2 is a G-compatible E-vector space:

$$\sigma(ef)(\bar{\tau}) = \sigma(e)\sigma\left(f\left(\lambda_{\sigma^{-1}}(\bar{\tau})\right)\right) = \sigma(e)\sigma(f)(\bar{\tau}).$$

Similarly, we have that EN, with the action defined in Proposition 2.2.5 is a G-compatible E-vector space:

$$\sigma\left(e'(e\nu)\right) = \sigma\left(e'e\nu\right) = \sigma\left(e'\right)\sigma(e)\sigma(\nu) = \sigma\left(e'\right)\sigma(e\nu).$$

Finally, we check that the E linear map α is G-equivariant, i.e. $\alpha(\sigma(e\nu \otimes f))(\bar{\tau}) = \sigma(\alpha(e\nu \otimes f))(\bar{\tau})$. The left hand side:

$$\begin{aligned} \alpha(\sigma(e\nu \otimes f))(\bar{\tau}) &= (\sigma(e\nu)\sigma(f))(\bar{\tau}) = \sigma(e)\sigma(f)\left(\sigma(\nu)^{-1}(\bar{\tau})\right) \\ &= \sigma(e)\sigma\left(f\left(\lambda_{\sigma^{-1}}\left(\sigma(\nu)^{-1}(\bar{\tau})\right)\right)\right) \\ &= \sigma(e)\sigma\left(f\left(\lambda_{\sigma^{-1}}\lambda_{\sigma}\nu^{-1}\lambda_{\sigma^{-1}}\right)(\bar{\tau})\right) \\ &= \sigma(e)\sigma\left(f\left(\nu^{-1}\lambda_{\sigma^{-1}}\right)(\bar{\tau})\right) \end{aligned}$$

where we have used that N is normalized by $\lambda(G)$. The left hand side:

$$\begin{aligned} \sigma(\alpha(e\nu \otimes f))(\bar{\tau}) = \sigma(e\nu f)(\bar{\tau}) &= \sigma(e)\sigma\left((\nu f)\left(\lambda_{\sigma^{-1}}(\bar{\tau})\right)\right) \\ &= \sigma(e)\sigma\left(f\left(\nu^{-1}\left(\lambda_{\sigma^{-1}}(\bar{\tau})\right)\right)\right) = \sigma(e)\sigma\left(f\left(\nu^{-1}\lambda_{\sigma^{-1}}\right)(\bar{\tau})\right). \end{aligned}$$

Then, by Proposition 1.3.24 we have that XE and EN are $(E \otimes KG)$-modules and the action α, being G-equivariant, is an $(E \otimes KG)$-modules homomorphism.

Claim 2: The extension $(XE)^G/K$ is Hopf Galois

Since E/K is a Galois extension with group G, it follows that $\mathrm{End}_K(E) \simeq E \otimes KG$. For Morita's theorem, we have that there is a equivalence of category between K-vector space and $E \otimes KG$-modules, so in particular we have that the $(E \otimes KG)$-modules homomorphism α corresponds to a unique K-vector spaces homomorphism:

$$\alpha^G : (EN)^G \otimes_K (XE)^G \longrightarrow (XE)^G.$$

It an easy verification that XE is a G-compatible E-algebra and EN is a E-compatible E-Hopf algebra; then $(XE)^G$ is a K-algebra and $(EN)^G$ is a K-Hopf algebra. Moreover, since α is a module algebra action, so is α^G. By Proposition 1.3.22 we know that $E\otimes_K (EN)^G \simeq EN, E\otimes_K (XE)^G \simeq XE$; so from the isomorphism $j : XE\otimes_E EN \to \mathrm{End}_E(XE)$, we get the isomorphism:

$$\left(E\otimes_K (XE)^G\right)\otimes_E \left(E\otimes_K (EN)^G\right) \simeq \mathrm{End}_E\left(E\otimes_K (XE)^G\right).$$

which is the same as:

$$E\otimes_K \left((XE)^G\otimes_K (EN)^G\right) \simeq E\otimes_K \mathrm{End}_K\left((XE)^G\right).$$

Now, by flatness of E, the map

$$j^G : (XE)^G\otimes_K (EN)^G \longrightarrow \mathrm{End}_K\left((XE)^G\right)$$

is an isomorphism and so $(XE)^G$ is a H-Galois extension of K, where $H = (EN)^G$.

Now we are able to conclude the proof: Let us consider the map:

$$\begin{aligned} f : L &\longrightarrow (XE)^G \\ l &\longmapsto \sum_{\bar\sigma\in X} \sigma(l)\, u_{\bar\sigma}, \end{aligned}$$

It is well-defined: if $l \in L$ and $\overline{\tau} = \overline{\sigma}$, then exist $\rho \in G'$ such that $\sigma = \tau\rho$. So, from the fact that $E^{G'} = L$ it follows that $\sigma(l) = \tau(\rho(l)) = \tau(l)$.
For any $\tau \in G$ and $l \in L$ we have:

$$\tau\left(\sum_{\bar\sigma} \sigma(l)\, u_{\bar\sigma}\right) = \sum_{\bar\sigma} \tau\sigma(l)\, u_{\bar\tau\bar\sigma} = \sum_{\bar\sigma} \sigma(l)\, u_{\bar\sigma},$$

so $\mathrm{Im}(f) \subseteq (XE)^G$. Since the $u_{\bar\sigma}$'s are a basis for XE, we get immediately that f is injective.
Finally we check the surjectivity: let $\sum_{\bar\sigma} e_{\bar\sigma} u_{\bar\sigma} \in (XE)^G$, then we have

$$\sum_{\bar\sigma} e_{\bar\sigma} u_{\bar\sigma} = \tau\left(\sum_{\bar\sigma} e_{\bar\sigma} u_{\bar\sigma}\right) = \sum_{\bar\sigma} \tau\left(e_{\bar\sigma}\right) u_{\bar\tau\sigma},$$

so in particular $\tau\left(e_{\bar\sigma}\right) = e_{\bar\tau\bar\sigma}$. If we take $\overline{\sigma}$ the identity class we have $\tau\left(e_{\bar 1}\right) = e_{\bar\tau}$ and so if we take also $\tau \in G'$, we have $\tau\left(e_{\bar 1}\right) = e_{\bar 1} \in E^{G'} = L$. Therefore $f\left(e_{\bar 1}\right) = \sum \sigma\left(e_{\bar 1}\right) u_{\bar\sigma} = \sum e_{\bar\sigma} u_{\bar\sigma}$. Thus $L \simeq (XE)^G$ and L/K is $(EN)^G$-Hopf Galois. □

Remark 2.2.6. The action of H on L come from the identification of $\mathrm{Hom}_G(G, L)$ with L via the valuation 1_G the identity of G. Explicitly, H acts on L via:

$$\left(\sum_{n\in N} x_n n\right)\cdot l = \sum_{n\in N} x_n n^{-1}(1_G)(l)$$

2.2.1 Application to Galois extensions

Let L/K be a Galois extension with group G; in the notation of Theorem 2.2, $E = L$ and $X = G$. The translation map

$$\begin{aligned} \lambda : G &\longrightarrow \mathrm{Perm}(G) \\ \sigma &\longmapsto \lambda_\sigma : \tau \mapsto \sigma\tau, \end{aligned}$$

embeds G in $\mathrm{Perm}(G)$ as a regular subgroup normalized by $\lambda(G)$. Another way to do this is given by the right translation:

$$\begin{aligned} \rho : G &\longrightarrow \mathrm{Perm}(G) \\ \sigma &\longmapsto \rho_\sigma : \tau \mapsto \tau\sigma^{-1}. \end{aligned}$$

It is easy to check that $\rho(G)$ is a regular subgroup of $\mathrm{Perm}(X)$, and moreover

$$\left(\lambda_\sigma \rho_\pi \lambda_{\sigma^{-1}}\right)(\tau) = \sigma\sigma^{-1}\tau\pi^{-1} = \rho_\pi(\tau),$$

so $\lambda(G)$ acts (by conjugation) on $\rho(G)$ leaving all elements fixed and in particular $\lambda(G)$ normalizes $\rho(G)$.

It holds:

$$\lambda(G) = \rho(G) \Leftrightarrow G \text{ is a abelian group.}$$

Indeed, if G is abelian, then $\lambda_\sigma = \rho_{\sigma^{-1}}$. To show the other implication, suppose $\lambda_\pi = \rho_\sigma$; thus $\sigma^{-1} = \rho_\sigma(1) = \lambda_\pi(1) = \pi$. Now, if there exist $\tau, \sigma \in G$ such that $\sigma\tau \neq \tau\sigma$, then $\rho_\sigma(\tau) = \tau\sigma^{-1} \neq \sigma^{-1}\tau = \lambda_{\sigma^{-1}}(\tau)$, against $\rho_\sigma = \lambda_{\sigma^{-1}}$.

We get that if L/K is a non abelian Galois extension, there are (at least) two different Hopf Galois structures.

Proposition 2.2.7. *Let L/K be a Galois extension. The regular subgroup $\rho(G)$ normalized by $\lambda(G)$ corresponds to the classical Galois structure.*

Proof. By Theorem 2.2, we know that $N = \rho(G)$ corresponds to the Hopf Galois structure $H = (LN)^G$, where G is identified with $\lambda(G)$. By the discussion above, $G \simeq \lambda(G) \curvearrowright \rho(G) = N$ trivially (that is, leaving all elements fixed), so $H = L^G N = KN$. The action $KN = H \curvearrowright (GL)^G$ is induced by the action $LN \curvearrowright GL$; moreover $(GL)^G \simeq L$, hence, if $l \in L$ corresponds to $\sum \tau(l) u_\tau \in (GL)^G$, for $\sigma \in G$ we have

$$\rho_\sigma\left(\sum_\tau \tau(l) u_\tau\right) = \sum_\tau \tau(l) \rho_\sigma(u_\tau) = \sum_\tau \tau(l) u_{\tau\sigma^{-1}} = \sum_\tau \tau\sigma(l)(u_\tau).$$

Thus, since $\sum_\tau \tau\sigma(l)(u_\tau)$ corresponds to $\sigma(l)$, the action $N = \rho(G) \curvearrowright (GL)^G$ corresponds to the action $G \curvearrowright L$ (and therefore the Hopf action of KN on $(GL)^G$ correspond to the Hopf action of KG on L). □

2.3 Byott's theorem

One difficulty with Greither-Pareigis criterion is that, applied directly, we need to find out which regular subgroups of $\mathrm{Perm}\left(G/G'\right)$ are normalized by G, and for large n, $\mathrm{Perm}\left(G/G'\right)$ has a huge number of regular subgroups. In this section we present a method that reverse the relationship between G and N.

2.3.1 New point of view

In this section suppose L/K is Galois with group G. We look for regular subgroups N of $\mathrm{Perm}(G)$ normalized by G. If N is a regular subgroup of $\mathrm{Perm}(G)$, as we have notice in the previous section, there is a bijection:

$$\begin{aligned} \cdot e_G : N &\to G \\ \eta &\mapsto \eta \cdot e_G = \eta\left(e_G\right) \end{aligned}$$

where e_G is the identity element of G. The previous bijection induces the following isomorphism:

$$\begin{aligned} \varphi : \mathrm{Perm}(G) &\to \mathrm{Perm}(N) \\ \pi &\mapsto (\cdot e_G)^{-1} \circ \pi \circ (\cdot e_G). \end{aligned}$$

Now, let us notice that under φ, N is mapped to $\lambda_N(N)$ in $\mathrm{Perm}(N)$: for every $\mu, \eta \in N$, we have:

$$\varphi(\mu)(\eta) = (\cdot e_G)^{-1}\left(\mu\left(\eta \cdot e_G\right)\right) = b^{-1}\left((\mu\eta) \cdot e_G\right) = \mu\eta.$$

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

$$\begin{aligned} \lambda_G : G \hookrightarrow \mathrm{Perm}(G) &\xrightarrow{\varphi} \mathrm{Perm}(N) \\ G \mapsto \lambda_G(G) &\quad\mapsto\quad G_0 \cong G, \end{aligned}$$

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

Thanks to this translation, we are able to rewrite the problem in term of the holomorph of N, that is smaller than $\mathrm{Perm}(G)$ and easy to describe.

Definition 2.3.1. Let N be a group. The holomorph of N is the normalizer of $\lambda(N)$ in $\mathrm{Perm}(N)$.

The next proposition show one of the big advantages of this translation, the holomorph has a simple structure:

Proposition 2.3.2. $\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$.

Proof. Firstly, we check that $\rho(N) \cdot \mathrm{Aut}(N) \subseteq \mathrm{Hol}(N)$. We start proving this for the two factors. $\rho(N)$ centralizes $\lambda(N)$, in particular $\rho(N)$ normalizes $\lambda(N)$. Indeed, given $\eta, \mu \in N$, by the definition of λ and ρ we have that $\rho(\eta)\lambda(\mu) = \lambda(\mu)\rho(\eta)$.

On the other hand, we want to prove that $\mathrm{Aut}(N)$ normalizes $\lambda(N)$. Given $\gamma \in \mathrm{Aut}(N)$, we want to see $\gamma\lambda(N) = \lambda(N)\gamma$ (in Perm (N)). Indeed, for every $\eta, \mu \in N$:

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

Notice that the same proof shows that $\mathrm{Aut}(N)$ normalizes $\rho(N)$. Hence, we have that the product is a subgroup as well. Indeed, for every $\eta, \eta' \in \rho(N)$ and $\sigma, \sigma' \in \mathrm{Aut}(N)$:

$$(\eta \cdot \sigma)\left(\eta' \cdot \sigma'\right) = \eta\left(\sigma\eta'\sigma^{-1}\right)\left(\sigma\sigma'\right) = \left(\eta\sigma\eta'\sigma^{-1}\right)\left(\sigma\sigma'\right). \tag{2.1}$$

Conversely, we check that $\mathrm{Hol}(N) \subseteq \rho(N) \cdot \mathrm{Aut}(N)$. Let $\pi \in \mathrm{Hol}(N)$, then for every $\eta \in N$, $\pi\lambda(\eta)\pi^{-1} \in \lambda(N)$. Hence for every $\eta \in N$, there exists $\gamma(\eta) \in N$ such that:

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

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 $\eta \in N$:

$$\begin{aligned}
\pi(\eta) &= \pi\left(\eta \mathrm{e}_N\right) \\
&= \pi\left(\lambda(\eta)\mathrm{e}_N\right) \\
&= \lambda(\gamma(\eta))\left(\pi\left(\mathrm{e}_N\right)\right) \\
&= \gamma(\eta)\pi\left(\mathrm{e}_N\right) \\
&= \left(\rho\left(\pi\left(\mathrm{e}_N\right)^{-1}\right)(\gamma(\eta))\right.
\end{aligned}$$

Hence $\pi = \rho\left(\pi\left(\mathrm{e}_N\right)^{-1}\right) \circ \gamma \in \rho(N) \cdot \mathrm{Aut}(N)$.
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 $\mathrm{Perm}(N)$. Therefore, $\mathrm{Aut}(N) \cap \rho(N) = \{1_N\}$, 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 2.1 leads to conclude that the product is, indeed, a semidirect product. □

2.3.2 Byott's theorem

Here we present Byott's translation theorem, from [Byo96]. 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 $\mathrm{Perm}\left(G/G'\right)$ normalized by $\lambda_G(G)$.

Theorem (Byott translation)**.** *Let $G' \leq G$ be finite groups, let $X = G/G'$ be the left coset of G' in G and let N be an abstract group of order $|X|$. Then there is a bijection*

between the following sets:

$$N = \{\alpha : N \hookrightarrow \mathrm{Perm}(X) \text{ injective homomorphism s.t. } \alpha(N) \text{ is regular}\}$$
$$G = \left\{\beta : G \hookrightarrow \mathrm{Perm}(N) \text{ injective homomorphism s.t. } \beta\left(G'\right) = \mathrm{Stab}_{\mathrm{Perm}(N)}\left(e_N\right)\right\}$$

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

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

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

Proof. We start creating a map from N into G. Let $\alpha \in N$, that is, $\alpha(N)$ is a regular subgroup of $\mathrm{Perm}(X)$. As we have previously notice α induces a bijection:

$$\begin{aligned} a : N &\to X \\ \eta &\mapsto \alpha(\eta)(\bar{e}) \end{aligned}$$

where $\bar{e}$ is the left coset in $X = G/G'$ of e_G. As before, the map a in turn yields an isomorphism:

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

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 injective homomorphism, since it is the composition of an injective homomorphism and an isomorphism. In order to prove that it is in G, it remains to show that $\left(C(a)^{-1} \circ \lambda_G\right)\left(G'\right) = \mathrm{Stab}_{\mathrm{Perm}(N)}\left(\mathrm{e}_N\right)$. For every $\sigma \in G$:

$$\begin{aligned} \left(C(a)^{-1} \circ \lambda_G\right)(\sigma)\left(\mathrm{e}_N\right) = \mathrm{e}_N &\Leftrightarrow \left(C(a)^{-1}\left(\lambda_G(\sigma)\right)\right)\left(\mathrm{e}_N\right) = \mathrm{e}_N \\ &\Leftrightarrow a^{-1}\left(\lambda_G(\sigma)\left(a\left(\mathrm{e}_N\right)\right)\right) = \mathrm{e}_N \\ &\Leftrightarrow \lambda_G(\sigma)\left(a\left(\mathrm{e}_N\right)\right) = a\left(\mathrm{e}_N\right) \\ &\Leftrightarrow \lambda_G(\sigma)(\bar{e}) = \bar{e} \\ &\Leftrightarrow \overline{\sigma e} = \bar{e} \\ &\Leftrightarrow \bar{\sigma} = e_G G' \end{aligned}$$

so that $C(a)^{-1} \circ \lambda_G \in G$, as desired.
The bijection we are looking for is the following:

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

Claim 1: $C(a)^{-1} \circ \alpha = \lambda_N$, so that $\alpha = C(a) \circ \lambda_N$.
Indeed, for every $\eta, \mu \in N$,

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

so that $C(a)^{-1}\circ\alpha = \lambda_N$, as desired.
Now, working in a similar way we define the inverse Ψ of Φ. If $\beta : G \to \mathrm{Perm}(N)$ is in G, then by definition $\beta\left(G'\right) = \mathrm{Stab}_{\mathrm{Perm}(N)}(\mathrm{e}_N)$. Thus β yields a bijection:

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

Indeed,

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

$$\begin{aligned} b(\bar{\sigma}) = b(\bar{\tau}) &\Leftrightarrow \beta(\sigma)(\mathrm{e}_N) = \beta(\tau)(\mathrm{e}_N)\\ &\Leftrightarrow \left(\beta(\tau)^{-1}\circ\beta(\sigma)\right)(\mathrm{e}_N) = \left(\beta(\tau)^{-1}\circ\beta(\tau)\right)(\mathrm{e}_N)\\ &\Leftrightarrow \left(\beta(\tau)^{-1}\circ\beta(\sigma)\right)(\mathrm{e}_N) = \mathrm{e}_N\\ &\Leftrightarrow \left(\beta\left(\tau^{-1}\right)\circ\beta(\sigma)\right)(\mathrm{e}_N) = \mathrm{e}_N\\ &\Leftrightarrow \beta\left(\tau^{-1}\sigma\right)(\mathrm{e}_N) = \mathrm{e}_N\\ &\Leftrightarrow \tau^{-1}\sigma \in G'\\ &\Leftrightarrow \sigma \in \tau G'\\ &\Leftrightarrow \bar{\sigma} = \bar{\tau}\end{aligned}$$

where:

1. $\beta(\tau) \in \mathrm{Perm}(N)$,
2. $\beta(\tau)^{-1}\circ\beta(\tau) = 1_N$,
3. $\beta(\tau)^{-1} = \beta\left(\tau^{-1}\right)$,
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 :

$$b(\bar{e}) = \beta(e_G)(\mathrm{e}_N) = 1_{\mathrm{Perm}(N)}(\mathrm{e}_N) = \mathrm{e}_N$$

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

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

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 N.

The bijection we seek from G to N is the following:

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

Claim 2: $C(b)^{-1} \circ \beta = \lambda_G$, so that $\beta = C(b) \circ \lambda_G$.
Indeed, for every $\sigma \in G, \bar{\tau} \in X$,

$$\begin{aligned} \left(C(b)^{-1} \circ \beta\right)(\sigma)(\bar{\tau}) &= \left(C(b)^{-1}(\beta(\sigma))\right)(\bar{\tau}) \\ &= \left(b^{-1} \circ \beta(\sigma)\right)(b(\bar{\tau})) \\ &= \left(b^{-1} \circ \beta(\sigma)\right)\left(\beta(\tau)(\mathrm{e}_N)\right) \\ &= b^{-1}\left((\beta(\sigma)\beta(\tau))(\mathrm{e}_N)\right) \\ &= b^{-1}\left(\beta(\sigma\tau)(\mathrm{e}_N)\right) \\ &= b^{-1}(b(\overline{\sigma\tau})) \\ &= \lambda_G(\sigma)(\bar{\tau}) \end{aligned}$$

Claim 3: Ψ and Φ are inverse maps.

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

$$\begin{aligned} b(\bar{\sigma}) &= \beta(\sigma)(\mathrm{e}_N) \\ &= \left(C(a)^{-1}(\lambda_G(\sigma))\right)(\mathrm{e}_N) \\ &= \left(a^{-1} \circ \lambda_G(\sigma)\right)(a(\mathrm{e}_N)) \\ &= \left(a^{-1} \circ \lambda_G(\sigma)\right)(\bar{e}) \\ &= a^{-1}(\lambda_G(\sigma)(\bar{e})) \\ &= a^{-1}(\overline{\sigma e}) \\ &= a^{-1}(\bar{\sigma}) \end{aligned}$$

Therefore, it follows that $\Psi \circ \Phi = 1_N$:

$$\begin{aligned}\Psi(\Phi(\alpha)) &= \Psi(\beta)\\ &= C(b)^{-1}\circ\lambda_N\\ &= C\left(b^{-1}\right)\circ\lambda_N\\ &= C(a)\circ\lambda_N\\ &= \alpha\end{aligned}$$

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

$$\begin{aligned}a(\eta) &= \alpha(\eta)(\bar{e})\\ &= \left(C(b)^{-1}\left(\lambda_N(\eta)\right)\right)(\bar{e})\\ &= \left(b^{-1}\circ\lambda_N(\eta)\right)(b(\bar{e}))\\ &= \left(b^{-1}\circ\lambda_N(\eta)\right)(\mathrm{e}_N)\\ &= b^{-1}\left(\lambda_N(\eta)\,(\mathrm{e}_N)\right)\\ &= b^{-1}\left(\eta\mathrm{e}_N\right)\\ &= b^{-1}(\eta)\end{aligned}$$

Therefore, it follows that $\Phi\circ\Psi = 1_G$:

$$\begin{aligned}\Phi(\Psi(\beta)) &= \Phi(\alpha)\\ &= C(a)^{-1}\circ\lambda_G\\ &= C\left(a^{-1}\right)\circ\lambda_G\\ &= C(b)\circ\lambda_G\\ &= \beta\end{aligned}$$

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 N

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

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

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

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

$$\begin{aligned} C(a\gamma)^{-1}(\pi) &= (a\gamma)^{-1} \circ \pi \circ (a\gamma) \\ &= \gamma^{-1} \circ \left(a^{-1}\pi a\right) \circ \gamma \\ &= C(\gamma)^{-1}\left(a^{-1}\pi a\right) \\ &= C(\gamma)^{-1}\left(C(a)^{-1}(\pi)\right) \\ &= \left(C(\gamma)^{-1}C(a)^{-1}\right)(\pi) \end{aligned}$$

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

$$\begin{aligned} \beta' &= \Phi\left(\alpha'\right) \\ &= \Phi(\alpha\gamma) \\ &= C(a\gamma)^{-1} \circ \lambda_G \\ &= C(\gamma)^{-1} \circ C(a)^{-1} \circ \lambda_G \\ &= C(\gamma)^{-1} \circ \beta \end{aligned}$$

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

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

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

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

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

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

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

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

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 $\lambda_N(N)$:

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

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:

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

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

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

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

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

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

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

□

Definition 2.3.3. Call an injective homomorphism $\alpha : N \hookrightarrow \mathrm{Perm}(X)$ such that $\alpha(N)$ is regular, a *regular embedding*.

Remark 2.3.4. Greither-Pareigis's Theorem shows that the number of Hopf Galois structure on L/K is in bijection with regular subgroups N of $\mathrm{Perm}(X)$. This by Byott translation are in bijection with the equivalence class of embedding of G into $\mathrm{Hol}(N)$ modulo conjugation by elements of $\mathrm{Aut}(N)$. This is really important since $\mathrm{Hol}(N)$ is way smaller then $\mathrm{Perm}(G)$ and easy to describe, as we have seen in 2.3.2.

2.4 Hopf Galois structure on prime power cyclic extensions

In this last section of the second chapter we study with how many different Hopf Galois structure could be enrich a cyclic Galois extension of degree a power of a prime. Thanks to the Greither-Pareigis Theorem the problem could be reduce to a purely group-theoretic question.

We want to prove the following theorem:

Theorem 2.4.1. *There are exactly p^{n-1} Hopf Galois structures on a cyclic Galois extension L/K of order p^n with p an odd prime.*

Firstly, we notice that if G is cyclic of order p^n then by Proposition 2.3.2 his holomorph is isomorphic to $\rho(G) \rtimes \mathrm{Aut}(G) \cong (\mathbb{Z}/p^n\mathbb{Z}) \rtimes (\mathbb{Z}/p^n\mathbb{Z})^*$ so there are only p^{n-1} different embedding of G in his holomorph.
Thanks to this remark the theorem follows from the following one:

Theorem 2.4.2. *Let p be an odd prime, G be a cyclic of order p^n and N a group of order p^n but not cyclic. Then there is no embedding of G into $Hol(N)$.*

Proof. The statement is equivalent to show that in $Hol(N)$ there are not element of order p^n.
By Proposition 2.3.2 we know that $Hol(N)$ is a semidirect product between N and $\mathrm{Aut}(N)$, with the propriety: for all $\eta \in N$ and $\alpha \in \mathrm{Aut}(N)$

$$\alpha\eta := \alpha\rho(\eta) = \rho(\alpha(\eta))\alpha = \alpha(\eta)\alpha.$$

Then more generally, if $e \geq 1$ then $(\eta\alpha)^e = (\prod_{i=0}^{e-1} \alpha^i(\eta))\alpha^e$, hence if $(\eta\alpha)^e = 1$ then $\alpha^e = 1$. Now suppose that exist an element in the holomorph of order p^n, then there is also a automorphism of N with order p. For classic group theory result this imply the existence of a composition series for N of the form:

$$\{e\} = N_0 < N_1 < N_2 < \ldots < N_n = N,$$

where $N_i \lhd N$, $\alpha(N_i) = N_i$ for all i and since N si not cyclic $N_2 = (\mathbb{Z}/p\mathbb{Z})^2$. For the second propriety α induce an automorphism of $N_i/N_{i+1} = (\mathbb{Z}/p\mathbb{Z})$, but remember that α has order p so it induce the identity. This cam be express as: for every $\eta_i \in N_i$ exist a $\eta_{i-1} \in N_{i-1}$ such that

$$\alpha(\eta_i) = \eta_i\eta_{i-q} \tag{2.2}$$

Claim: for any $\eta \in N$, $\alpha^{p^{s-1}} = \eta\eta_{n-s}$ for some $\eta_{n-s} \in N_{n-s}$.
The claim certainly holds for $s = 1$. For $s = 2$: Suppose that $\alpha^r(\eta) = \eta\eta_{n-1}^r\eta_{n-2}$ for some $\eta_{n-2} \in N_{n-2}$, then exist a $\eta'_{n-2} \in N_{n-2}$ such that:

$$\alpha^{r+1}(\eta) = \eta\eta_{n-1}(\eta_{n-1}\eta'_{n-2})^r\alpha(\eta_{n-2}).$$

Now, since N_i are normal in N_{i+1}, $(\eta_{n-1}\eta'_{n-2})^r = \eta_{n-1}^r\eta''_{n-2}$ for some $\eta_{n-2} \in N_{n-2}$, then $\alpha^{r+1}(\eta)$ has the same structure of the case r. Finally, since $\eta_{n-1}^p \in N_{n-2}$ we have that $\alpha^p(\eta) = \eta\eta_{n-2}$ so the claim holds for 2. Using the same argument we can prove that the claim always work.
In particular, $\alpha^{p^{n-1}}(\eta) = \eta$ since $N_0 = \{1\}$, and than no element of $Aut(N)$ has order p^n.
Let $\eta\alpha$ be the element of $Hol(N)$ of order p^n, we have already notice that α has

order a power of p. So using what we prove in the proof of the claim for $s = 2$ we find that:

$$(\eta\alpha)^p = (\prod_{i=0}^{p-1} \alpha^i(\eta))\alpha^p = \eta(\prod_{i=1}^{p-1} \eta\eta_{n-1}^{(i)})\alpha^p$$
$$= \eta(\eta^{p-1}\prod \eta_{n-1}^{(i)'})\alpha^p = \eta^p\eta_{n-1}\alpha^p \in N_{n-1}\langle\alpha^p\rangle,$$

where $\eta_{n-1}^{(i)}, \eta_{n-1}^{(i)'}$ and η_{n-1} are in N_{n-1}. Then by induction we obtain $(\eta\alpha)^{p^{n-2}} \in N_2\langle\alpha^{p^{n-2}}\rangle$.
Let us call $\gamma = \alpha^{p^{n-2}}$ and let $\eta_2 \in N_2$. Then we have:

$$(\eta_2\gamma)^p = \eta_2\gamma(\eta_2)...\gamma^{p-1}(\eta_2)\gamma^p = \eta_2\gamma(\eta_2)...\gamma^{p-1}(\eta_2).$$

Now since γ has order p and $|N_1| = p$ we have that $\gamma(\eta_2) = \eta_2\eta_1$ for 2.2 and $\gamma^2(\eta_2) = \gamma(\eta_2\eta_1) = \eta_2\eta_1 \cdot \eta_1 = \eta_2\eta_1^2$ so reiterating $\gamma^n(\eta_2) = \eta_2\eta_1^n$. Finally, since $N_2 = (\mathbb{Z}/p\mathbb{Z})^2$ we have:

$$(\eta_2\gamma)^p = \eta_2(\eta_2\eta_1)...(\eta_2\eta_1^{p-1}) = \eta_2^p\eta_1^{\frac{p(p-1)}{2}} = 1.$$

So we have that $(\eta\alpha)^{p-1} = 1$ that is a contradiction.

□

In particular we have prove the following:

Corollary 2.4.3. *Let L/K be a Galois extension of fields of degree p an odd prime. Then L/K admits only one Hopf–Galois structure, namely the classical one.*

CHAPTER 3

Hopf-Galois Number Theory

In this chapter we present associated orders and the concept of tame H-extension. In usual Galois module theory we see that the concept of being tame is a necessary and sufficient condition for an extension of local fields to admit a NIB[1], this result is called the Noether's Theorem. We prove a generalization of Noether's Theorem , due to L.N.Childs, that holds for Hopf Galois extension. At the end of the chapter we prove that in the local case the concept of Galois, free and tame extension coincide.

3.1 Integrals and orders

3.1.1 Integrals

Now we introduce the concept of integral element of an Hopf algebra, this will help us to understand the structure of H as a H^*-module.

Definition 3.1.1. Let H be a R-Hopf algebra. An element θ of H is called *left integral* if it satisfies: for all $h \in H$

$$h\theta = \varepsilon(h)\theta.$$

An element θ of H is called *right integral* if it satisfies: for all $h \in H$

$$\theta h = \varepsilon(h)\theta.$$

Remark 3.1.2. Let M be a left H-module, then the set of invariants, M^H, is a H-submodule of M. Then, viewing H as a left H-module via multiplication, we find that the set of left integrals is H^H, therefore it is an ideal of H.

[1]Normal Integral Basis

Notation 3.1.3. *Thanks to the previous remark we call the ideal of integral of a Hopf algebra H by $I(H)$ and if it is clear from the context we will write just I.*

As an example we look at the group algebra RG, where G is a finite group:

Example 3.1.4. 1. Let $H = RG$ for G a finite group. Consider $x = \sum_{\sigma\in G} r_\sigma \sigma \in RG$ and $\theta = \sum_{\sigma\in G} \sigma$, then we have:

$$\begin{aligned} x\theta &= \sum_{\sigma\in G} a_\sigma \sigma \cdot \left(\sum_{\tau\in G} \tau\right) \\ &= \sum_{\sigma\in G} a_\sigma \cdot \left(\sum_{\tau\in G} \tau\right) \\ &= \varepsilon(x)\theta. \end{aligned}$$

so $R\theta \subset RG^{RG}$. Now we prove that this is an equality. Let $x = \sum_{\tau\in G} r_\tau \tau \in RG^{RG}$ and $\sigma \in G$ then:

$$x = \varepsilon(\sigma)x = \sigma x = \sum_{\tau\in G} r_\tau \sigma\tau = \sum_{\tau\in G} r_\tau \rho(\tau),$$

where ρ is a permutation of G. So for every $\tau, \gamma \in G$ we have $r_\tau = r_\gamma$, so the thesis.

2. Let $H = (RG)^* = \sum_{\sigma\in G} Re_\sigma$ where $e_\sigma(\tau) = \delta_{\sigma\tau}$ for every $\sigma, \tau \in G$. We know that H is commutative, so the module of left and right integrals coincide. It can be proven that the module of integrals is generated as an ideal by e_1. For example:
$$e_\sigma e_1 = \delta_{1\sigma} e_1 = \varepsilon(e_\sigma)e_1,$$
then by linearity e_1 is an integral.

The structure of H as a module over its dual is explicated by the following theorem:

Theorem (Larson-Sweedler)**.** *Let H be a finite R-Hopf algebra, then the action of H over H^* defines an isomorphism $H^* \cong H \otimes I(H^*)$.*

Corollary 3.1.5. *Let H be a finite R-Hopf algebra, then the module $I(H^*)$ is a projective R-module of rank* 1.

Proof. We may assume that R is connected (i.e. without other idempotents except for 0 and 1). In this case, H is a projective R-module of rank n, and the same holds for H^*. Larson-Sweedler Theorem we have $H^* \cong H \otimes I$ as R-module, and for the splitting of the surjective map ε we have that R is a direct summand of H. Then I is projective and for dimension reason it has rank one. □

Remark 3.1.6. In PIDs the projective modules are free, so if we assume R to be PID we see that $I(H^*)$ is free of rank one. If $I(H^*) = R\theta$, then $H^* = H\theta$ is a free H-module and the map:

$$\begin{aligned} H &\to H^* \\ x &\mapsto x \cdot \theta, \end{aligned}$$

is a left H-module isomorphism.

Now we introduce a new type of algebra:

Definition 3.1.7. An associative unital algebra A over a ring R is a Frobenius algebra if it has finite dimension and is equipped with a non-degenerate bilinear form $\sigma : A \times A \to R$ that satisfies the following equation:

$$\sigma(ab, c) = \sigma(a, bc).$$

Proposition 3.1.8. *Let R be a PID and H a finite R-Hopf algebra, then H is a Frobenius with the bilinear form:*

$$\begin{aligned} \beta : H \otimes H &\longrightarrow R \\ h \otimes k &\longmapsto \langle hk, \theta \rangle. \end{aligned}$$

Proof. The defined map is clearly bilinear. We need to prove that is associative and non-degenerate. For the first, let $h, g, k \in H$ then $\beta(hg, k) = \langle hgk, \theta \rangle = \beta(h, gk)$. For the second, let $\{h_1, ..., h_n\}$ be a R-basis of H, and let $\{h_1^*, ..., h_n^*\}$ be the dual basis in H^*. Then for Remark 3.1.6 $h_i^* = k_i\theta$ for some $k_i \in H$, and so $\{k_1, ..., k_n\}$ is another R-basis of H. For the definition of the action we have:

$$\sigma_i^j = \langle h_i, k_j\theta \rangle = \langle h_i k_j, \theta \rangle = \beta(h_i, k_j).$$

Then from a common argument of representation theory β is non-degenerate. □

Know we prove one last lemma about the integrals that will be useful in the next sections:

Lemma 3.1.9. *Let θ be a left integral of H, then for all $h \in H$ we have:*

$$(h \otimes 1)((1 \otimes \lambda)\Delta(\theta)) = ((1 \otimes \lambda)\Delta(\theta))(1 \otimes h).$$

Proof.

$$\begin{aligned} (h \otimes 1)((1 \otimes \lambda)\Delta(\theta)) &= \sum h\theta_{(1)} \otimes \lambda(\theta_{(2)}) \\ &= \sum h_{(1)}\varepsilon(h_{(2)}\theta_{(1)} \otimes \lambda(\theta_{(2)}) \\ &= \sum h_{(1)}\theta_{(1)} \otimes \lambda(\theta_{(2)})\varepsilon(h_{(2)} \\ &= \sum h_{(1)}\theta_{(1)} \otimes \lambda(\theta_{(2)})\lambda(h_{(2)}h_{(3)} \\ &= \sum (1 \otimes \lambda)\Delta(h_{(1)}\theta)(1 \otimes h_{(2)}) \\ &= \sum (1 \otimes \lambda)\Delta(\varepsilon(h_{(1)})\theta)(1 \otimes h_{(2)}) \\ &= \sum (1 \otimes \lambda)\Delta(\theta)(1 \otimes \varepsilon(h_{(1)})h_{(2)}) = (1 \otimes \lambda)\Delta(\theta)(1 \otimes h) \end{aligned}$$

□

3.1.2 Hopf Orders

In this short section, we introduce the important concept of Hopf Order.

Definition 3.1.10. Let R be a Dedekind domain with quotient field K of characteristic 0 and let A be a finite K-Hopf algebra. An *R-order of A* is a R-submodule H of A such that:

1. H is finite,
2. $KH = A$.

In this context we may identify $H \otimes_R H$ with a subset of $A \otimes_K A$. In fact, let us consider the homomorphism $\varphi : H \otimes_R H \to A \otimes_K A$ that sends $\sum h_i \otimes_R k_j$ to $\sum h_i \otimes_K k_j$. This is injective, in order to prove this, since injectivity is a local propriety, we can assume that R is local. With this assumption H is free, let $\{a_1, ..., a_n\}$ be a R-basis of H, then $\{a_i \otimes a_j | i, j = 1, ..., n\}$ is a basis of $H \otimes_R H$. The map φ send this basis into a K-basis of $A \otimes_K A$ so it is injective. Thanks to this identification we can define the Hopf orders:

Definition 3.1.11. Let R be a Dedekind domain with quotient field K of characteristic 0 and let A be a finite K-Hopf algebra. An R-order of A is a Hopf order if it equipped with the operation induced from those of A by restriction is a R-Hopf algebra.

Example 3.1.12. Let G a finite group and $A = KG$. Then the ring group RG is a Hopf order.

Moreover, the Hopf order in the example is minimal in KG:

Proposition 3.1.13. *If H is a Hopf order over R in KG, then $RG \subset H$.*

Proof. We may assume that R is local, so H is finitely generated and free. Then H^* is a finite R-Hopf order in $(KG)^*$. Now, $(KG)^*$ is commutative, so it has a unique maximal R-order. On the other hand, it has K-basis $\{e_\sigma\}_{\sigma \in G}$, where $e_\sigma(\tau) = \delta_{\sigma\tau}$, which is the basis dual to the basis of KG formed by the elements of G. Moreover, it is easy to check that this is a basis of primitive pairwise orthogonal idempotents of $(KG)^*$. Thus, the unique maximal order is $(RG)^*$, with basis $e_\sigma \sigma \in G$. Since H is an R-order, $H^* \subseteq (RG)^*$, hence $RG \subseteq H$. □

3.1.3 Associated orders

Let L/K be an A-Galois extension, where K is the fraction field of a Dedekind domain R and A a K-Hopf algebra. Let S be the integral closure of R in L. When L/K is a classical Galois extension, so $A = KG$, we consider the module structure of S over its associated order:

$$\mathfrak{A}_{KG} = \{\lambda \in KG \mid \lambda S \subseteq S\}$$

In complete analogy, for an arbitrary Hopf-Galois structure, we have:

Definition 3.1.14. The *associated order* of S in A is:

$$\mathfrak{A}_A = \{\alpha \in A \mid \alpha S \subseteq S\}$$

Its algebraic properties are similar to those for the classical case. Clearly $\mathfrak{A}_A$ is an R-algebra and moreover it is an R-order in A. However, it is not necessarily an R-Hopf algebra. For instance, if $L/\mathbb{Q}$ is a finite abelian extension with group G which is wildly ramified at some odd prime, then $\mathfrak{A}_{KG}$ is not an R-Hopf algebra (see Corollary 5.6 of [Chi87]). The following proposition justify the choice of $\mathfrak{A}$ as the "correct" order:

Proposition 3.1.15. *If L/K is A-Galois and H is an R-order in A such that S is H-free, then $H = \mathfrak{A}_A$.*

Proof. Let t be a generator of S as H-module. Tensorizing by K, we have that t is a generator of L as free A-module. Let $\alpha \in \mathfrak{A}_A$, so $\alpha t \in S$, but $S = Ht$ then there is some $h \in H$ such that $\alpha \cdot t = h \cdot t$. This equality in particular holds in $L = A \cdot t$, and hence $\alpha = h \in H$. □

Now we make an example where S is free over the associated order but not over $\mathbb{Z}G$:

Example 3.1.16. We consider the extension $L = \mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}$. Then $L/\mathbb{Q}$ is Galois with group $G = \mathbb{Z}/2\mathbb{Z} = \langle\sigma\rangle$. The ring of integers of L is $S = \mathbb{Z}[\sqrt{2}]$. We know that $L/\mathbb{Q}$ is tamely ramified at a prime p if and only if the image of the trace $\mathrm{tr} : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}$ is not divisible by p. Since $\mathrm{tr}(a + b\sqrt{2}) = 2a$ we have $\mathrm{tr}(S) = 2\mathbb{Z}$, then the only wildly ramified prime is 2. By Noether's theorem, S is not locally free as $\mathbb{Z}G$-module, so it is not $\mathbb{Z}G$-free. However, S is $\mathfrak{A}_{\mathbb{Q}[G]}$-free. Indeed, the elements

$$e_1 = \frac{1+\sigma}{2}, \quad e_{-1} = \frac{1-\sigma}{2},$$

are primitive pairwise orthogonal idempotents of $\mathbb{Q}[G]$ and then $\mathbb{Z}[e_1, e_{-1}]$ is the maximal $\mathbb{Z}$-order in $\mathbb{Q}[G]$. In particular, $\mathfrak{A}_{\mathbb{Q}[G]} = \mathbb{Z}[e_1, e_{-1}]$. Let $\alpha = 1 + \sqrt{2}$, then:

$$e_1(\alpha) = 1, \quad e_{-1}(\alpha) = \sqrt{2}$$

so $S = \mathfrak{A}_{\mathbb{Q}[G]}\alpha$ and hence S is $\mathfrak{A}_{\mathbb{Q}[G]}$ free.

3.2 Tame extension

In this section we want to generalize the concept of tame extension for the Hopf-Galois setting. Whereupon we study some important theorem in Galois module theory in the setting of Hopf-Galois. Finally, we prove that the notion of being a tame extension in the local case coincides with being free or being Galois.

In the classic Galois setting we have the definition:

Definition 3.2.1. A Galois extension of p-adic fields L/K is tamely ramified if p does not divide the ramification index $e(L/K)$.

It is not hard to show that: L/K is tamely ramified if and only if the trace map

$$\begin{aligned} \mathrm{tr} : S &\longrightarrow R \\ a &\longmapsto \theta(a) = \sum_{\sigma \in G} \sigma(a) \end{aligned}$$

is surjective. Now, recall that θ generates $I(KG)$. Then L/K is tamely ramified if and only if $I(KG)S = R$. This motivates the following definition:

Definition 3.2.2. Let R be a commutative connected ring and let H be a cocommutative R-Hopf algebra which is finite as R-module. Let S be a finite R-algebra and assume that S is an H-module algebra with $S^H = R$. We say that S is a tame H-extension of R or H-tame if:

1. $\mathrm{rank}_R(S) = \mathrm{rank}_R(H)$.
2. S is a faithful H-module.
3. $I(H)S = R$.

The initial two prerequisites are compatibility conditions that are guaranteed in the Galois scenario. In fact, they are always satisfied when S and R represent valuation rings of a local field A-Galois extension L/K. The condition that R is connected (i.e., lacking non-trivial idempotents) it is required so that projective modules have a well defined rank. Specifically, the rank is a function that is defined at $\mathrm{Spec}(R)$ and is locally constant. If R is connected, then this function is constant.

On the other hand, the third condition means that $I(H)S$ is as large as possible, because of the following result:

Proposition 3.2.3. *Let H be a finite cocommutative R-Hopf algebra and let S be an H-module algebra. Then $I(H)S \subseteq S^H$.*

Proof. Let $\xi = \sum_i \theta_i s_i$, where $\theta_i \in I(H)$ and $s_i \in S$ for all i. Given $h \in H$,

$$h\xi = h\left(\sum_i \theta_i s_i\right) = \sum_i (h\theta_i)\, s_i = \sum_i \varepsilon(h)\theta_i s_i = \varepsilon(h)\xi.$$

Thus, $\xi \in S^H$. □

3.2.1 H-tame imply H-free

In this subsection we want to generalize the Noether Theorem for classical tame extension. We start by proving a theorem that shows that tame imply being projective:

Theorem 3.2.4. *Let R be a local ring. Let H be a finite cocommutative R-Hopf algebra and S a finite R-algebra which is an H-module algebra. If S is H-tame, then S is H-projective.*

Proof. Let $I(H) = R\theta$ be the module of left integrals of H. Since S is H-tame, then $\theta S = R$, so there exists $z \in S$ such that $\theta z = 1$. Since S is R-projective and H is R-free, the H-module $H \otimes_R S$ (H acts on $H \otimes_R S$ by product in the first factor) is projective. In order to prove that S is H-projective, we prove it is a direct summand of $H \otimes_R S$.

Let $\mu : H \otimes S \to S$ be the R-linear map defined by $\mu(h \otimes s) = hs$, which clearly is an H-module homomorphism. If we prove that this map splits, then $H \otimes S = \mathrm{Ker}(\mu) \oplus S$ as desired. Let us define $\nu : S \to H \otimes_R S$ by $\nu(s) = \sum_{(\theta)} \theta_{(1)} \otimes z\left(\lambda\left(\theta_{(2)}\right) s\right)$. We need to prove that ν is an H-module homomorphism and $\mu \circ \nu = \mathrm{Id}_S$. First, we prove that ν is an H-module homomorphism. For every $h \in H, s \in S$, we have:

$$\begin{aligned} h \cdot (\nu(s)) &= h\left(\sum_{(\theta)} \theta_{(1)} \otimes z\left(\lambda\left(\theta_{(2)}\right) s\right)\right) \\ &= \sum_{(\theta)} \left(h\theta_{(1)}\right) \otimes z\left(\lambda\left(\theta_{(2)}\right) s\right) \\ &= (1 \otimes z)\left(\sum_{(\theta)} \left(h\theta_{(1)}\right) \otimes \lambda\left(\theta_{(2)}\right)\right)(1 \otimes s) \\ &= (1 \otimes z)(h \otimes 1)((1 \otimes \lambda)\Delta(\theta))1 \otimes s) \end{aligned}$$

Now using Lemma 3.1.9 we have the equality:

$$\begin{aligned} h(\nu(s)) &= (1 \otimes z)((1 \otimes \lambda)\Delta(\theta))(1 \otimes h)1 \otimes s) \\ &= (1 \otimes z)\left(\sum_{(\theta)} \theta_{(1)} \otimes \lambda\left(\theta_{(2)}\right) h\right)(1 \otimes s) \\ &= \sum_{(\theta)} \theta_{(1)} \otimes z\left(\lambda\left(\theta_{(2)}\right)(hs)\right) \\ &= \nu(hs) \end{aligned}$$

which proves that ν is an homomorphism of H-modules.

Finally, we show that $\mu \circ \nu$ is the identity. Let $s \in S$. Then

$$\begin{aligned}\mu\circ\nu(s) &= \sum_{(\theta)}\theta_{(1)}\left(z\left(\lambda\left(\theta_{(2)}\right)s\right)\right)\\ &= \sum_{\theta}\left(\theta_{(1)}z\right)\left(\theta_{(2)}\left(\lambda\left(\theta_{(3)}\right)s\right)\right)\\ &= \sum_{\theta}\left(\theta_{(1)}z\right)\left(\varepsilon\left(\theta_{(2)}\right)s\right)\\ &= \sum_{(\theta)}\left(\left(\theta_{(1)}\varepsilon\left(\theta_{(2)}\right)\right)z\right)s\\ &= (\theta z)s = s,\end{aligned}$$

as we wanted. In the second equality we used that S is a H-module algebra and so the product μ_S is a H-module morphism. □

Now we state, without proving it, an important general result:

Theorem 3.2.5. *(Schneider [Sch77]). Let R be a local domain with fraction field K of characteristic zero. Let H be a finite cocommutative R-Hopf algebra and let P and Q be finite left H-modules. If $K\otimes_R P \cong K\otimes_R Q$ as $K\otimes_R H$-modules, then $P\cong Q$ as H-modules.*

We apply the previous theorem:

Proposition 3.2.6. *Let L/K be an A-Galois extension of local fields of characteristic 0 and let us call S and R the corresponding valuation rings. Let H be an R-Hopf order in A such that $H\subseteq\mathfrak{A}_A$ and S is H-projective. Then, S is H-free (in particular, $H=\mathfrak{A}_A$).*

Proof. Let us check that we can apply Schneider's theorem. H is an R-Hopf order in A, and hence a finite cocommutative R-Hopf algebra. Since L/K is A-Galois, $L\cong A$ as A-modules. But $L = K\otimes_R S$ and $A = K\otimes_R H$, so Schneider theorem gives that $S\cong H$ as H-modules. □

As a consequence of Theorem 3.2.4 and Proposition 3.2.6 , we obtain the following generalization of Noether's Theorem:

Theorem 3.2.7. *Let R be a local domain with quotient field K of characteristic zero. Let H be a finite cocommutative R-Hopf algebra and S be a finite R-algebra. Suppose S is H-tame of R then S is a free H-module of rank one.*

In particular we have the following formulation:

Theorem 3.2.8. *Let L/K be an A-Galois extension of p-adic fields and call S and R the corresponding valuation rings. Let H be an R-Hopf order in A such that $H\subseteq\mathfrak{A}_A$ and S is H-tame. Then, S is H-free (in particular, $H=\mathfrak{A}_A$).*

3.2.2 Hopf order imply $\mathfrak{A}_A$-free

Thanks to Theorem 3.2.8 we have understood the importance of being tame over an R-order of A. Now we show that for the associated order this condition is implied by being an Hopf order:

Theorem 3.2.9. *Let L/K be an A-Galois extension of local fields, let R be the valuation ring of K and let S be the integral closure of R in L. If $\mathfrak{A}_A$ is an R-Hopf order in A, then S is $\mathfrak{A}_A$-tame.*

Proof. Since R is local, for Corollary 3.1.5 the ideal $I = I(\mathfrak{A}_A)$ is R-free of rank one, let us say generated by θ. Since L/K is A-Galois, $L^A = K$, hence $S^{\mathfrak{A}_A} = R$. By Proposition 3.2.3, $\theta S \subseteq S^{\mathfrak{A}_A} = R$, from which θS is an ideal of R. If π is a uniformizer of R, this means that $\theta S = \pi^i R$ for some $i \geq 0$, so $\frac{\theta}{\pi^i} S = R$. In particular, $\frac{\theta}{\pi^i} \in \mathfrak{A}_A$.

Let us check that $\frac{\theta}{\pi^i}$ is actually a left integral of $\mathfrak{A}_A$. Indeed, given $\alpha \in \mathfrak{A}_A$, since θ is a left integral, $\frac{\theta}{\pi^i}\alpha = \frac{\varepsilon_{\mathfrak{A}_A}(\theta)}{\pi^i}\alpha$. Now

$$\varepsilon_{\mathfrak{A}_A}(\theta) = \varepsilon_{\mathfrak{A}_A}\left(\frac{\theta}{\pi^i}\pi^i\right) = \varepsilon_{\mathfrak{A}_A}\left(\frac{\theta}{\pi^i}\right)\varepsilon_{\mathfrak{A}_A}\left(\pi^i\right) = \varepsilon_{\mathfrak{A}_A}\left(\frac{\theta}{\pi^i}\right)\pi^i.$$

Adding this to the last expression gives $\frac{\theta}{\pi^i}\alpha = \varepsilon_{\mathfrak{A}_A}\left(\frac{\theta}{\pi^i}\right)\alpha$, as desired.

Then, we have proved that $\frac{\theta}{\pi^i} \in I$, while θ is a generator of I as a R-module. Then, $i = 0$ and $\theta S = R$, so S is $\mathfrak{A}_A$-tame. □

The previous Theorem together with Theorem 3.2.8 give us a criteria for being free over the associated order:

Corollary 3.2.10. *If $\mathfrak{A}_A$ is an R-Hopf order, then S is $\mathfrak{A}_A$-free.*

The converse of the previous corollary is false: we present a counterexample in Remark 4.3.15.

3.2.3 H-Galois implies H-tame

We start to investigate the relationship between H-Galois and H-tame. In this section we prove that the first condition is in general stronger. This should be expected, since in the classical case $H = RG$ and S the valuation ring of an extension of local fields, Galois is equivalent to unramified and tame to tamely ramified.
To prove this implication, we will need Morita theory. Let R be a commutative ring with unity and H a finite cocommutative R-Hopf algebra. Let S be an H-Galois extension and let $E = \mathrm{End}_R(S)$.

Proposition 3.2.11. *For any left E-module M, we have*

$$M^H \cong I(H)M$$

In particular, $M \cong S \otimes I(H)M$ as left E-modules.

Proof. Since S is H-Galois, by Proposition 1.3.22, for any E-module M have the isomorphism:

$$M^H \cong \mathrm{Hom}_E(S, M).$$

Using the previous isomorphism and the one in Remark 1.3.19 we have:

$$M^H \cong \mathrm{Hom}_E(S, E) \otimes_E M$$

In particular, for $M = E$ we have

$$E^H \cong \mathrm{Hom}_E(S, E)$$

Then,

$$M^H \cong E^H \otimes_E M,$$

and it is enough to prove that $E^H \cong I(H)E$.
Since S is H-Galois, $E \cong H \otimes S$ as left H-modules. Then, the last isomorphism is equivalent to $(H \otimes_R S)^H \cong I(H)(H \otimes_R S)$. Now, if $P = \sum_{i=1}^n Rv_i$ is a finite free R-module with basis $\{v_1, ..., v_n\}$, then:

$$(H \otimes P)^H = \left(\sum_{i=1}^n Hv_i\right)^H = \sum_{i=1}^n I(H)v_i = \sum_{i=1}^n I(H)(Hv_i) = I(H)(H \otimes P),$$

so the isomorphism holds for any free R-module. Since S is R-projective, it is the direct summand of a free R-module, and then it also holds for S.

Finally, using the previous equivalence,

$$M \cong S \otimes M^H \cong S \otimes I(H)M$$

□

Proposition 3.2.12. *Let S be an H-Galois extension of R. Then, S is H-tame.*

Proof. Since S is H-Galois, $\mathrm{rank}_R(S) = \mathrm{rank}_R(H)$ and S is H-faithful. On the other hand, applying Proposition 3.2.11 to the E-module $M = S$, we have $I(H)S = R$. Then S is H-tame. □

3.2.4 Equivalence between notions

If the Hopf algebra is local, then the three notions studied in this section are equivalent:

Theorem 3.2.13. *Let R be a local ring with maximal ideal m, let H be a local cocommutative R-Hopf algebra with module of integrals $R\theta$ and let S be a finite R-algebra which is also a faithful H-module algebra. The following are equivalent:*

1. *S is H-tame.*
2. *S is H-free.*
3. *S is H-Galois.*

If so, any element $t \in S$ satisfying $\theta t = 1$ is a free generator of S as H-module.

Proof. The part 1. imply 2. is given by Theorem 3.2.7. The part 3. imply 1. is given by Proposition 3.2.12. Finally for 2. imply 3. we use the following theorem that we only state:

Theorem 3.2.14. *Let H be a finite local cocommutative Hopf algebra over a field K, and let S be a H-module algebra which is free of rank one, then S is an H-Galois extension.*

The proof can be found in section 14 of [Chi00]. Since S is free it is isomorphic to H as H-module, so localizing in m we have that S/mS is isomorphic to H/mH as H/mH-module. Now we notice that $H/mH = H'$ is a local cocommutative $K := R/mR$-Hopf algebra, so for the previous theorem S/mS is H/mH-Galois. From Nakayama's lemma follows that being

$$(S \otimes_R S) \otimes_R R/mR = S/mS \otimes_K S/mS \to S/mS \otimes_K (H/mH)^* (S \otimes_R H^*) \otimes_R R/mR$$

an isomorphism, then $S \otimes S \to S \otimes H^*$ it is. □

CHAPTER 4

Integral Hopf–Galois structures

In this last chapter we report and detail the results of [Byo02] by N.P.Byott.
Consider a totally ramified, normal extension L/K of p-adic fields with a degree of p^2, with primitive pth root for the unity ζ contained in K. The study revolves around examining the behavior of the valuation ring $\mathcal{O}_L$ within the diverse Hopf-Galois structures present in L/K. We report the characterization of the possible Hopf Galois structure (Theorem 4.2.1) and the Hopf order associated to a fixed structure (Theorem 4.3.12). In the attempt to answer the question "When $\mathcal{O}_L$ is Hopf Galois?", Byott firstly find some arithmetic necessary conditions on an extension L/K that makes $\mathcal{O}_L$ Hopf Galois (Lemma 4.4.2); secondly he studies the structure of an extension with such proprieties (Lemma 4.4.4); finally he finds necessary and sufficient conditions under which $\mathcal{O}_L$ receives a Hopf-Galois structure with respect to a fixed Hopf order in the corresponding Hopf algebra (Proposition 4.4.7).
Then we move our attention to the realizability of an Hopf order $\mathfrak{O}$, in the sense that there is an extension L/K such that $\mathcal{O}_L$ is $\mathfrak{O}$-Galois. Theorem 4.5.2 gives sufficient and necessary conditions for this question.
Finally, the main result is given by Theorem 4.6.4A-D, that is a complete characterisation of the behavior of $\mathcal{O}_L$ in the different Hopf Galois structures, distinguishing the cases of cyclic and elementary abelian extensions, and of p odd and $p = 2$.

4.1 Some notion about local extension of degree p

In this section we will recall some propriety of extensions of p-adic field that can be found in [Ser79]. After that we briefly introduce some result about Hopf-Galois structure on this extensions.

Let K be an extension $\mathbb{Q}_p$ of degree n. We write $\mathcal{O}_K$ for the valuation ring (ring of integers) of K, $P = (\pi)$ for the unique maximal ideal of $\mathcal{O}_K$ and $\mathrm{ord}_K : K \to$

$\mathbb{Z}\cup\{\infty\}$ for the normalized valuation on K. Finally, we call $e_K = \mathrm{ord}_K(p)$ the absolute ramification index of K.

Could be useful to introduce a valuation on the group of units $\mathcal{O}_K^\times$ of $\mathcal{O}_K$.

Definition 4.1.1. Let $x \in \mathcal{O}_K^\times$ we define:

$$\mathrm{ord}_K^\times(x) := \mathrm{ord}_K(x-1).$$

An easy but very useful propriety is the following:

$$\mathrm{ord}_K^\times(xy) \geq \min\left(\mathrm{ord}_K^\times(x), \mathrm{ord}_K^\times(y)\right), \tag{4.1}$$

with equality holds if and only if $\mathrm{ord}_K^\times(x) \neq \mathrm{ord}_K^\times(y)$.
Thanks to this valuation we have a filtration of the unit group $\mathcal{O}_K^\times$:

$$U_{n,K} := \left\{x \in \mathcal{O}_K^\times \mid \mathrm{ord}_K^\times(x) \geq n\right\} \quad \text{for } n \geq 0.$$

Thanks to the propriety (4.1) we have that this filtration is made of subgroups, not only of sets. We now state some properties of these subgroups:

Proposition 4.1.2. *(i) For all $n \geq 1$, $\frac{U_n}{U_{n+1}} \cong \mathbb{Z}/p^f\mathbb{Z}$*

(ii) For all $n \geq 1$, $\frac{U}{U_n} \cong \left(\frac{\mathcal{O}_F}{P^n}\right)^\times$

From now on let us assume that K contains a primitive p-th root of unity ζ, then $e_K = (p-1)\,\mathrm{ord}_K^\times(\zeta)$ is a multiple of $p-1$.

Using the binomial theorem and the completeness of K, one obtains the following well-known results:

Let $u \in U_n \backslash U_{n+1}$, then exist a $\alpha \in \mathcal{O}_L^\times$ such that $u = 1 + \alpha\pi^n$. For the Newton binomial formula we have:

$$u^p = (1+\alpha\pi^n)^p = 1 + p\alpha\pi^n + \left(\frac{p}{2}\right)\alpha^2\pi^{2n} + \ldots + \alpha^p\pi^{pn}.$$

Then using that $\mathrm{ord}_K(\alpha) = 0$, $\mathrm{ord}_K(p) = e_F$ and $\mathrm{ord}_K(u) = m$ we obtain:

Proposition 4.1.3. *Let K contain a primitive p-th root of unity ζ, and set $e'_K := \mathrm{ord}_K^\times(\zeta) = e_K/(p-1)$. Then*

(i) $\mathrm{ord}_K^\times(x^p) = p\,\mathrm{ord}_K^\times(x)$ *if* $\mathrm{ord}_K^\times(x) < e'_K$;

(ii) $\mathrm{ord}_K^\times(x^p) = \mathrm{ord}_K^\times(x) + e$ *if* $\mathrm{ord}_K^\times(x) > e'_K$;

(iii) $U_n = U_{n-e_K}^p$ *if* $n > pe'_K$;

(iv) $\mathrm{ord}_K^\times(x^p) \geq pe'_K$ *if* $\mathrm{ord}_K^\times(x) = e'_K$, *with equality unless* $\mathrm{ord}_K^\times(\zeta^a x) > e'_K$ *for some* $a \in \mathbb{Z}$

(v) the group $U_{pe'_K}/U_{e'_K}^p$ has order p.

Notation 4.1.4. *For $0 \leq j \leq e' := e'_K$ we write $j' = e' - j$.*

Let us begin by recalling some definitions and findings from ramification theory. Suppose that L is a normal finite extension of K with a Galois group $G = \mathrm{Gal}(L/K)$. In this case, we can define the ramification groups of L/K as follows:

Definition 4.1.5. Let $t \geq -1$ than we define the *i-th ramification group* to be:

$$G_t = \{\sigma \in G \mid \mathrm{ord}_L(\sigma(x) - x) \geq t+1 \text{ for all } x \in \mathcal{O}_L\}.$$

It is easy to check that $G = G_{-1} \supseteq G_0 \supseteq \cdots \supseteq G_n = \{id\}$ and $G_i \lhd G$, since the chain will stop after $max_\sigma\{\mathrm{ord}_L(\sigma(\alpha)-\alpha)\}+1$ steps, where $\alpha \in \mathcal{O}_L$ is such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Moreover, we call G_0 the inertia group.

If $x \in \mathcal{O}_L$ with $\mathrm{ord}_L(x) \not\equiv 0 \bmod (p)$, and if $\sigma \in G_t$ but $\sigma \notin G_{t+1}$ for some $t \geq 1$, then

$$\mathrm{ord}_L(\sigma(x) - x) = \mathrm{ord}_L(x) + t, \quad \mathrm{ord}^\times_L(\sigma(x)/x) = \mathrm{ord}^\times_L(x) + t \tag{4.2}$$

Definition 4.1.6. The *ramification numbers* (*break numbers*) of L/K are the values of t for which $G_{t+1} \neq G_t$.

Remark 4.1.7. The extension L/K is said to be unramified if the only ramification number is $t = -1$, which can only happen only if G is cyclic. On the other hand, the extension is called totally ramified if all the ramification numbers satisfy $t \geq 0$.

In order to understand the relation between the ramification number in the tower of extension, it is interesting to study the ramification group of subgroups and quotients of our Galois group. For the sub groups we have the following result:

Lemma 4.1.8. *Let $H < G$ and call $M = L^H$, then we have $H_i = H \cap G_i$.*

Proof. See [Ser79, Prop. 2, Page 62] □

In the case of quotients it is more complicated, we need to introduce a function associated with the extension L/K:

Definition 4.1.9. Let $u \in R$ then we define $G_u = G_{\lfloor u \rfloor}$ and the following function:

$$\begin{aligned} \varphi_{L/K} : \mathbb{R} &\longrightarrow \mathbb{R} \\ u &\longmapsto \int_0^u \frac{dt}{[G_0 : G_t]}. \end{aligned}$$

It is easy to notice that for $u \in [-1, 0]$ the function is the identity and for $u \in (m, m+1]$ we have:

$$\varphi_{L/K}(u) = \frac{1}{|G_0|} \sum_{i=1}^{m} |G_i| + (u - m)|G_{m+1}|. \tag{4.3}$$

Now we are able to state the result for the quotients:

Theorem 4.1.10 (Herbrand). *Let $H \lhd G$ and $M = L^H$, then*

$$\left(\frac{G}{H}\right)_v = \frac{G_u H}{H},$$

where $v = \varphi_{L/M}(u)$.

Proof. See [Ser79, Lemma 5, pag. 75] □

If L/K has degree p, we have that $|G| = p$ so there is a unique ramification number that we call $t_{L/K}$.

For future use, we next record some properties of the norm $N_{L/K}$:

Proposition 4.1.11. *Let L/K be a totally ramified normal extension of degree p, with Galois group $G = \langle\sigma\rangle$, and with ramification number t. Then*

(i) $N_{L/K}\left(U_{t+pk+1,L}\right) = U_{t+k+1,K}$ *for* $k \geq 1$;

(ii) $\left\{\sigma(x)/x \mid x \in \mathcal{O}_L^\times\right\} = U_{t+1,L} \cap \mathrm{Ker}\,(N_{L/K})$.

Proof. The first point can be found in [Ser79] as Corollary 3 at page 85. The second point can be found in [Gre92] as Lemma II.3.6 □

4.1.1 Behavior of $\mathcal{O}_L$ as a Galois module

As we have seen in Chapter 2 section 4, in the cyclic extension of degree p there is only one Hopf-Galois structure, the classical one. Then Base Change Theorem and Theorem 3.2.13 tell us that $\mathcal{O}_L$ could be a Hopf-Galois extension of $\mathcal{O}_K$ only if is Galois over the associated order. So in the study of Hopf Galois structure on L/K such that $\mathcal{O}_L$ is Galois, is interesting to find all the possible Hopf order occurring in the various Galois Hopf structure. In this case as already reminded we have only the classical Galois structure an the following proposition describe the Hopf orders:

Proposition 4.1.12. *For a cyclic group $G = \langle\sigma\rangle$ of order p, the only Hopf orders in the group algebra $K[G]$ are the orders*

$$\mathfrak{O}_j = \mathcal{O}_K\left[\pi^{-j}(\sigma - 1)\right] \quad \text{for } 0 \leq j \leq e'$$

Proof. See Proposition 3.3 of [Lar76] □

Now we are interested in understanding when $\mathcal{O}_L$ is $\mathfrak{O}_i$-Galois. The problem has been solved in [Chi87] and [Gre92]. We state the key result:

Theorem 4.1.13. *Let L be a normal extension of K of degree p, with Galois group $G = \langle\sigma\rangle$. Then $\mathcal{O}_L$ is $\mathfrak{O}_0$-Galois if and only if L/K is unramified. For $1 \leq j \leq e'$, the following are equivalent:*

(i) $\mathcal{O}_L$ is $\mathfrak{O}_j$-Galois;

(ii) $t_{L/K} = pj - 1$

(iii) $L = K(z)$ *for some* $z \in L$ *such that* $z^p \in K, \sigma(z) = \zeta z$, *and* $\mathrm{ord}_K^\times(z^p) = pj' + 1$.

If these conditions hold, then L/K *is totally ramified,* $\mathrm{ord}_L^\times(z) = pj' + 1$, *and, setting*

$$\mu = \pi^{-j'}(z - 1)$$

we have $\mathrm{ord}_L(\mu) = 1$ *and* $\mathcal{O}_L = \mathcal{O}_K[\mu]$.

Proof. See [Byo02, Theorem 3.4] □

Remark 4.1.14. This result is really strong cause it prove that in this kind of extension $t_{L/K}$ determines whether $\mathcal{O}_L$ is Hopf–Galois.

Corollary 4.1.15. *For a normal extension* L/K *of degree* p, $\mathcal{O}_L$ *is Hopf Galois if and only if* $t_{L/K} \equiv -1 \bmod p$.

Corollary 4.1.16. *Let* G *be a group of order* p, *and let* $\mathfrak{O}$ *be a Hopf order in* $K[G]$. *Then there exists an extension* L *of* K *such that* $\mathcal{O}_L$ *is* $\mathfrak{O}$*-Galois.*

Proof. By Proposition 4.1.12, we have $\mathfrak{O} = \mathfrak{O}_j$ for some $j \geq 0$.
If $j = 0$, take L to be the unique unramified extension of K of degree p, it work thanks to Theorem 4.1.13.
If $j > 0$, we take $w \in K$ with $\mathrm{ord}_K^\times(w) = pj' + 1$ and set $L = K(z)$ with $z^p = w$. Clearly L/K is cyclic of degree p with Galois group generated by a map σ such that $\sigma(z) = \zeta_p z$. Finally, if we check that $z \notin K$, by Theorem 4.1.13 we have that $\mathcal{O}_L$ is $\mathfrak{O}_j$-Galois. Notice that if $z \in K$ then for Proposition 4.1.3 we should have that $\mathrm{ord}_K^\times(w)$ is equal to $p\,\mathrm{ord}_K^\times(z)$ or $\mathrm{ord}_K^\times(z) + e$ or greater then pe', but all this three cases are absurd because $\mathrm{ord}_K^\times(w) = pj' + 1 \leq p(e' - 1) + 1 < pe' = e' + e$ and is not divisible by p. □

4.2 Determining the Hopf-Galois Structures and Hopf Algebras

Now let L/K be a Galois extension of fields of degree p^2, with group G. Thus G is either cyclic or elementary abelian. We present some results from the article [Byo96] that show that L/K has p Hopf–Galois structures if G is cyclic and has p^2 Hopf–Galois structures if G is elementary abelian. As always in order to investigate the number of Hopf Galois structure of an extension we reduce to a group theoretic question thanks to Greither-Pareigis's Theorem. We describe explicitly the p^2 regular subgroups of $\mathrm{Perm}(G)$ which are normalised by $\lambda(G)$.

Theorem 4.2.1. *(Byott). Let L/K be a Galois extension of fields with group G. Let $T \leq G$ have order p, let $d \in \{0, 1, \ldots, p-1\}$, and fix $\sigma, \tau \in G$ satisfying:*

$$T = \langle \tau \rangle, \quad \begin{cases} \sigma^p = \tau & \text{if cyclic} \\ \sigma^p = 1 & \text{otherwise.} \end{cases}, \quad G = \langle \sigma, \tau \rangle$$

There are well defined elements $\rho, \eta \in \mathrm{Perm}(G)$ determined by:

$$\rho\left(\sigma^k \tau^l\right) = \sigma^k \tau^{l-1}$$
$$\eta\left(\sigma^k \tau^l\right) = \sigma^{k-1} \tau^{l+(k-1)d} \qquad \text{for } k, l \in \mathbb{Z}$$

We have $\rho\eta = \eta\rho$ and

$$\rho^p = 1, \quad \eta^p = \begin{cases} \rho & \text{if } G \text{ cyclic or non-cyclic with } p = 2, d = 1 \\ 1 & \text{otherwise} \end{cases}$$

Now set $N = N_{T,d} = \langle \rho, \eta \rangle$. Then N is a subgroup of $\mathrm{Perm}(G)$ of order p^2, and $N \cong G$ unless $p = 2, d = 1$. In all cases, N is a regular subgroup of $\mathrm{Perm}(G)$, and is normalised by $\lambda(G)$. Thus N gives rise to a Hopf-Galois structure on L/K, with Hopf Algebra $H = H_{T,d} = L\left[N_{T,d}\right]^G$. If $d = 0$ then $N = \lambda(G)$, giving the classical structure regardless of the choice of T. If $d \neq 0$ then the $p-1$ possible choices of d, together with the $p+1$ (resp. 1) possible choices of T in the case G is elementary abelian (resp. cyclic), yield $p^2 - 1$ (resp. $p-1$) distinct groups N, each giving rise to a non-classical structure on L/K. This Hopf Galois structure are the unique on L/K.

Proof. See [Byo96, Theorem 2.5]. □

Thanks to 2.4.1 we already knew part of the previous Theorem, but describing each of the (possibly cyclic) groups $G = (\sigma, \tau)$ and $N = (\rho, \eta)$ in terms of two generators has enable us to treat the cyclic and elementary abelian cases simultaneously and to handle the exceptional case $p = 2$.

Remark 4.2.2. When G is an elementary abelian group, we derive $p+1$ distinct representations of the group $N = \rho(G)$ by setting $d = 0$ and allowing T to vary over all subgroups of G with order p. Nevertheless, when $d \neq 0$, the group T is uniquely determined by N (and consequently by $H = L[N]^G$) due to the fact that the intersection of $\lambda(G)$ and N is $\langle \rho \rangle = T_l$.

Notice that in the case of an odd prime p and G a cyclic group the element η of theorem 4.2.1 can be written as:

$$\eta^r(\sigma^i) = \sigma^{(i-r)+(ir-\frac{r(r+1)}{2})pd}. \tag{4.4}$$

From now on we will investigate two particular extensions as an example of application of the theory:

Example 4.2.3. Let $K = \mathbb{Q}_p(\zeta_p)$ and $L = \mathbb{Q}_p(\zeta_{p^3})$, then L/K is a totally ramified cyclic Galois extension of degree p^2. If we take $p = 3$, then $G = Gal(L/K) = \mathbb{Z}/9\mathbb{Z}$ is generated by:

$$\begin{aligned} \sigma : L &\longrightarrow L \\ \zeta_{27} &\longmapsto \zeta_{27}^4. \end{aligned}$$

We investigate the possible Hopf Galois structures in this extension using Theorem 4.2.1. Identifying G with $\lambda(G) < \mathrm{Perm}(G)$ we have that σ is identified with the permutation $(1,2,3,4,5,6,7,8,9)$. Now using the formula (4.4) we obtain that if $d = 1$ then $\eta(\sigma^i) = \sigma^{(i-1)4}$, otherwise if $d = 2$ we have $\eta(\sigma^i) = \sigma^{(i-1)7}$. This tells us that in N_1 (resp.N_2) the generator η is identified with the permutation $(9,5,7,6,2,4,3,8)$ (resp. $(0,2,7,6,8,4,3,5,1)$)

Example 4.2.4. Let $K = \mathbb{Q}_2$ and[1] $L = \mathbb{Q}_2(\sqrt{2}, \zeta_4)$, then L/K is a totally ramified elementary abelian Galois extension of degree 4. The Galois group $G = Gal(L/K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is generated by:

$$\begin{aligned} a : L &\longrightarrow L & \qquad b : L &\longrightarrow L, \\ \zeta_4 &\longmapsto -\zeta_4, & \qquad \sqrt{2} &\longmapsto -\sqrt{2} \end{aligned}$$

Similarly to Example 4.2.3 we investigate the possible Hopf Galois structures. Identifying G with $\lambda(G) < \mathrm{Perm}(G)$ we have that a is identified with the permutation $(0,1)(2,3)$ and b with $(0,2)(1,3)$. For $d = 0$ we have the classical structure for every subgroup of order 2 of G. On the other hand, for $d = 1$ we have three different structures in correspondence with the three subgroups of order 2 of G. In the case $T = \langle b \rangle$ we have $\rho = (0,2)(1,3)$ and $\eta = (0,3,2,1)$, for $T = \langle a \rangle$ we have $\rho = (0,1)(2,3)$ and $\eta = (0,3,1,2)$ and, finally for $T = \langle ab \rangle$ we have $\rho = (0,3)(1,3)$ and $\eta = (0,2,3,1)$. So we found, according to Theorem 4.2.1, that when $d = 1$ we have $N \ncong G$.

Now we give a more explicit description of the algebra $H_{T,d}$.
By Remark 4.2.2 we know that $K[\rho] \subset H$, then we start studying this subgroup. Since K contains the p-th root of unity, the group algebra $K[\rho]$ has a basis of mutually orthogonal idempotents:

$$e_s = \frac{1}{p} \sum_{k=0}^{p-1} \zeta^{-ks} \rho^k \quad \text{for } 0 \le s \le p-1 \tag{4.5}$$

satisfying

$$\rho e_s = e_s \rho = \zeta^s e_s. \tag{4.6}$$

Let $M = L^T$ be the subfield of L fixed by $T = \langle \tau \rangle$. Thus M/K is cyclic of degree p. Fix $v \in M^\times$ satisfying

[1] We call the forth root of unity ζ_4 and not i in order to avoid confusion in the other part of the example.

$$\sigma(v) = \zeta^{-d} v, \tag{4.7}$$

and set

$$a_v = \sum_{s=0}^{p-1} v^s e_s \in M[\rho]. \tag{4.8}$$

Proposition 4.2.5. *With the above notation, for $d \neq 0$, we have $H_{T,d} = K\left[\rho, a_v\eta\right]$*

Proof. Let $H = H_{T,d}$.

By Greither-Pareigis theorem, $H = L[N]^G$ for some regular subgroup N of $\mathrm{Perm}(G)$ which is normalised by $\lambda(G)$, and where G acts on L as the Galois group and on N by conjugation via λ.

We recall that H has dimension p^2 as a K-algebra. Since $\rho^p = 1_N$ and

$$\left(a_v\eta\right)^p = \sum_{s=0}^{p-1} v^{ps} e_s \eta^p = \sum_{s=0}^{p-1} v^{ps} e_s \in K[\rho]$$

we have that $K\left[\rho, a_v\eta\right]$ is also a K-subalgebra of $L[N]$ of dimension p^2. It will therefore suffice to show that $K\left[\rho, a_v\eta\right]$ is fixed element wise by G. We see easily that ${}^g\rho = \rho$ for all $g \in G$, and so every element of $K[\rho]$ is fixed by G. In particular this implies that the idempotents $e_s \in K[\rho]$ are fixed by G. Now $K\left[a_v\eta, \rho\right]$ is generated over $K[\rho]$ by $a_v\eta$, so it remains only to show that $a_v\eta$ is fixed by G. We calculate ${}^\tau\eta = \eta, {}^\sigma\eta = \rho^d\eta$ and recall that $v \in L^T = L^{\langle\tau\rangle}$. Then:

$$\begin{aligned}
\tau\left(a_v\eta\right) &= \sum_{s=0}^{p-1} \tau(v)^s \left({}^\tau\left(e_s\eta\right)\right) \\
&= \sum_{s=0}^{p-1} v^s e_s \eta \\
&= a_v\eta
\end{aligned}$$

and

$$\begin{aligned}
\sigma\left(a_v\eta\right) &= \sum_{s=0}^{p-1} \sigma(v)^s \left({}^\sigma\left(e_s\eta\right)\right) \\
&= \sum_{s=0}^{p-1} \sigma(v)^s e_s \rho^d \eta \\
&= \sum_{s=0}^{p-1} \zeta^{-ds} v^s e_s \zeta^{ds} \eta \\
&= a_v\eta,
\end{aligned}$$

where we use (4.6) and (4.7). This completes the proof. □

Example 4.2.6. Assume we are in the setting of Example 4.2.3. In this case we have that necessarily $T = \langle \tau \rangle$ with $\tau = \sigma^3$ and $M = \mathbb{Q}_3(\zeta_9)$. We need to find a v that satisfies equation 4.5:
if we assume $d = 0$ it is pretty easy and we can take $v = \zeta_3$. In the case $d = 2$ we can take $v = \zeta_9^2$, indeed

$$\sigma(\zeta_9^2) = \sigma(\zeta_{27}^6) = \zeta_{27}^2 4 = \zeta_9^8 = \zeta_9^2 \cdot \zeta_9^6 = \zeta_9^2 \cdot \zeta_3^{-1}.$$

Similarly, if $d = 2$ we can take $v = \zeta_9^7$.

Example 4.2.7. Assume we are in the setting of Example 4.2.4. We need to find a v that satisfies equation 4.5, in this case we can take the following:

- $d = 0$: $v = 1$
- $d = 1$ and $T = \langle b \rangle$: $v = \zeta_4$, and $a_v = (Id + \rho)\left(\frac{1-\zeta_4}{2}\right)$
- $d = 1$ and $T = \langle a \rangle$: $v = \sqrt{2}$, and $a_v = (Id + \rho)\left(\frac{1-\sqrt{2}}{2}\right)$
- $d = 1$ and $T = \langle ab \rangle$: $v = \zeta_4\sqrt{2}$, and $a_v = (Id + \rho)\left(\frac{1-\zeta_4\sqrt{2}}{2}\right)$.

4.3 Hopf order of rank p^2

As we said in Section 4.1.1 in order to investigate the Hopf Galois structure of $\mathcal{O}_L$ is important to know all the possible Hopf order over which it can be a Hopf Galois module. In this section we study the Hopf orders contained in the Hopf algebras found in Theorem 4.2.1. We start explaining what it means for a sequence of R-Hopf algebra homomorphism:

$$R \to J \xrightarrow{f} H \xrightarrow{g} P \to R$$

to be exact. Let H be a R-Hopf algebra, the kernel of the counit ε is denominated H^+.

Definition 4.3.1. Let $f : J \to H$ be a Hopf algebra homomorphism. Then f is normal if $f(J^+)H = Hf(J^+)$.

Now we want to definite a similar propriety for the surjective map g. In order to do that we have to introduce some particular subalgebras:

Definition 4.3.2. Let $g : H \to P$ be a Hopf algebra homomorphism. The *algebra of right coinvariants*, $H^{co(g)}$, is the equalizer of the two maps from H to $H \otimes P$: $(1 \otimes g) \circ \Delta$ and $(1 \otimes i\varepsilon) \circ \Delta$. The *algebra of left coinvariants*, ${}^{co(g)}H$, is the equalizer of the two maps from H to $P \otimes H$: $(g \otimes 1) \circ \Delta$ and $(i\varepsilon \otimes 1) \circ \Delta$.

Definition 4.3.3. The Hopf algebra morphism $g : H \to P$ is *conormal* if ${}^{co(g)}H = H^{co(g)}$.

Now we state a Proposition that will clarifies how to create short exact sequence starting from a surjective and conormal map:

Proposition 4.3.4. *If g is conormal and $H_1 = H^{co(g)}$ is an R-module direct summand of H, then H_1 is a sub-Hopf algebra of H.*

Proof. See [Chi00, Chapter 1, Proposition 4.10]. □

Definition 4.3.5. If $g : H \to P$ is conormal and $H^{co(g)}$ is a Hopf algebra, then $H^{co(g)} = hker(g)$ is called the *Hopf kernel* of g.

Definition 4.3.6. A *short exact sequence of R-Hopf algebras* is a sequence of Hopf algebra maps $f : J \to H$, $g : H \to P$, such that f is injective and normal, g is surjective and conormal, $P \cong H/J$ via g and $J \cong hker(g)$ via f.

Related to the concept of short exact sequence we state the following lemma:

Lemma 4.3.7. *Let R be a noetherian integral domain and let $J \hookrightarrow H \to P$ be a short exact sequence of finite R-Hopf algebras. Let S be an H-module algebra, and set*

$$S^J = \{s \in S \mid j \cdot s = \varepsilon(j)s \text{ for all } j \in J\}$$

Then:
S is H-Galois over $R \Leftrightarrow$

$$S^J \text{ is } P\text{-Galois over } R \text{ and } S \text{ is } J \otimes_R S^J\text{-Galois over } S^J.$$

Proof. The proof can be found in [Gre92] as Lemma II.1.7. □

Let K and L be two fields as in the previous section. If $\mathcal{O}_L$ is $\mathfrak{O}$-Galois for a $\mathcal{O}_K$-Hopf algebra $\mathfrak{O}$, then $\mathfrak{O}$ must be a Hopf order in one of the $\mathcal{O}_K$-Hopf algebras denoted as $H = H_{T,d}$ in Theorem 4.2.1. Consequently, we say that $\mathcal{O}_L$ is Hopf-Galois with respect to H. If $\mathcal{O}_L$ is Hopf-Galois with respect to any Hopf-Galois structure on L/K, we simply refer to it as Hopf-Galois.

We express H as $H = L[N]^G$, where $N = N_{T,d} = \langle \rho, \eta \rangle$. Within $N/\langle \rho \rangle$, we denote the image of η as $\bar{\eta}$. As a result, the short exact sequence of abelian groups:

$$0 \to \langle \rho \rangle \to N \to \langle \bar{\eta} \rangle \to 0$$

gives rise to a short exact sequence of K-Hopf algebras:

$$K[\rho] \hookrightarrow H \to K[\bar{\eta}]$$

In this sequence, the idempotent $e_s \in H$ of (4.5) is mapped to 1 when $s = 0$ and to 0 when $1 \leq s \leq p-1$. Let $\mathfrak{O}^{(1)} = \mathfrak{O} \cap K[\rho]$ and $\mathfrak{O}^{(2)}$ be the image of $\mathfrak{O}$ in $K[\bar{\eta}]$. Consequently, $\mathfrak{O}^{(1)}$ and $\mathfrak{O}^{(2)}$ are $\mathcal{O}_K$-Hopf orders in the K-Hopf algebras $K[\rho]$ and $K[\bar{\eta}]$, respectively. Thus, we have a short exact sequence of $\mathcal{O}_K$-Hopf algebras:

$$\mathfrak{O}^{(1)} \hookrightarrow \mathfrak{O} \to \mathfrak{O}^{(2)}.$$

We can improve the previous discussion using the characterization of Hopf orders in KG:

Lemma 4.3.8. *Let L, K as in the previous discussion, let $M = L^T$ and suppose that $\mathcal{O}_L$ is $\mathfrak{O}$-Galois for some Hopf order $\mathfrak{O} \subset H = H_{T,d}$. Then we have a short exact sequence of $\mathcal{O}_K$-Hopf algebras:*

$$\mathfrak{O}_i \hookrightarrow \mathfrak{O} \to \mathfrak{O}_j, \tag{4.9}$$

for some $0 \leq i, j \leq e'$.
Furthermore, if L/K is totally ramified then $i, j > 0$ and $t_{M/K} = pj - 1$, $t_{L/M} = p^2 i - 1$.

Proof. From the preceding discussion and Proposition 4.1.12 we have the short exact sequence (4.9). By Lemma 4.3.7, $\mathcal{O}_L$ is $\mathfrak{O}_i \otimes \mathcal{O}_M$-Galois over $\mathcal{O}_M$ and $\mathcal{O}_M$ is $\mathfrak{O}_j$-Galois over $\mathcal{O}_K$. (More precisely, $\mathcal{O}_L$ is Galois for $\mathcal{O}_M\left[\pi^{-i}(\rho - 1)\right] = \mathcal{O}_M\left[\pi_M^{-pi}(\rho - 1)\right]$ where ρ acts on L like $\tau \in \mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$, and $\mathcal{O}_M$ is Galois for $\mathcal{O}_K\left[\pi^{-j}(\bar{\eta} - 1)\right]$ where $\bar{\eta}$ acts on M like $\sigma T \in G/T = \mathrm{Gal}(M/K)$.) If we assume that L/K is totally ramified then M/K and L/M are both totally ramified, so in particular not unramified. Applying Theorem 4.1.13 to M/K we find that $j > 0$ and $t_{M/K} = pj - 1$. Applying the same Theorem to L/M, and noting that since the extension is totally ramified $\mathrm{ord}_M(\pi) = p$, we obtain $i > 0$ and[2] $t_{L/M} = p^2 i - 1$. □

Notice that is not unique the short exact sequence of a certain order $\mathfrak{O}$:

Remark 4.3.9. If L/K is elementary abelian and $d = 0$, then we obtain the same H for any of the $p+1$ choices of T and correspondingly obtain $p+1$ short exact sequences (4.9) containing the same $\mathfrak{O}$. The parameters i, j may depend on the choice of T.

We need to compute the ramification numbers for our examples to understand which Hopf Galois structures are interesting in the sense of Lemma 4.3.8:

Example 4.3.10. Let us assume that we are in the setting of Example 4.2.3. We can write explicitly the ramification group of the extension $\mathbb{Q}_p(\zeta_{p^3})/\mathbb{Q}_p$:

- $G_0 = G$,
- $G_1 = G_2 = \{a \in (\mathbb{Z}/27\mathbb{Z})^* \mid a \cong 1 \bmod 3\}$
- $G_3 = \ldots = G_8 = \{a \in (\mathbb{Z}/27\mathbb{Z})^* \mid a \cong 1 \bmod 9\}$

[2]Note that $\mathcal{O}_M\left[\pi^{-i}(\rho - 1)\right] = \mathfrak{O}_{pi}$ since if π_M is an uniformizer of $\mathcal{O}_M$ we have that $\pi_M^p = \pi$.

Using Lemma 4.1.8 and noticing that $G_1 = Gal(L/K)$ we have that the ramification numbers of L/K are $t_1 = 2 = p-1$ and $t_2 = 8 = p^2-1$. So thanks to Lemma 4.3.8 we can reduce to study the structure with $i = j = 1$. Moreover, we notice that $e_K = \mathrm{ord}_K(p) = p-1$ and $e'_K = ord^*_K(\zeta_3) = 1$, consequently in our case we have that $i' = j' = 0$.

Example 4.3.11. Let us assume that we are in the setting of Example 4.2.4. Let us consider the subextensions $F_1 = \mathbb{Q}_2(\zeta_4)$ and $F_2 = \mathbb{Q}_2(\sqrt{2})$. The former has ramification number $t_{F_1} = 1$ and uniformizer $\pi_{F_1} = \zeta_4 + 1$, the latter has ramification number $t_{F_2} = 2$ and uniformizer $\pi_{F_2} = \sqrt{2}$. Since $t_{F_2} > t_{F_1}$ we have that $t_1 = t_{F_1} = 1$ and $t_2 = 2(t_{F_2} - t_{F_1}) + t_{F_1} = 3$. So thanks to Lemma 4.3.8 we can reduce to study the structure with $i = j = 1$. Moreover, we notice that $e_K = \mathrm{ord}_K(2) = 1$ and $e'_K = 1$, consequently in our case we have that $i' = j' = 0$. In order to understand who is G_2 we notice that $\pi_L = \frac{1+\zeta_4}{\sqrt{2}} - 1$ is a uniformizer and $\mathrm{ord}_L(a(\pi) - \pi) = \mathrm{ord}_L(-\frac{1+\zeta_4}{\sqrt{2}} - \frac{1+\zeta_4}{\sqrt{2}}) = \mathrm{ord}_L(2\frac{1+\zeta_4}{\sqrt{2}}) = 4$. From this follows that $G_2 = G_3 = \langle b \rangle$. Let us assume that we are in the setting of Example 4.2.4.

Now, as done for the extension of degree p, we aim to provide a comprehensive description of all the $\mathcal{O}_K$-Hopf algebras $\mathfrak{O}$ which are Hopf orders in a given Hopf algebra $H = H_{T,d} = L[N]^G$. In this case, thanks to Lemma 4.3.8, we can also assume that they fit into a short exact sequence (4.9) for given i and j. This problem was solved by Byott, Greither and Childs in some of their previous work. The theory has been summarized in Chapters 9 of [Chi00]. The following theorem summarizes the results and gives a complete characterization of the Hopf orders depending on a parameter $v \in M^\times$ (notice that this parameter is the same that appear in the explicit description of H in Proposition 4.2.5):

Theorem 4.3.12. *Let $H = H_{T,d}$ be a K-Hopf algebra giving a Hopf-Galois structure to L/K, let $M = L^T$ and let $0 \le i, j \le e'$. Then the Hopf orders $\mathfrak{O}$ of H that fit into the short sequence (4.9) are the orders:*

$$\mathfrak{S}_v = \mathcal{O}_K\left[\pi^{-i}(\rho - 1), \pi^{-j}\left(a_v\eta - 1\right)\right]$$

where $v \in \mathcal{O}_M^\times$ with $\sigma(v) = \zeta^{-d}v$ and one of the following holds:

(i) (Hopf orders of elementary abelian type) N is elementary abelian and

$$v^p \in U_{pi'+j,K} \cap U_{pj+i',K} \tag{4.10}$$

(ii) (Greither orders) N is cyclic, $pj \le i$, and

$$v^p \in U_{pi'+j,K} \quad \text{and} \quad \zeta v^p \in U_{pj+i',K} \tag{4.11}$$

(iii) (dual Greither orders) N is cyclic, $pi' \leq j'$, and v^p satisfies the preceding condition (4.11).

In each of these cases we have $\mathfrak{S}_v = \mathfrak{S}_w \Leftrightarrow vw^{-1} \in U_{i'+j,K}$.

Proof. The correspondence between Hopf order and the element v is the Theorem 3 of [Byo93]. Moreover, arguing as in Theorem 2.1 of [Chi96] we find the necessity and sufficiency of one of the condition (i), (ii) or (iii). □

Example 4.3.13. Thanks to Example 4.3.10, we need to investigate only the case $i = j = 1$. Hence, the only case of Theorem 4.3.12 that is interesting for us is (iii). Since $j' = i' = 0$ the condition needed for v^3 becomes:

$$v^3 \in U_{1,K} \quad \text{and} \quad \zeta_3 v^3 \in U_{3,K}.$$

In Example 4.2.6 we decided to take as v one of the following ζ_3, ζ_9^2 or ζ_9^7, depending on the d chosen. For example, if $d = 1$ then $v = \zeta_9^2$ so we have that $v^3 = \zeta_3^2 \in U_{1,K}$ and $\zeta_3 v^3 = 1 \in U_{3,K}$, so in this case the unique Hopf order to consider is the dual Greither order: $\mathfrak{S}_{\zeta_9^2} = \mathcal{O}_K\left[(\zeta_3 - 1)^{-1}(\rho - 1), (\zeta_3 - 1)^{-1}\left(a_{\zeta_9^2}\eta - 1\right)\right]$. On the other hand, for $d = 0$ and $i = j = 1$ there are no Hopf orders, indeed $v^3 = 1$ and so $v^3\zeta_3 = \zeta_3 \notin U_{3,K}$.

Example 4.3.14. Thanks to Example 4.3.11, we need to investigate only the case $i = j = 1$. In this case, the only case of Theorem 4.3.12 that is interesting for us is (i). The condition 4.10 becomes $v^p \in U_{1,K} \cap U_{2,K} = U_{2,K}$. For that reason the case $d = 1$ with $T = \langle a \rangle$ or $T = \langle ab \rangle$ doesn't have an Hopf order since they have respectively $v = \sqrt{2}$ and $v = \zeta_4\sqrt{2}$. So we exclude this two case, in accordance with Lemma 4.4.2 that tells us that the only interesting case are the ones with $T = G_{t_2}$. In the case $d = 1$ and $T = \langle b \rangle$ we have the Hopf order:

$$\mathfrak{S}_{\zeta_4} = \mathbb{Z}_2\left[\frac{\eta^2 - 1}{2}, \frac{(\eta + \eta^3)\frac{1-\zeta_4}{2} - 1}{2}\right].$$

Remark 4.3.15. In Example 4.3.13 we found an extension L/K of p-adic fields such that in the classical Galois structure there are not Hopf orders, so the associated order can't be an Hopf order. Moreover thanks to Theorem 1 of [Let98]:

Theorem 4.3.16. *Let L be a finite extension of a p-adic field K. If the extension $L/\mathbb{Q}_p$ is abelian, then $\mathcal{O}_L \cong \mathfrak{A}_{L/K}$.*

We have that the extension $\mathbb{Q}_p(\zeta_p^3)/\mathbb{Q}_p(\zeta_p)$ is an example of extension with $\mathcal{O}_L$ free over the associated order (of the classical structure) but such that the associated order is not an Hopf order.

In the previous Theorem there is an ambiguity on the name of the different orders:
if N is cyclic both the conditions $pj \geq i, pi' \geq j'$ may hold. In this case each Hopf

order can be viewed either as a Greither order or as a dual Greither order (with the same parameter v). It is convenient to remove this ambiguity, in order to avoid any possible misunderstanding, by making the following assumption:

Convention 4.3.17. *For N cyclic, we regard a Hopf order with parameters i, j as a Greither order if $i + j \leq e'$ (that is, if $j \leq i'$) and as a dual Greither order if $i + j > e'$.*

The names of the various classes of orders are justified by the following consideration:

Remark 4.3.18. Away from the line $i + j = e'$, the dual of a Greither order is a dual Greither order, and the converse is true, since duality interchanges i' and j. When $i + j = e'$, the previous convention forces us to label the dual of a Greither order as another Greither order. This slight anomaly will not cause us any difficulties.

The pairs (i, j) for which Greither orders and dual Greither orders can occur are then as indicated in figure 4.1.

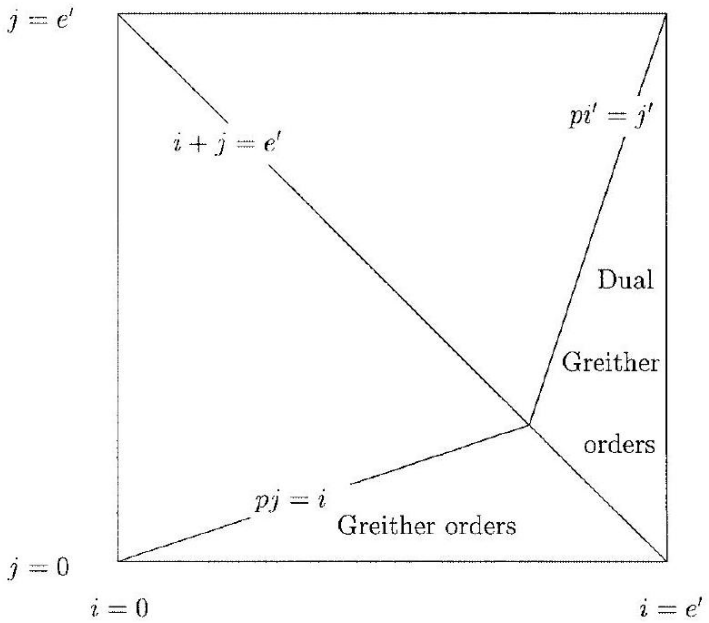


Figure 4.1: Regions of definition of Greither orders and dual Greither orders.

Remark 4.3.19. (i) In the case of Greither orders we have $\zeta \in U_{pj+i',K}$, since $\mathrm{ord}_K^{\times}(\zeta) = e'$ and $pj \leq i$, so that (4.10) and (4.11) are equivalent. In the case of dual Greither order the condition (4.11) for the dual orders can be rewrite as:

$$\zeta v^p \in U_{pi'+j,K} \cap U_{pj+i',K}$$

(ii) To construct the Hopf algebra $H_{T,d}$ and the Hopf order $\mathfrak{S}_v$ inside it, we do not need to specify the field L completely. The data required to construct $\mathfrak{S}_v$ consist of the group N, the integers i, j, and the parameter v (which determines the field $M = K(v)$ if $d \neq 0$).

4.4 Field extensions of degree p^2

From now on, we consider only totally ramified extensions L/K. In this section we study the arithmetic of a totally ramified normal extension L/K of degree p^2 in which $\mathcal{O}_L$ is Hopf Galois. This study bring us to answer the question:

When $\mathcal{O}_L$ is Hopf Galois?

4.4.1 Necessary condition for being Galois

In this subsetion our aim is to find some arithmetic necessary condition on an extension L/K that makes $\mathcal{O}_L$ Hopf Galois. Let us describe briefly our setting:

Thanks to assumption of total ramification we need to consider only Hopf orders $\mathfrak{S}_v$, as in Theorem 4.3.12, with $i, j > 0$. The extension L/K either has two distinct ramification numbers $t_1 < t_2$ (so G_{t_2} has order p) or has a unique ramification number t (so G_t has order p^2 but G_{t+1} is trivial). In the latter case we set $t_1 = t_2 = t$. We consider a presentation of $G = \mathrm{Gal}(L/K)$ as in Theorem 4.2.1 and as already done we take $T = \langle \tau \rangle$ and $M = L^T$.

Now we have two important subgroups of G, both of order p. The first one is T that appear in the chosen rappresentation of G, the second one is G_{t_2} that except for the case with only one ramification number has also order p. Notice that the second group is only related with the arithmetic of L/K. If G is cyclic, these subgroups necessarily coincide. If G is elementary abelian, they may or may not coincide. Let $H = H_{T,d}$ be a Hopf algebra endowing L/K with a Hopf-Galois structure, as in Theorem 4.2.1. In the remark 4.2.2 we notice that T is completely determined by H except when $d = 0$, and in this last case all the subgroup T give the classical Hopf Galois structure. So there is a natural convention that we will adopt:

Convention 4.4.1. *If L/K has two distinct ramification numbers then, in the classical Hopf-Galois structure on L/K, we take T to be G_{t_2}. That is, if $H = H_{T,d}$ determines a Hopf-Galois structure on L/K, we shall always assume that either $T = G_{t_2}$ or $d \neq 0$. (If L/K has a unique ramification number, T may be chosen arbitrarily.)*

Now we prove a lemma that shows some necessary condition on the arithmetic of the extension in order to have the existence of an Hopf order that makes $\mathcal{O}_L$ Hopf Galois. Returning to the previous discussion the following lemma state also that in the assumption of being Galois the two subgroups that we point out from the arithmetic and the presentation have to coincide:

Lemma 4.4.2. *Suppose that $\mathcal{O}_L$ is $\mathfrak{S}_v$-Galois, where $\mathfrak{S}_v$ is a Hopf order in $H = H_{T,d}$ with parameters i, j, d as in Theorem 4.3.12. Then $M = K(z)$ with $z^p \in K, \sigma(z) = \zeta z$ and $\mathrm{ord}_M^\times(z) = pj' + 1$. The ramification numbers $t_1 \leq t_2$ of L/K satisfy*

$$t_1 = t_{M/K} = pj - 1, \quad t_2 = t_{L/M} = p^2 i - 1,$$

so that, in particular, $j \leq pi$. If $t_1 \neq t_2$ then $T = G_{t_2}$. Moreover:

$$v = cz^{-d} \quad \text{for some } c \in \mathcal{O}_K^\times. \tag{4.12}$$

Proof. Since M/K is totally ramified, we have $t_{M/K} = pj - 1$, $t_{L/M} = p^2 i - 1$ by Lemma 4.3.8, and $M = K(z)$, with z as stated, by Lemma 4.1.13. From Theorem 4.3.12, $v \in \mathcal{O}_M^\times$ so $vz^d \in \mathcal{O}_M^\times$ and $\sigma(v) = \zeta^{-d} v$. Since vz^d is fixed by both τ, σ we have that it belong to $\mathcal{O}_M^\times \cap K = \mathcal{O}_K^\times$, giving (4.12).

- If $t_1 < t_2$ and $T = G_{t_2}$ then using Lemma 4.1.8 we have $t_{L/M} = t_2$, and, using Herbrand's Theorem, we find that $t_1 = t_{M/K}$. Thus $j < pi$.
- If $t_1 = t_2$ then using the same statement used in the previous case we have $t_{L/M} = t_{M/K} = t_1$ and $j = pi$.
- Finally if $t_1 < t_2$, $T \neq G_{t_2}$, then we find a contradiction. By Convention 4.4.1 we have that $d \neq 0$. Now using Lemma 4.1.8 we obtain $t_{L/M} = t_1$, and by Herbrand's Theorem and (4.3) we find $t_{M/K} = t_1 + (t_2 - t_1)/p > t_1$. Thus $j > pi$. Now either (4.10) or (4.11) holds, so $\mathrm{ord}_K^\times(v^p) \geq pi' + j > pe'$. Whence using that the extension M/K has degree p and is totally ramified we obtain $\mathrm{ord}_M^\times(v^p) > p^2 e'$. Using Proposition 4.1.3, it follows that[3]:

  $$\mathrm{ord}_M^\times(v) \geq pe' > pj' + 1 = \mathrm{ord}_M^\times(z) = \mathrm{ord}_M^\times(z^{-d}),$$

  from which using 4.12 we deduce:

  $$\mathrm{ord}_M^\times(c) = \mathrm{ord}_M^\times(z^{-d}) = pj' + 1.$$

  This is impossible since $c \in K$: $\mathrm{ord}_M^\times(c) = p\,\mathrm{ord}_K^\times(c) \equiv 0 \pmod{p}$.

□

Example 4.4.3. The results from Lemma 4.4.2 are almost trivial in the case of our example. Indeed, being a cyclic extension, the condition $T = G_{t_2}$ is trivial and it is clear that we can take $z = \zeta_9$. The only thing to check is equation 4.12:

- if $d = 0$: we have $v = \zeta_3 \in \mathcal{O}_K^\times$,
- if $d = 1$: we have $v = \zeta_9^2 = \zeta_9^3 \cdot \zeta_9^8 = \zeta_3 \cdot \zeta_9^{-1}$,

[3] We are using that since the extension is totally ramified we have $j > 0$.

- if $d = 2$: we have $v = \zeta_9^7 = \zeta_9^{-2}$.

When L/K has two distinct ramification numbers, Lemma 4.4.2 indicates that our focus should be solely on Hopf-Galois structures where $T = G_{t_2}$. Consequently, in the context of an elementary abelian L/K with two distinct ramification numbers, it can be deduced that $\mathcal{O}_L$ is Hopf-Galois in a maximum of p out of the p^2 Hopf-Galois structures available, the same number of possible extension as in the cyclic case.

4.4.2 When is $\mathcal{O}_L$ $\mathfrak{S}_v$-Galois?

Now we know some arithmetic propriety that L/K must have to be consistent with $\mathcal{O}_L$ being Hopf-Galois. So our focus shifts to study those extension L of K that have the required properties. The following proposition algebraically characterizes these extensions depending on a parameter $\beta \in M^\times$:

Lemma 4.4.4. *Let L/K be a totally ramified extension of degree p^2, with Galois group G as in 4.2.1, and let $M = L^T$. Suppose that $t_{M/K} = pj - 1$ and $t_{L/M} = p^2 i - 1$ with $j \le pi$. Then there exist $z \in M$ and $x \in L$ such that*

$$M = K(z), \quad \sigma(z) = \zeta z, \quad \tau(z) = z, \quad z^p \in K, \quad \operatorname{ord}_K^\times\left(z^p\right) = pj' + 1$$

and

$$L = M(x), \quad \tau(x) = \zeta x, \quad x^p \in M, \quad \operatorname{ord}_M^\times\left(x^p\right) = p^2 i' + 1.$$

Setting $\mu = \pi^{-j'}(z-1)$ and $\nu = \pi^{-i'}(x-1)$, we have $\operatorname{ord}_M(\mu) = \operatorname{ord}_L(\nu) = 1$ and $\mathcal{O}_L = \mathcal{O}_K[\nu]$. Also, $\sigma(x) = \beta x$ for some $\beta \in M$ satisfying

$$N_{M/K}(\beta) = \begin{cases} 1 & \text{if } G \text{ is elementary abelian} \\ \zeta & \text{if } G \text{ is cyclic;} \end{cases} \tag{4.13}$$

and

$$\operatorname{ord}_M^\times(\beta) = pi' + j, \quad \operatorname{ord}_M^\times\left(\beta^p\right) = p^2 i' + pj.$$

Proof. The existence of z and x as stated comes from Lemma 4.1.13, applied first to the extension M/K and then to the extension L/M. This also shows that $\operatorname{ord}_M(\mu) = \operatorname{ord}_L(\nu) = 1$, so that $\mathcal{O}_L = \mathcal{O}_K[\nu]$ since L/K is totally ramified.

Now define $\beta \in L^\times$ as the element such that $\sigma(x) = \beta x$. Then $\tau\sigma(x) = \tau(\beta)\tau(x) = \tau(\beta)\zeta x$, while on the other hand $\tau\sigma(x) = \sigma(\tau(x)) = \sigma(\zeta x) = \zeta\sigma(x) = \zeta\beta x$. Thus $\tau(\beta) = \beta$ and hence $\beta \in M$. Also

$$N_{M/K}(\beta) = N_{M/K}(\sigma(x)/x) = \prod_{r=0}^{p-1} \sigma^r(\sigma(x)/x) = \sigma^p(x)/x. \tag{4.14}$$

If G is elementary abelian then $\sigma^p = 1$ and $N_{M/K}(\beta) = 1$. If G is cyclic then $\sigma^p = \tau$ and $N_{M/K}(\beta) = \tau(x)/x = \zeta$. This proves (4.13).

As $j \leq pi$ by hypothesis, so $t_1 \leq t_2$ and either the equality hold or not we have $\sigma \in G_{t_1}$ but $\sigma \notin G_{t_1+1}$. Since $\mathrm{ord}_M^\times(\mu) = 1$ and $\mathrm{ord}_M^\times(\pi) = p$ we may write $x^p = 1 + \pi^{pi'}\mu u$ where $u \in \mathscr{O}_M^\times$. Then

$$\left(\beta^p - 1\right) x^p = \sigma(x)^p - x^p = \pi^{pi'}(\sigma - 1) \cdot (\mu u).$$

So by (4.2):

$$\begin{aligned} \mathrm{ord}_M^\times\left(\beta^p\right) &= {}^4\,\mathrm{ord}_M((\beta^p - 1)x^p) \\ &= \mathrm{ord}_M(\pi^{pi'}) + \mathrm{ord}_M(\mu u) + t_{M/K} = p^2 i' + pj. \end{aligned}$$

.

In particular, we have $\mathrm{ord}_M^\times\left(\beta^p\right) \leq p^2 e' = p\,\mathrm{ord}_M^\times(\zeta)$. Using Proposition 4.1.3, we therefore have $\mathrm{ord}_M^\times(\beta) = p^{-1}\,\mathrm{ord}_M^\times\left(\beta^p\right) = pi' + j$.

□

Example 4.4.5. Let us assume to be in the setting of Example 4.2.3. In this case we are in the hypothesis of Lemma 4.4.4 so we can explicitly find $z \in M = \mathbb{Q}_3(\zeta_9)$, $x \in L = \mathbb{Q}_3(\zeta_{27})$ and $\beta \in M$.
The value of z had already been determined in Example 4.3.13, while as x we can take ζ_{27}. Indeed, $\tau(\zeta_{27}) = \zeta_{27}^{4^3} = \zeta_{27}^{64} = \zeta_{27}^{10} = \zeta_3\zeta_{27}$, $\zeta_{27}^3 = \zeta_9 \in M$ and $\mathrm{ord}_M^\times(\zeta_9) = 1$. Finally, we compute β:

$$\sigma(\zeta_{27}) = \zeta_{27}^4 = \zeta_9\zeta_{27},$$

so $\beta = \zeta_9$.

Example 4.4.6. Let us assume to be in the setting of Example 4.2.4. We are in the hypothesis of Lemma 4.4.4 so we can explicitly find $z \in M = \mathbb{Q}_2(\zeta_4)$, $x \in L = \mathbb{Q}_2(\zeta_4, \sqrt{2})$ and $\beta \in M$. The value of z is ζ_4 but the value of x can't be $\sqrt{2}$ since it is not a unity. So we take $x = \frac{1+\zeta_4}{\sqrt{2}}$. Now we find β:

$$a\left(\frac{1+\zeta_4}{\sqrt{2}}\right) = \frac{1-\zeta_4}{\sqrt{2}} = -\zeta_4 \cdot \frac{1+\zeta_4}{\sqrt{2}},$$

then $\beta = -\zeta_4$.

We have seen in Theorem 4.3.12 that if $\mathfrak{O}$ is a Hopf order in one of the Hopf algebras $H_{T,d}$, and $\mathfrak{O}$ fits into the short exact sequence $\mathfrak{O}_i \hookrightarrow \mathfrak{O} \twoheadrightarrow \mathfrak{O}_j$, then $\mathfrak{O} = \mathfrak{S}_v$ for some parameter v. Our next task is to determine, in function of v and β, when $\mathscr{O}_L$ is $\mathfrak{S}_v$-Galois:

[4] Remember that x^p is in $\mathscr{O}_M^\times$ so doesn't change the valuation

Proposition 4.4.7. *Let L/K be a totally ramified normal extension of degree p^2, let $H = H_{T,d}$ be one of the Hopf algebras giving a Hopf-Galois structure to L/K, and suppose that $t_{M/K} = pj-1$, $t_{L/M} = p^2 i - 1$ with $j \leq pi$, where $M = L^T$. Then:*

$$\mathcal{O}_L \text{ is } \mathfrak{S}_\nu\text{-Galois if and only if } \nu\beta \equiv 1 \left(\mathrm{mod}\, \pi^{i'+j}\mathcal{O}_M\right).$$

Proof. Theorem 4.1.13 and the given ramification numbers ensure that $\mathcal{O}_L$ is $\mathfrak{O}_i \otimes_{\mathcal{O}_K} \mathcal{O}_M$-Galois over $\mathcal{O}_M$, and $\mathcal{O}_M$ is $\mathfrak{O}_j$-Galois over $\mathcal{O}_K$. Thus by Lemma 4.3.7, $\mathcal{O}_L$ will be $\mathfrak{S}_\nu$-Galois if and only if $\mathcal{O}_L$ admits the action of $\mathfrak{S}_\nu$. Now we introduce a $\mathcal{O}_L$-submodule of $\mathfrak{S}_\nu$ such that as a ring it generates the whole algebra:

$$\mathfrak{M} = \mathcal{O}_K\left[\pi^{-i}(\rho-1)\right] + \mathcal{O}_K\left[\pi^{-i}(\rho-1)\right]\pi^{-j}\left(a_\nu\eta - 1\right).$$

Then $\mathfrak{M}$ is a free $\mathcal{O}_K$-direct summand in the free $\mathcal{O}_K$-module $\mathfrak{S}_\nu$.

By definition of $\mathfrak{M}$: $\mathcal{O}_L$ will admit an action of $\mathfrak{S}_\nu$ if it admits one of $\mathfrak{M}$. Moreover, L is an H-module algebra so since $\mathcal{O}_L = \mathcal{O}_K[\nu]$ with ν as in Lemma 4.4.4, we only have to check that:

$$c \cdot \nu \in \mathcal{O}_L \quad \text{for all } c \in \mathfrak{M}.$$

After the previous simplification we start looking at the action, using remark 2.2.6 we calculate:

$$\pi^{-i}(\rho-1)\cdot\nu = \pi^{-e'}(\tau(x)-x) = \pi^{-e'}(\zeta-1)x \in \mathcal{O}_K + \mathcal{O}_K\nu.$$

As $c \cdot r = \varepsilon(c)r \in \mathcal{O}_K$ for all $r \in \mathcal{O}_K$, it follows that $\mathcal{O}_K + \mathcal{O}_K\nu$ is stable under the action of $\mathcal{O}_K\left[\pi^{-i}(\rho-1)\right]$. Finally we deduce the last simplification: $\mathcal{O}_L$ admits an action of $\mathfrak{S}_\nu$ if and only if $\pi^{-j}\left(a_\nu\eta - 1\right)\cdot\nu \in \mathcal{O}_L$.
Using how the action work, see 2.2.6, we have that $(a_\nu\eta)\cdot(mx) = \nu\sigma(mx)$ for any $m \in M$. Using this remark we find:

$$\begin{aligned}
\pi^{-j}\left(a_\nu\eta - 1\right)\cdot\nu &= \pi^{-i'-j}\left(a_\nu\eta - 1\right)\cdot(x-1) \\
&= \pi^{-i'-j}\left(a_\nu\eta\cdot x - x\right) \\
&= \pi^{-i'-j}(\nu\sigma(x) - x) \\
&= \pi^{-i'-j}(\nu\beta - 1)x,
\end{aligned}$$

and this last expression lies in $\mathcal{O}_L$ if and only if $\mathrm{ord}_K(\pi^{-i'-j}(\nu\beta-1)x) \geq 0$ if and only if $\nu\beta \equiv 1\left(\mathrm{mod}\,\pi^{i'+j}\mathcal{O}_M\right)$, since $x \in \mathcal{O}_L^\times$. □

Now using Proposition 4.4.7 we can understand which Hopf Galois structure on L/K induces a Hopf Galois structure on $\mathcal{O}_L$ in our examples:

Example 4.4.8. As we have seen in Example 4.4.5 we have $\beta = \zeta_9$. Now using Proposition 4.4.7 we can understand which Hopf Galois structure on L/K induces a Hopf Galois structure on $\mathscr{O}_L$. The element v has to solve:

$$v\zeta_9 \equiv 1 \pmod{(\zeta_3 - 1)\mathscr{O}_M},$$

then we must have $v = \zeta_9^2$ and consequentially $d = 1$.

Example 4.4.9. As we have seen in Example 4.4.6 we have $\beta = -\zeta_4$. The element v has to solve:

$$v \cdot -\zeta_4 \equiv 1 \pmod{(2\mathscr{O}_M},$$

then we must have $v = \zeta_4$ and consequentially $d = 1$.

Thanks to examples 4.4.8 and 4.4.9, we found two extensions, one cyclic and one elementary abelian, such that $\mathscr{O}_L$ is not Hopf Galois on the classical structures but it is on a non-classic one.

4.5 Realizing

In this section we study some propriety of realizability. We are interest in which of the the Hopf orders $\mathfrak{S}_v$ of Theorem 4.3.12 are realizable in the sense that there is an extension L/K such that $\mathscr{O}_L$ is $\mathfrak{S}_v$-Galois. With the same meaning we are also interest in condition on i, j and d.

4.5.1 Which Hopf order is feasible?

Firstly we focus on the feasibility of the Hopf order $\mathfrak{S}_v$. As done before the idea is to find some necessary condition on v. In this regard it is useful the Proposition 4.4.7, that has the following as an easy corollary:

Corollary 4.5.1. *Let $\mathscr{O}_L$ be $\mathfrak{S}_v$-Galois. Then:*

$$\mathrm{ord}_M^\times(v) = \mathrm{ord}_K^\times\left(v^p\right) = pi' + j.$$

Proof. From Lemma 4.4.2 we have $j \leq pi$ and Lemma 4.4.4 gives us:

$$\mathrm{ord}_M^\times(\beta) = pi' + j \leq pe' = e'_M.$$

Thus $\mathrm{ord}_M^\times(\beta) < p\left(i' + j\right) \leq \mathrm{ord}_M^\times(v\beta)$ where the last inequality hold using the Proposition 4.4.7. Then from (4.1) we have that $\mathrm{ord}_M^\times(v) = \mathrm{ord}_M^\times(\beta) = pi' + j$ otherwise the order of the product $v\beta$ coincide with the minimum and so it is impossible for it to be strictly greater than the order of β.

We now consider v^p. If $\mathrm{ord}_M^\times(v) < pe'$, then by Proposition 4.1.3, $\mathrm{ord}_M^\times(v^p) = p\,\mathrm{ord}_M^\times(v)$ and hence $\mathrm{ord}_K^\times(v^p) = \mathrm{ord}_M^\times(v)$. On the other hand, if $\mathrm{ord}_M^\times(v) = pe'$ then

$j = pi > i$, so that $i' + j > e'$. Thus $\operatorname{ord}_M^\times(v\beta) \geq p\left(i' + j\right) > pe'$, and by Proposition 4.1.3:

$$\operatorname{ord}_M^\times\left(v^p\beta^p\right) = \operatorname{ord}_M^\times(v\beta) + \operatorname{ord}_M(p) > pe' + p(p-1)e' = p^2e'.$$

But from Lemma 4.4.4 we know that $\operatorname{ord}_M^\times\left(\beta^p\right) = p^2i' + pj = p^2e'$, so that again $\operatorname{ord}_K^\times(v^p) = p^{-1}\operatorname{ord}_M^\times\left(\beta^p\right) = pi' + j$ □

Having established a necessary condition, we now proceed to demonstrate its sufficiency. In the case where $d \neq 0$, the field $M = K(v)$ is determined by the parameter v. Hence, assuming M and $\mathfrak{S}_v$ are given, we proceed to construct the required field L as an extension of M. The construction of L is primarily attributed to Greither [Gre92], who previously focused exclusively on the cyclic case. However, in this treatment, we consider both the cyclic and elementary abelian cases simultaneously, thanks to the representation 4.2.1.

Theorem 4.5.2. *Let M be a given extension of K, cyclic of degree p, with $t_{M/K} = pj - 1 > 0$. Let i be an integer with $j \leq pi$, and let $\mathfrak{S}_v$ be a Hopf order as in Theorem 4.3.12, where the parameter v lies in M. Then there exists a totally ramified normal extension L/K of degree p^2 such that $M \subset L$ and $\mathcal{O}_L$ is $\mathfrak{S}_v$-Galois if and only if $\operatorname{ord}_K^\times(v^p) = pi' + j$.*

Proof. The condition $\operatorname{ord}_K^\times(v^p) = pi' + j$ is necessary by Corollary 4.5.1, and since $pi' + j \leq pe'$ it implies that $\operatorname{ord}_M^\times(v) = pi' + j$.
Now we prove sufficiency. We start noticing some simple facts: by Theorem 4.3.12 the Hopf algebra $\mathfrak{S}_v$ is a Hopf order in $H = H_{T,d} \subset M[N]$, $\eta \in N$ induces an automorphism σ of M which generates $\operatorname{Gal}(M/K)$ and we have that $\sigma(v) = \zeta^{-d}v$. From Lemma 4.4.4 we know that a proper β has some condition that may respect, in particular $N_{M/K}(\beta)$ and $\operatorname{ord}^\times(\beta)$ are fixed. Proposition 4.4.7 suggest to look for a β as a product of v^{-1} and an element $\varepsilon \in U_{pj+pi',M}$. In order to understand what norm must have ε we calculate:

$$N_{M/K}(v) = \prod_{r=0}^{p-1}\sigma^r(v) = \prod_{r=0}^{p-1}\zeta^{-rd}v = \zeta^{-p(p-1)d/2}v^p$$
$$= \begin{cases} v^p & \text{if } p \text{ is odd or } d = 0, \\ -v^p & \text{if } p = 2 \text{ and } d = 1. \end{cases}$$

Next set:

$$w = \begin{cases} v^p & \text{if } N \text{ is elementary abelian} \\ \zeta v^p & \text{if } N \text{ is cyclic.} \end{cases}$$

In either case, the conditions in Theorem 4.3.12 ensure that $w \in U_{pj+i',K}$. By Proposition 4.1.11, we have

$$N_{M/K}\left(U_{pj+pi',M}\right) = U_{pj+i',K}$$

so there exists $\varepsilon \in U_{pj+pi',M}$ with $N_{M/K}(\varepsilon) = w$. Now ε has all the necessary condition that we are looking for, so let $\beta = \varepsilon v^{-1}$. Then $N_{M/K}(\beta) = wN_{M/K}(v)^{-1}$. Thus if p is odd or $d = 0$ then:

$$N_{M/K}(\beta) = \begin{cases} 1 & \text{if } N \text{ is elementary abelian,} \\ \zeta & \text{if } N \text{ is cyclic,} \end{cases}$$

while if $p = 2$ and $d = 1$ we have $\zeta = -1$ and the two cases above are reversed. In all cases, $N_{M/K}\left(\beta^p\right) = 1$, and since the order of ε is strictly greater then the one of v from (4.1) we have:

$$\mathrm{ord}_M^\times(\beta) = \mathrm{ord}_M^\times(v) = pi' + j \leq pe'.$$

As $\mathrm{ord}_K^\times(v^p) = pi' + j$ by hypothesis, we can act as in Corollary 4.5.1, this time with the role of v and β reversed, in order to obtain:

$$\mathrm{ord}_M^\times\left(\beta^p\right) = p\,\mathrm{ord}_M^\times(\beta) = p^2 i' + pj \geq pj = t_{M/K} + 1.$$

Hence β^p realize the hypothesis of Proposition 4.1.11 that give us an $y \in \mathcal{O}_M^\times$ such that $\sigma(y)/y = \beta^p$. Multiplying y by an element of $\mathcal{O}_K^\times$, we may assume that $\mathrm{ord}_M^\times(y)$ is not divisible by p. Then by (4.2):

$$p^2 i' + pj = \mathrm{ord}_M^\times(\sigma(y)/y) = \mathrm{ord}_M^\times(y) + t_{M/K},$$

so $\mathrm{ord}_M^\times(y) = p^2 i' + 1$.

Now let $L = M(x)$ with $x^p = y$. Then L/M is normal of degree p and[5] $t_{L/M} = p^2 i - 1$. Since $\sigma(x^p) = (\beta x)^p$, we may extend σ to an automorphism of L (which we again denote by σ) with $\sigma(x) = \beta x$. As $\beta^p \neq 1$ it follows that the group of K-automorphisms of L is strictly larger than $\mathrm{Gal}(L/M)$, and hence that L/K is a normal extension of degree p^2.

We next verify that $G = \mathrm{Gal}(L/K)$ has the correct isomorphism type, as given by Theorem 4.2.1. By equation (4.14): $\sigma^p(x) = N_{M/K}(\beta)x$. For odd p with N elementary abelian (and for $p = 2$, with either $d = 0$, N elementary abelian or $d = 1$, N cyclic) we have $N_{M/K}(\beta) = 1$, so that $\sigma^p = 1$. This shows that G is elementary abelian of order p^2, generated by σ and the subgroup $\mathrm{Gal}(L/M)$ of order p. In the remaining cases, $N_{M/K}(\beta) = \zeta$, so $\sigma^p \neq 1$ and G is cyclic of order p^2, generated by σ.

It now follows from Theorem 4.2.1 that H induces a Hopf-Galois structure on L/K. Since by construction $v\beta = \varepsilon \equiv 1 \left(\mathrm{mod}\, \pi^{i'+j}\mathcal{O}_M\right)$, Proposition 4.4.7 shows that $\mathcal{O}_L$ is $\mathfrak{S}_v$-Galois, as required. □

[5] It comes from the fact that it is an Kummer extension and the valuation of $y - 1$ is known.

4.5.2 Which i, j and d are achievable?

We next determine the values of i, j and d for which there exists a Hopf order $\mathfrak{S}_v$ of $H_{T,d}$ some some T that fits in 4.9 and an extension L/K such that $\mathcal{O}_L$ that fits $\mathfrak{S}_v$-Galois. As done for the feasibility of the Hopf order $\mathfrak{O}_v$ we start by proving a theorem that give some necessary condition and then we prove that all the case that appear in the theorem can occur. The second part is constructive so sometimes we may also assume extra hypotheses to simplify the process.

Theorem 4.5.3. *Let L be a totally ramified normal extension of K of degree p^2, with ramification numbers $t_1 = pj - 1 \leq t_2 = p^2 i - 1$. Let $\mathfrak{S}_v$ be a Hopf order in $H = H_{T,d}$ as in Theorem 4.3.12. If $\mathcal{O}_L$ is $\mathfrak{S}_v$-Galois then one of the following holds:*

(i) [Region A]: $pj \leq i, i + j \leq e'$, *and* $p \mid j$;

(ii) [Region B]: $pj > i, i + j \leq e', (p+1)j < pi + 1$, *and* $p \mid j$;

(iii) [Region C]: $(p+1)j > pi + 1, j \leq pi, p \mid j$, *and* $d = 0$;

(iv) [Line segment L]: $(p+1)j = pi + 1, i + j \leq e', j \equiv 1 (\mathrm{mod}\ p)$, *and* $d \neq 0$

(v) [Line segment M]: $pi' = j', e'/(p+1) < j < \left[(p-1)e' + 1\right]/p$, *and* $p \mid j$

(vi) [Line segment N]: $pi' = j', j > \left[(p-1)e' + 1\right]/p, p \mid j$, *and* $d = 0$

(vii) [Point P]: $i = \left[\left(p^2 - 1\right)e' + 1\right]/p^2, j = \left[(p-1)e' + 1\right]/p,\ j \equiv 1\ (\mathrm{mod}\ \ p)$, *and* $d \neq 0$.

In case (i), $\mathfrak{S}_v$ is either of elementary abelian type or is a Greither order. In cases (ii)-(iv), $\mathfrak{S}_v$ is of elementary abelian type. In cases (v)-(vii), $\mathfrak{S}_v$ is a dual Greither order.

Proof. By Lemma 4.4.2, $j \leq pi$ and $v = cz^{-d}$, where $c \in \mathcal{O}_K^\times$ and where z generates the intermediate field $M = L^T = K(z)$ and satisfies $\mathrm{ord}_M^\times(z) = pj' + 1$. Moreover, we have $\mathrm{ord}_M^\times(v) = \mathrm{ord}_K^\times(v^p) = pi' + j$ by Corollary 4.5.1.

Claim: either $i + j \leq e'$ or $\mathfrak{S}_v$ is a dual Greither order with $pi' = j'$.
For this we consider the three cases in Theorem 4.3.12. If N is elementary abelian then $\mathrm{ord}_K^\times(v^p) \geq pj + i'$ by (4.10), so we have $pi' + j \geq pj + i'$, which simplifies to $i + j \leq e'$. If $\mathfrak{S}_v$ is a Greither order then automatically $i + j \leq e'$ by Convention 4.3.17. Finally, if $\mathfrak{S}_v$ is a dual Greither order then $i + j > e'$ and $pi' \leq j'$, and it remains to show that in fact $pi' = j'$. Suppose for a contradiction that $pi' < j'$. Then $\mathrm{ord}_K^\times(v^p) = pi' + j < e' = \mathrm{ord}_K^\times(\zeta)$, and hence by propriety (4.1) also $\mathrm{ord}_K^\times(\zeta v^p) = pi' + j$. By (4.11) we therefore have $pi' + j \geq pj + i'$. This simplifies to $i + j \leq e'$, giving the required contradiction. Hence $pi' = j'$.

For the remainder of the proof, we distinguish three possibilities:

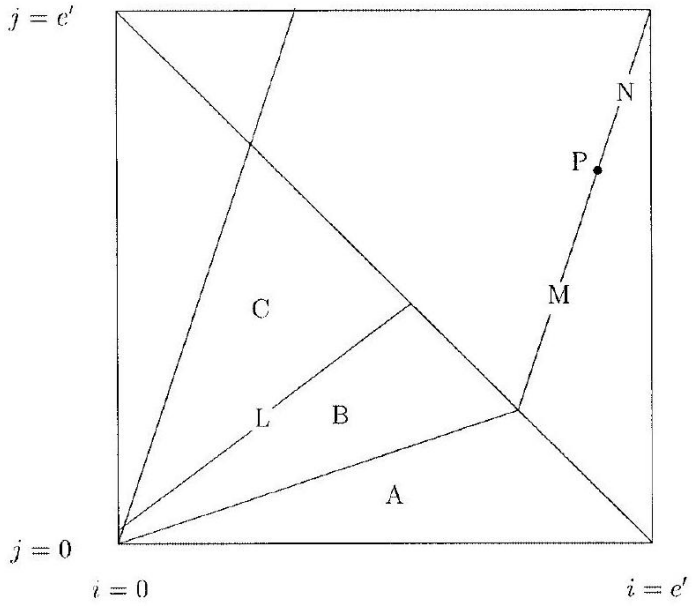


Figure 4.2: Values of (i, j) where $\mathscr{O}_L$ can be Hopf-Galois.

(a) $pj' + 1 > pi' + j$, that can be rewrite as $(p+1)j < pi + 1$. This inequality is certainly implied by $pj \le i$. Then for Proposition 4.5.1 the initial inequality can be written as $\mathrm{ord}^{\times}(z) > \mathrm{ord}_M^{\times}(v)$. Using that $v = cz^{-d}$ and the usual argument with the propriety (4.1), we have that

$$pi' + j = \mathrm{ord}_M^{\times}(v) = \mathrm{ord}_M^{\times}(c) = p\,\mathrm{ord}_K^{\times}(c),$$

where for the last equality we used that $c \in \mathscr{O}_K^{\times}$ and M/K is totally ramified. Hence $p \mid j$. If $i + j \le e'$ then for the convention $\mathfrak{S}_v$ cannot be a dual Greither order, then if N is cyclic $\mathfrak{S}_v$ has to be a Greither order. This gives cases (i) and (ii) since for what we have noticed by Theorem 4.3.12 the cyclic case imply $pj \le i$. If $i + j > e'$ then $\mathfrak{S}_v$ is a dual Greither order and $pi' = j'$, giving case (v).

(b) $pj' + 1 < pi' + j$, that can be rewrite as $(p+1)j > pi + 1$. Notice that since $\mathrm{ord}_M^{\times}(z) \equiv 1 \pmod{p}$ and $c \in K$, we cannot have the equality $\mathrm{ord}_M^{\times}(c) = \mathrm{ord}_M^{\times}(z)$. Thanks to propriety (4.1) and $v = cz^{-d}$ this imply that $\mathrm{ord}_M^{\times}(v) = \min(\mathrm{ord}_M^{\times}(z), \mathrm{ord}_M^{\times}(c))$. Again, as in (a), for Proposition 4.5.1 the initial inequality can be written as $\mathrm{ord}_M^{\times}(z) < \mathrm{ord}_M^{\times}(v) = \min(\mathrm{ord}_M^{\times}(z), \mathrm{ord}_M^{\times}(c))$ then we must have $d = 0$ and then $v = c \in \mathscr{O}_K^{\times}$. As $\mathrm{ord}_M^{\times}(v) = pi' + j$, this implies that $p \mid j$. If $i + j \le e'$ this gives case (iii), while if $i + j > e'$ then $\mathfrak{S}_v$ is a dual Greither order with $pi' = j'$, giving case (vi).

(c) $pj' + 1 = pi' + j$, that can be rewrite as $(p+1)j = pi + 1$. Using arguments similar to cases (a) and (b) we have $\mathrm{ord}_M^\times(v) = \mathrm{ord}_M^\times(z) \equiv 1 (\mathrm{mod}\, p)$ so that $j \equiv 1 \pmod{p}$. As $v = cz^{-d}$ with $\mathrm{ord}_M^\times(c) \equiv 0 \pmod{p}$, it follows that $\mathrm{ord}_K^\times(c) > \mathrm{ord}_M^\times(v)$ and $d \neq 0$. If $i + j \leq e'$ we have case (iv), and if $i + j > e'$ then $\mathfrak{S}_v$ is a dual Greither order with $pi' = j'$, giving case (vii).

□

Now we investigate the possible case depending on the the type of extension (cyclic or elementary abelian):

Remark 4.5.4. We distinguish two case:
Odd p: If L/K is cyclic, all the Hopf orders involved will either be Greither orders or dual Greither orders, which implies that points in regions B or C, as well as on line segment L, cannot occur. Similarly, points on line segments M and N, along with the point P, cannot occur when L/K is elementary abelian.
$p = 2$: If L/K is cyclic, points in region C cannot occur since, if $d = 0$, $\mathfrak{S}_v$ must be either a Greither order or a dual Greither order. However, points in region B are possible since here we can have $d = 1$ so that the Hopf order is of elementary abelian type. Similar considerations demonstrate that point P cannot occur for L/K cyclic, and points on the line segments L and N cannot occur for L/K elementary abelian.

As a consequence we recover the Corollary 3.4 of [Chi96]:

Remark 4.5.5. If p is odd, L/K is cyclic, and $0 < pj \leq i$, then only case (i) of Theorem 4.5.3 can arise. So under this hypothesis $p \mid j$ and the relevant Hopf orders here are always Greither orders.

Now we want to check that all the possibilities list in the Theorem 4.5.3 can occur. In order to do that can be useful to add some hypothesis to make it easier to create some appropriate field extension using the Theorem 4.5.2:

Lemma 4.5.6. *Let i, j, d be given with $1 \leq i, j \leq e'$ and $0 \leq d \leq p-1$, satisfying one of the conditions (i)–(vii) of Theorem 4.5.3. In some cases we add some hypotheses: In cases (v)–(vii), suppose that K contains a primitive p^2th-root of unity, ϕ and in case (v), assume also that $d = 0$.*
Then there exists a Hopf order $\mathfrak{S}_v$ as in Theorem 4.3.12, with the given parameters i, j, d, and a normal extension L of K such that $\mathcal{O}_L$ is $\mathfrak{S}_v$-Galois. Moreover except for case (vii) L may be chosen to contain a given normal extension M of K of degree p such that $t_{M/K} = pj - 1$, and any generator $\mathrm{Gal}(M/K)$ may be chosen as σ in Theorem 4.3.12.

Proof. As usual let $M = K(z)$, where z is chosen so that $\mathrm{ord}_M^\times(z) = pj' + 1$ and $\sigma(z) = \zeta z$. In cases (v)-(vii), we may assume that ϕ is chosen so that $\phi^p = \zeta$. The general idea is to create a $v \in M$ that respect the hypothesis of Theorem 4.5.2. Again we distinguish several possibilities:

(a) Cases (i)-(iii). Here $p \mid j$, and by Proposition 4.1.3 we can find $c \in \mathcal{O}_K^\times$ with $\mathrm{ord}_K^\times(c) = i' + (j/p) \le e'$ and $\mathrm{ord}_K^\times(c^p) = pi' + j$. Set $v = cz^{-d}$. Since $\mathrm{ord}_M^\times(z) > \mathrm{ord}_M^\times(c)$ in cases (i) and (ii), and $d = 0$ in case (iii), we have $\mathrm{ord}_K^\times(v^p) = \mathrm{ord}_K^\times(c^p) = pi' + j$. Since $i + j \le e'$ we have that $pi' + j \ge pj + i'$, indeed $pi' + j - pj - i' = (p-1)(e' - i - j) \ge 0$. Then (4.10) holds. Thus in case (ii) and (iii), that occur only for elementary abelian extension, we have a Hopf order $\mathfrak{S}_v$ of elementary abelian type satisfying the condition of Theorem 4.5.2, which gives the existence of L as stated. Moreover, in case (i), v satisfies (4.11), so we obtain a Greither order (or a elementary abelian order depending on the extension type) $\mathfrak{S}_v$ and a corresponding field L.

(b) Case (iv). Take $v = z^{-d}$. Since $d \neq 0$ we have[6] $\mathrm{ord}_M^\times(v) = \mathrm{ord}_M^\times(z) = pi' + j$, so that again v satisfies (4.10). As above, Theorem 4.5.2 completes the proof.

(c) Cases (v), (vi). Here $d = 0$ and $pi' + j = e'$. Take $v = \phi^{-1} \in K$. Then $v^p = \zeta^{-1}$ and $\zeta v^p = 1$. Hence $\mathrm{ord}_K^\times(v^p) = pi' + j$ and (4.11) is satisfied. We therefore have a dual Greither order $\mathfrak{S}_v$, and Theorem 4.5.2 yields a suitable field L.

(d) Case (vii). In this case we take $M = K(\phi)$. For i, j to be integral we require $e' \equiv 1 \pmod{p^2}$. In particular e' is not divisible by p, so M is a totally ramified extension of K of degree p. (Recall that we always assume $\zeta \in K$.) Since by hypothesis $pj' + 1 = e' = \mathrm{ord}_K^\times(\zeta)$, we have $\mathrm{ord}_M^\times(\phi) = pj' + 1$, whence[7] $t_{M/K} = pj - 1$. We make a specific choice of σ depending on the given d; namely, we take $\sigma \in \mathrm{Gal}(M/K)$ such that $\sigma(\phi) = \zeta^d \phi$. We then set $z = \phi^f$ and $v = z^{-d}$, where $fd \equiv 1 \pmod{p}$. Thus $\sigma(z) = \zeta z$, $v^p = \zeta^{-1}$, and $\zeta v^p = 1$. We then obtain $\mathfrak{S}_v$ and L as in (c).

□

4.6 Final classification

In this final section, we address a fundamental question:

Suppose we have a totally ramified, normal extension L of K with a degree of p^2, and $\mathcal{O}_L$ is Hopf-Galois in one of the Hopf-Galois structures on L/K. What occurs in the other Hopf-Galois structures on L/K?

If L/K possesses a unique ramification number, then we have $j = pi$. Under this assumption, the only case from Theorem 4.5.3 that aligns with the given values of i and j is case (iii). However, this case implies that $d = 0$, resulting in the classical Hopf-Galois structure as the only possibility for $\mathcal{O}_L$ to be Hopf-Galois.

[6] Notice that under the hypothesis of (iv) we have that $pj' + 1 = pi' + j$.

[7] We are using the connection between the order of the generator and the ramification break that occur in Kummer extension.

On the other hand, when L/K features two distinct ramification numbers, Lemma 4.4.2 tell us that $\mathcal{O}_L$ can only be Hopf-Galois with respect to a Hopf algebra $H = H_{T,d}$ where $T = G_{t_2}$. Consequently, we can consider T as fixed, and our focus shifts to examining the effect of altering the parameter d. The subsequent lemma describes, in terms of i and j, the conditions under which a change in d still define a Hopf-Galois structure for L/K such that $\mathcal{O}_L$ is Galois:

Lemma 4.6.1. *Let $\mathcal{O}_L$ be Hopf-Galois with respect to $H_{T,d}$. We assume L/K is totally ramified, with ramification numbers $t_1 = pj-1$ and $t_2 = p^2 i - 1$, where $j \le pi$.*

(i) If $i \ge 2j$, then $\mathcal{O}_L$ is Hopf-Galois with respect to $H_{T,d'}$ for all $d' \in 0, 1, \dots, p-1$. Thus, $\mathcal{O}_L$ is Hopf-Galois with respect to exactly p of the Hopf-Galois structures on L/K.

(ii) If $i < 2j$, then $\mathcal{O}_L$ is Hopf-Galois with respect to a unique Hopf-Galois structure on L/K.

Proof. We have that $\mathcal{O}_L$ is $\mathfrak{S}_v$-Galois for some Hopf order $\mathfrak{S}_v$ in $H_{T,d}$, where the parameter v satisfies $\mathrm{ord}_M^\times(v) = pi'+j$, $v = z^{-d}c$ with $c \in \mathcal{O}_K^\times$, and $v\beta \equiv 1 \left(\mathrm{mod}\ \pi^{i'+j}\mathcal{O}_M\right)$. Here β is as in Lemma 4.4.4 and does not depend on d. We first note that

$$\begin{aligned} z \equiv 1 \pmod{\pi^{i'+j}\mathcal{O}_M} &\Leftrightarrow \mathrm{ord}_M^\times(z) \ge p\left(i'+j\right) \\ &\Leftrightarrow pj'+1 \ge p\left(i'+j\right) \\ &\Leftrightarrow {}^{8}\, j' \ge i'+j \\ &\Leftrightarrow e'-j \ge e'-i+j \\ &\Leftrightarrow i \ge 2j. \end{aligned}$$

If $i \ge 2j$ we may therefore replace $v = z^{-d}c$ by $\tilde{v} = z^{-\tilde{d}}c$ for any $\tilde{d} \in \{0, 1, \dots, p-1\}$. We then have $\tilde{v} \equiv v (\mathrm{mod} \pi^{i'+j}\mathcal{O}_M)$ and hence $\tilde{v}\beta \equiv 1 \pmod{\pi^{i'+j}\mathcal{O}_M}$. Thus $\mathcal{O}_L$ will be $\mathfrak{S}_{\tilde{v}}$-Galois, provided that $\mathfrak{S}_{\tilde{v}}$ is indeed a Hopf order in $H_{T,\tilde{d}}$. But v satisfies one of the conditions (4.10) and (4.11), and $\mathfrak{S}_{\tilde{v}}$ will be a Hopf order if $\tilde{v}$ satisfies the same condition. Thus it suffices to verify that $z^p \in U_{pi'+j,K} \cap U_{pj+i',K}$. As $i \ge 2j$ we have $pi+1 \ge 2pj+1 > (p+1)j$, so that $\mathrm{ord}_K^\times(z^p) = pj'+1 > pi'+j$, and $2pj - i \le (p-1)i < (p-1)e'+1$, so that $pj'+1 > pj+i'$, as required.

Now suppose $i < 2j$. If $\mathcal{O}_L$ is Hopf-Galois with respect to $H_{T,\tilde{d}}$ then $\mathcal{O}_L$ is $\mathfrak{S}_{\tilde{v}}$-Galois for some $\tilde{v} = z^{-\tilde{d}}\tilde{c}$ with $\tilde{c} \in \mathcal{O}_K^\times$. We therefore have $\tilde{v}\beta \equiv 1 \equiv v\beta \pmod{\pi^{i'+j}\mathcal{O}_M}$. Thus $\tilde{v} \equiv v \pmod{\pi^{i'+j}\mathcal{O}_M}$, so $z^{d-\tilde{d}} \equiv \tilde{c}c^{-1} \pmod{\pi^{i'+j}\mathcal{O}_M}$. If $\tilde{d} \ne d$, it follows that $\mathrm{ord}_M^\times(\tilde{c}c^{-1}) = \mathrm{ord}_M^\times(z) = pj'+1 \not\equiv 0 \pmod{p}$, contradicting $\tilde{c}c^{-1} \in K$. Hence we must have $\tilde{d} = d$. Thus $\mathcal{O}_L$ is Hopf-Galois with respect to only one Hopf-Galois structure. □

We can interpret Lemma 4.6.1 in terms of Fig. 4.2 as follows:

[8] Because, in the equation above, the left side can't be divisible by p so the inequality is strict.

Remark 4.6.2.

- Odd p: In this case the line $i = 2j$ divides the region B into two regions B_1, B_2, and the line segment M into two segments M_1, M_2, as shown in Fig. 4.3. In regions A, B_1, and on line segment M_1 (including the points on the boundary $i = 2j$), if $\mathcal{O}_L$ is Hopf-Galois, it will be Hopf-Galois with respect to exactly p of the Hopf-Galois structures. In regions B_2, C, on line segments L, M_2, N, and at point P, there can be at most one Hopf-Galois structure on L/K in which $\mathcal{O}_L$ is Hopf-Galois.

- $p = 2$: In this case, the line $i = 2j$ is already depicted in Fig. 4.2 as the boundary between regions A and B. Outside of region A, there can be at most one Hopf-Galois structure on L/K in which $\mathcal{O}_L$ is Hopf-Galois.

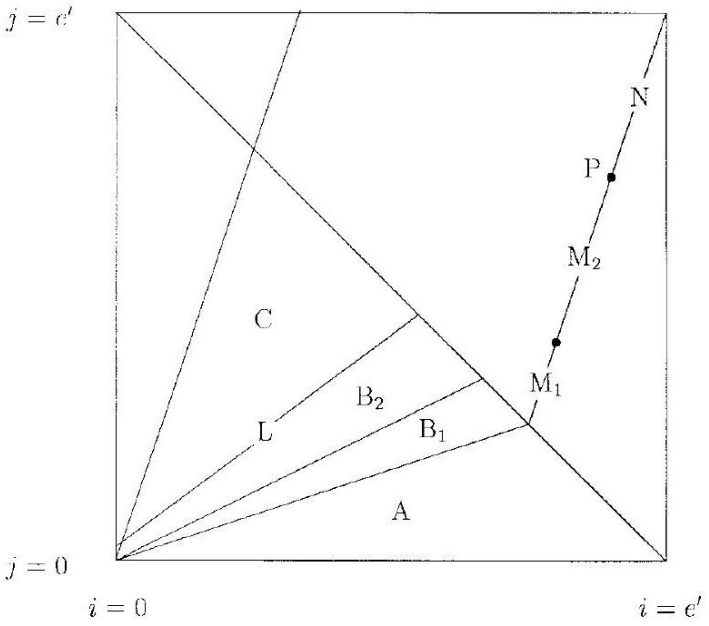


Figure 4.3: Values of (i, j) where $\mathcal{O}_L$ can be Hopf-Galois in one or in p of the Hopf-Galois structures.

By combining Lemma 4.6.1 with Theorem 4.5.3 and Remarks 4.6.2 and 4.5.4, we can provide a comprehensive answer to our question regarding the behavior of $\mathcal{O}_L$ in different Hopf-Galois structures on L/K. Depending on the values of i and j, $\mathcal{O}_L$ is Hopf-Galois in either just one or exactly p of the Hopf-Galois structures on L/K. We will now present the complete statement, taking into account the various cases: p odd, or $p = 2$ and G cyclic or G elementary abelian.
The following hypotheses and notation are assumed in each of the following theorems $A - D$:

Notation 4.6.3. *L/K is a totally ramified normal extension of degree p^2, with ramification numbers $t_1 = pj-1 \le t_2 = p^2 i - 1$ and with Galois group $G = \mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle$. We write $T = \langle \tau \rangle$ and set $G' = G_{t_2}$ if $t_1 < t_2$, taking G' to be an arbitrary subgroup of G of order p if $t_1 = t_2$.*

Theorem 4.6.4A. *Let p be odd and let L/K be cyclic. If $\mathcal{O}_L$ is Hopf-Galois with respect to some Hopf-Galois structure on L/K then one of the following holds:*

(i) [Region A] : $pj \le i, i+j \le e'$. Then $p \mid j, \mathfrak{S}_v$ is a Greither order, and $\mathcal{O}_L$ is Hopf-Galois with respect to all p Hopf-Galois structures on L/K.

(ii) [Line segment M_1]: $pi' = j', e'/(p+1) < j \le (p-1)e'/(2p-1)$. Then $p \mid j, \mathfrak{S}_v$ is a dual Greither order, and $\mathcal{O}_L$ is Hopf-Galois with respect to all p Hopf-Galois structures on L/K.

(iii) [Line segments M_2, N, point P]: $pi' = j', j > (p-1)e'/(2p-1)$. Then $\mathfrak{S}_v$ is a dual Greither order, and $\mathcal{O}_L$ is Hopf-Galois with respect to exactly one of the p Hopf-Galois structures on L/K. This Hopf-Galois structure is the classical one if $j > \left[(p-1)e'+1\right]/p$ and is one of the non classical ones if $j = \left[(p-1)e'+1\right]/p$. Moreover, $j \equiv 1 \pmod{p}$ if $j = [(p-1)e'+1]/p$ and $j \mid p$ otherwise.

Theorem 4.6.4B. *Let p be odd and let L/K be elementary abelian. If $\mathcal{O}_L$ is Hopf-Galois with respect to some Hopf-Galois structure on L/K then one of the following holds:*

(i) [Regions A, B_1] : $2j \le i, i+j \le e'$. Then $p \mid j, \mathfrak{S}_v$ is a Hopf order of elementary abelian type, and $\mathcal{O}_L$ is Hopf-Galois with respect to exactly p of the p^2 Hopf-Galois structures on L/K, namely those with $T = G'$ (including the classical one).

(ii) [Regions B_2, C, line segment L] : $2j > i, j \le pi, i+j \le e'$. Then $\mathfrak{S}_v$ is a Hopf order of elementary abelian type, and $\mathcal{O}_L$ is Hopf-Galois with respect to exactly one of the p^2 Hopf-Galois structures on L/K. If $(p+1)j > pi+1$ (respectively, $(p+1)j = pi+1$) then this is the classical Hopf-Galois structure (respectively, one of the non-classical Hopf-Galois structures). In any case, it is one of the p Hopf-Galois structures corresponding to the subgroup $T = G'$. Moreover, $j \equiv 1 \pmod{p}$ if $j = \left[(p-1)e'+1\right]/p$ and $j \mid p$ otherwise.

Theorem 4.6.4C. *Let $p = 2$ and let L/K be cyclic. If $\mathcal{O}_L$ is Hopf-Galois with respect to some Hopf-Galois structure on L/K then one of the following holds:*

(i) [Region A] : $2j \le i, i+j \le e'$. Then $2 \mid j$, and $\mathfrak{O}_L$ is Hopf-Galois with respect to both Hopf-Galois structures on L/K. In the classical Hopf-Galois structure $\mathfrak{S}_v$ is a Greither order, and in the non-classical Hopf-Galois structure $\mathfrak{S}_v$ is of elementary abelian type.

(ii) *[Region B, line segment L] :* $2j \geq i, 3j \leq 2i+1, i+j \leq e'$. *Then* $d = 1$, *so* $\mathcal{O}_L$ *is Hopf-Galois with respect to the non-classical Hopf-Galois structure but not with respect to the classical one, and* $\mathfrak{S}_v$ *is of elementary abelian type. Moreover,* j *is even unless* $3j = 2i+1$ *(in which case* j *is odd).*

(iii) *[Line segments M, N] :* $2i' = j', i+j > e'$. *Then* $d = 0$ *and* j *is even, so* $\mathfrak{S}_v$ *is a dual Greither order, and* $\mathcal{O}_L$ *is Hopf-Galois with respect to the classical Hopf-Galois structure on* L/K, *but not with respect to the non-classical one.*

Theorem 4.6.4D. *Let* $p = 2$ *and let* L/K *be elementary abelian. If* $\mathcal{O}_L$ *is Hopf-Galois with respect to some Hopf-Galois structure on* L/K *then one of the following holds:*

(i) *[Region A]:* $2j \leq i, i+j \leq e'$. *Then* $2 \mid j$ *and* $\mathcal{O}_L$ *is Hopf-Galois with respect to two of the four Hopf-Galois structures on* L/K, *namely the classical one (in which* $\mathfrak{S}_v$ *is a Hopf order of elementary abelian type) and the non-classical one with* $d = 1$ *and* $T = G'$ *(in which* $\mathfrak{S}_v$ *is a Greither order).*

(ii) *[Regions B, C]:* $2j \geq i, j \leq 2i, i+j \leq e'$. *Then* $d = 0$ *and* j *is even. Thus* $\mathfrak{S}_v$ *is of elementary abelian type and* $\mathcal{O}_L$ *is Hopf-Galois with respect to the classical Hopf-Galois structure but not with respect to any of the three non-classical ones.*

(iii) *[Line segment M, point P] :* $2i' = j', e'/3 < j \leq \left(e'+1\right)/2$. *Then* $\mathfrak{S}_v$ *is a dual Greither order, so* $d = 1$. *Thus* $\mathcal{O}_L$ *is Hopf-Galois with respect to exactly one of the four Hopf-Galois structures on* L/K, *namely the non classical one with* $d = 1$ *and* $T = G'$. *Moreover,* j *is odd if* $j = \left(e'+1\right)/3$ *(this can occur only if* $e' \equiv 2 \pmod 6\big)$, *and* j *is even otherwise.*

Bibliography

[Byo93] Nigel P Byott. Cleft extensions of hopf algebras, ii. *Proceedings of the London Mathematical Society*, 3(2):277–304, 1993.

[Byo96] Nigel P. Byott. Uniqueness of hopf galois structure for separable field extensions. *Communications in Algebra*, 24:3217–3228, 1996.

[Byo02] Nigel P. Byott. Integral hopf–galois structures on degree p2 extensions of p-adic fields. *Journal of Algebra*, 248:334–365, 2002.

[CGK+21] Lindsay N Childs, Cornelius Greither, Kevin P Keating, Alan Koch, Timothy Kohl, Paul J Truman, and Robert G Underwood. *Hopf algebras and Galois module theory*, volume 260. American Mathematical Soc., 2021.

[CH86] Lindsay N. Childs and Susan Hurley. Tameness and local normal bases for objects of finite hopf algebras. *Transactions of the American Mathematical Society*, 298(2):763–778, 1986.

[Chi87] Lindsay N. Childs. Taming wild extensions with hopf algebras. *Transactions of the American Mathematical Society*, 304:111–140, 1987.

[Chi96] Lindsay N. Childs. Hopf galois structures on degree p 2 cyclic extensions of local fields. 1996.

[Chi00] Lindsay Childs. *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory: Hopf Algebras and Local Galois Module Theory*. Number 80. American Mathematical Soc., 2000.

[CSCS69] Stephen U Chase, Moss E Sweedler, Stephen U Chase, and Moss E Sweedler. *Hopf algebras and Galois theory*. Springer, 1969.

[Gre92] C. Greither. Extensions of finite group schemes, and hopf galois theory over a complete discrete valuation ring. *Mathematische Zeitschrift*, 210(1):37–68, 1992.

[Lar76] Richard Gustavus Larson. Hopf algebra orders determined by group valuations. *Journal of Algebra*, 38(2):414–452, 1976.

[Leo59] Heinrich-Wolfgang Leopoldt. Über die hauptordnung der ganzen elemente eines abelschen zahlkörpers. *Journal für die reine und angewandte Mathematik*, 201:119–149, 1959.

[Let98] Günter Lettl. Relative galois module structure of integers of local abelian fields. *Acta Arithmetica*, 85(3):235–248, 1998.

[PG87] Bodo Pareigis and Cornelius Greither. Hopf galois theory for separable field extensions. *Journal of Algebra*, (1):239–258, 1987.

[Sch77] Hans Jürgen Schneider. Cartan matrix of liftable finite group schemes. *Communications in Algebra*, 5:795–819, 1977.

[Ser79] J.P. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer-Verlag, 1979.

[Swe69] M.E. Sweedler. *Hopf Algebras*. Mathematics lecture note series. W. A. Benjamin, 1969.

[Und15] Robert G Underwood. *Fundamentals of Hopf algebras*. Springer, 2015.