UNIVERSITAT POLITÈCNICA DE CATALUNYA

DOCTORAL THESIS

An effective method to study the Hopf Galois module structure of certain extensions of fields

Author:
Daniel Gil-Muñoz

Supervisors:
Anna Rio
Teresa Crespo

A thesis submitted in fulfillment of the requirements for the degree of

Doctor in Mathematics

May 7, 2021

Declaration of Authorship

I, Daniel Gil-Muñoz, declare that this thesis titled, “An effective method to study the Hopf Galois module structure of certain extensions of fields” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date: Barcelona, May 7th 2021

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Abstract

Doctor in Mathematics

An effective method to study the Hopf Galois module structure of certain extensions of fields

by Daniel Gil-Muñoz

We develop a method to compute a basis of the associated order $\mathfrak{A}_H$ in a Hopf Galois structure H of the ring of integers $\mathcal{O}_L$ of an extension of number or p-adic fields L/K. We state and prove a necessary and sufficient condition for a given element $\beta \in \mathcal{O}_L$ to be a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module. Whenever it exists, one can use such a free generator and a basis of $\mathfrak{A}_H$ to build a basis which can be seen as an analog of the normal integral basis in the Galois case. We use this method to determine the associated order and the existence of normal integral basis generators for different classes of extensions of fields, such as Galois extensions of degrees 2, 3 and 4, and separable degree p extensions of $\mathbb{Q}_p$ with normal closure having Galois group isomorphic to the dihedral group D_p of $2p$ elements. We shall use the theory of induced Hopf Galois structures to study the same problem for the normal closure itself, i.e. a dihedral degree $2p$ extension of $\mathbb{Q}_p$. We give complete answers for the cases $p = 3$ and $p = 5$.

Acknowledgements

Son muchas las personas a las que debo el haber llegado hasta aquí.

Quiero dar las gracias, en primer lugar, a Anna Rio, mi directora de tesis, por su tiempo y su dedicación durante estos años, por la propuesta del tema, y sobre todo por su ayuda tanto en lo académico como en el resto de los aspectos que supone hacer un doctorado. Especiales agradecimientos también a mi otra directora de tesis, Teresa Crespo, por su disponibilidad y por sus útiles comentarios y consejos que me han servido para mejorar esta tesis y de los que he aprendido enormemente.

Doy las gracias también a María de los Ángeles Gómez Molleda, mi tutora del trabajo de fin de grado, por introducirme en el fascinante mundo de la teoría de números, por orientarme en mi carrera académica, y por sus consejos y ánimos durante este periodo. También a Xavier Guitart, mi tutor del trabajo final de máster, por sus directrices a la hora de hacer y escribir matemáticas, y que me han sido de una ayuda inestimable en este y otros trabajos.

Gracias a mis compañeros de piso durante más tiempo en este periodo, Dan Paraschiv y Gladston Duarte, por la cercanía y la estabilidad. Gracias a mis compañeros doctorandos en teoría de números: Óscar Rivero, Francesca Gatti, Armando Gutiérrez, Guillem Sala y Víctor Hernández, cuya compañía ha coloreado mis días. También a mis compañeros organizadores del Seminario Informal de Matemáticas de Barcelona (SIMBa): Sergi Baena, Carlos Cruz, Enric Florit, Andriana Karuk, Ignasi Sánchez, Damià Torres, David Martínez, Ainoa Murillo, Salvador Borrós, Clara Cufí, Eduard Vilalta y Pau Mir, así como a los antiguos: Andrés Rojas, Liena Colarte, Martí Salat y Camilo Torres, por esta gran experiencia matemática.

También quiero agradecer al grupo de teoría de números de Barcelona por hacerme sentir parte de esta gran familia: Montse Vela, Jordi Quer, Joan Carles Lario, Victor Rotger, Santiago Molina, Edu Soto, Francesc Fité, Pilar Bayer, Jordi Guardia, Artur Travesa, Nuria Vila, y muchos otros. Gracias a mis amigos de los congresos en teoría de números: Marta Salguero, Jose Granados y Carlos Pastor.

I want to thank wholeheartedly Nigel Byott for his dedication during my three-month stay in Exeter and for making his best so that I could feel comfortable there. I am really grateful to him for his useful and intelligent comments on the contents of this thesis, and his papers and contributions, from which I have learned a lot. Thanks also to Lindsay Childs for his time reading my thesis and his helpful comments, as well as his wonderful book on Hopf Galois theory, which has been my main guide in my first months of thesis. I want to thank also the participants of the Galois and Hopf Galois conferences and work groups: Paul Truman, Alan Koch, Robert Underwood, Griffith Elder, Timothy Kohl, Henri Johnston, Fabio Ferri, Ilaria del Corso, Lorenzo Stefanello, and many others.

Y para terminar, como no podía ser de otra forma, quiero dar las gracias a mis padres, Cristóbal y Francisca, y a mi hermana Marina, por ser el sostén de mi vida, y a quienes debo ser la persona que soy hoy.

Barcelona, 7 de mayo de 2021.

Contents

Declaration of Authorship iii

Abstract vii

Acknowledgements ix

Introduction 1

1 Preliminaries 5
- 1.1 Hopf algebras 5
- 1.2 Hopf Galois structures 8
- 1.3 Greither-Pareigis theory 9
  - 1.3.1 The Greither-Pareigis theorem 9
  - 1.3.2 Consequences 9
- 1.4 Extensions of number fields 12
- 1.5 Extensions of p-adic fields 13
- 1.6 Galois module structure of the algebraic integers 15

2 The reduction method 19
- 2.1 Linear representation associated to a Hopf Galois structure 20
- 2.2 From linear maps to matrices 21
  - 2.2.1 Change of bases 24
- 2.3 Reducing the matrix of the action 26
  - 2.3.1 Reduced matrices 27
  - 2.3.2 The Hermite normal form 29
- 2.4 Determination of a basis 31
- 2.5 Freeness over the associated order 34
  - 2.5.1 Matrix associated to an element 34
  - 2.5.2 Criteria for freeness 35
- 2.6 Bases of eigenvectors 37
  - 2.6.1 Associated order and freeness 39
  - 2.6.2 The eigenvectors property in the Galois case 40
- 2.7 Absolute extensions of fields with low degree 42
  - 2.7.1 Quadratic extensions 42
  - 2.7.2 Cubic cyclic extensions 45

3 Quartic Galois extensions 53
- 3.1 Determination of the Hopf Galois structures 53
  - 3.1.1 Case 1: G is cyclic 55
  - 3.1.2 Case 2: G is elementary abelian 56
- 3.2 Cyclic quartic extensions of $\mathbb{Q}$ 56
  - 3.2.1 The classical Galois structure 58
  - 3.2.2 Non-classical Hopf Galois structure 60

3.2.3 Summary of results . . . 66
3.3 Biquadratic extensions of $\mathbb{Q}$ . . . 67
3.3.1 Classical Galois structure . . . 67
3.3.2 Non-classical Hopf Galois structures . . . 70
3.3.3 Summary of results . . . 81
3.4 Totally ramified cyclic quartic extensions of $\mathbb{Q}_2$ . . . 82
3.4.1 Classical Galois structure . . . 83
3.4.2 Non-classical Hopf Galois structure . . . 85
3.4.3 Summary of results . . . 87
3.5 Totally ramified biquadratic extensions of $\mathbb{Q}_2$ . . . 88
3.5.1 Classical Galois structure . . . 88
3.5.2 Non-classical Hopf Galois structures . . . 91
3.5.3 Summary of results . . . 95

4 Separable degree p extensions with dihedral Galois closure 97
4.1 The unique Hopf Galois structure . . . 97
4.2 The integral setting . . . 99
4.3 The Gram matrix of E/K . . . 100
4.4 The case $K = \mathbb{Q}_3$ . . . 103
4.4.1 The action on the 3-part . . . 103
4.4.2 Basis of $\mathfrak{A}_{H_1}$ . . . 106
4.4.3 Freeness over $\mathfrak{A}_H$ . . . 107
4.4.4 Summary of results . . . 108
4.5 The case $K = \mathbb{Q}_5$ . . . 108
4.5.1 The action on E . . . 109
4.5.2 Basis of $\mathfrak{A}_{H_1}$ . . . 112
4.5.3 Freeness over $\mathfrak{A}_{H_1}$ . . . 113
4.5.4 Summary of results . . . 113
4.6 Radical cubic extensions of $\mathbb{Q}$ . . . 114

5 Induced Hopf Galois structures 117
5.1 Inducing a Galois extension . . . 118
5.2 Inducing a Hopf Galois extension . . . 121
5.2.1 Induced permutation subgroups . . . 122
5.2.2 The Induction Theorem . . . 124
5.2.3 Induced Hopf algebras . . . 126
5.2.4 Induced Hopf actions . . . 127
5.3 Induced Hopf Galois module structure . . . 128
5.3.1 Relation between the matrices of actions . . . 129
5.3.2 Induced bases . . . 133
5.3.3 Determination of the induced associated order . . . 133
5.3.4 Induced freeness . . . 135
5.3.5 Freeness after tensoring by $\mathcal{O}_F$ . . . 136

6 Dihedral degree $2p$ extensions of $\mathbb{Q}_p$ 139
6.1 Description of the Hopf Galois structures . . . 140
6.1.1 The Hopf algebras involved . . . 141
6.2 The arithmetic of the extension . . . 142
6.2.1 Integral bases . . . 142
6.2.2 Discriminant and ramification . . . 143
6.3 Dihedral Hopf Galois module structure . . . 145

6.3.1 Weakly ramified cases . . . 145
The associated order . . . 145
Module structure over the associated order . . . 146
6.3.2 The radical cases . . . 146
6.4 Cyclic Hopf Galois module structure . . . 148
6.4.1 The case $p = 3$ . . . 149
Summary of results . . . 155
6.4.2 The case $p = 5$ . . . 155
Summary of results . . . 158
6.5 The extension L/F . . . 158
6.5.1 The associated order $\mathfrak{A}_{L/F}$ . . . 159
Radical cases . . . 159
Weakly ramified cases . . . 160
6.5.2 Module structure of $\mathcal{O}_L$ over $\mathfrak{A}_{L/F}$ . . . 163

Conclusions **165**

A Separable degree p^n extensions with Frobenius Galois closure **169**

B Complete form of some items **173**

Bibliography **191**

Introduction

A normal basis of a Galois extension of fields is a basis of the top field of the extension whose elements correspond to a single orbit of the action of the Galois group. Concretely, if L/K is a Galois extension with Galois group G, a normal basis is a K-basis of L of the form

$$\{\sigma(\alpha) \mid \sigma \in G\}, \tag{1}$$

for some $\alpha \in L$. The Galois action can be extended K-linearly to an action of the K-group algebra $K[G]$ on L, which endows L with $K[G]$-module structure. Condition (1) is then equivalent to L being a free $K[G]$-module of rank one with generator α, that is $L \cong K[G]$ as a left $K[G]$-module. This identifies L with the regular representation of G. In virtue of the normal basis theorem, every Galois extension of fields possesses a normal basis, which solves the problem of the existence. The interest of normal bases relies in the fact that elements written with respect to one of these are more manageable and easier to operate with, which makes them attractive from both theoretical and practical points of view.

If L/K is an extension of local or global fields, then we may ask whether a similar description is available for the ring of integers $\mathcal{O}_L$ of the top field L. If the extension is Galois with Galois group G, then $\mathcal{O}_L$ is certainly an $\mathcal{O}_K[G]$-module, commonly referred to as the *Galois module structure of* $\mathcal{O}_L$. Thus, we may ask whether this module is free (in which case, it is of rank one). If it is indeed free and $\alpha \in \mathcal{O}_L$ is a generator, then the Galois conjugates of this α is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ which is a normal basis, i.e. an integral normal basis. The answer when L/K is an extension of local fields is given by Noether's theorem: $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-free if and only if L/K is tamely ramified. Equivalently, in the global case, the tameness of L/K is a necessary and sufficient condition of $\mathcal{O}_L$ being a locally free $\mathcal{O}_K[G]$-module.

Galois extensions of local (resp. global) fields that are not tamely ramified (resp. tamely ramified at a prime) are called wildly ramified (resp. wildly ramified at that prime). Let L/K be some such extension. Since tameness is a necessary condition in Noether's theorem, $\mathcal{O}_L$ is not $\mathcal{O}_K[G]$-free (resp. $\mathcal{O}_K[G]$-locally free). For studying those extensions, Leopoldt noted that $\mathcal{O}_L$ might still be free over

$$\mathfrak{A}_{K[G]} = \{h \in K[G] \mid h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\},$$

where $\cdot\colon K[G] \otimes_K L \longrightarrow L$ is the classical Galois action of $K[G]$ on L. This is called the associated order of $\mathcal{O}_L$ in $K[G]$. Leopoldt also proved that for abelian extensions $L/\mathbb{Q}$ of number fields, the number ring $\mathcal{O}_L$ of L is $\mathfrak{A}_{K[G]}$-free of rank one. This result is generally known as Leopoldt's theorem. It generalizes Noether's theorem since $\mathcal{O}_K[G] \subset \mathfrak{A}_{K[G]}$ with equality if and only if L/K is tamely ramified.

Although the introduction of the associated order led to a considerably better comprehension of the Galois module structure of the algebraic integers, it has visible limitations, for instance there are extensions that have no normal integral basis as defined above. In his paper [Chi87], Childs obtained results on the Galois module structure of $\mathcal{O}_L$ based in the Hopf algebra structure of $K[G]$. This led to the development of Hopf Galois module theory, in which $K[G]$ is replaced by another Hopf Galois structure of L/K: a K-Hopf algebra acting on L satisfying similar properties as $K[G]$ with the Galois action.

The notion of Hopf Galois structure is the beginning of Hopf Galois theory, which is a generalization of Galois theory by the use of Hopf algebras. Concretely, if L/K is a finite extension of fields (not necessarily Galois) and G is a subgroup of $\mathrm{Aut}_K(L)$, then L/K is a Galois extension with group G if and only if the map

$$\begin{array}{rccc} j\colon & L\otimes_K K[G] & \longrightarrow & \mathrm{End}_K(L) \\ & x\otimes h & \longmapsto & j(x\otimes h)(y)=x(h\cdot y) \end{array}$$

is bijective. The Hopf Galois condition for the extension L/K then arises naturally by replacing $K[G]$ by an arbitrary K-Hopf algebra and the Galois action $K[G]\otimes_K L\longrightarrow L$ by any action $\cdot\colon H\otimes_K L\longrightarrow L$ that endows L with H-module algebra structure. The pair formed by H and the module algebra action is what we call a Hopf Galois structure of the extension, and the extension is called Hopf Galois or H-Galois. Then, the classical Galois theory is generalized in the sense that given a Galois extension L/K, the K-group algebra of the Galois group and its action on L is a Hopf Galois structure of L/K. This approach was introduced by Chase and Sweedler in their book [CS69].

If L/K is now an H-Galois extension of local or global fields, the associated order of $\mathcal{O}_L$ in H is defined as

$$\mathfrak{A}_H=\{h\in H\,|\,h\cdot x\in\mathcal{O}_L \text{ for all } x\in\mathcal{O}_L\},$$

and this is easily proved to be the unique $\mathcal{O}_K$-order in $\mathfrak{A}_H$ over which $\mathcal{O}_L$ could be $\mathfrak{A}_H$-free (see Proposition 1.29). Then, the question turns to the study of the $\mathfrak{A}_H$-module structure of $\mathcal{O}_L$, which is naturally referred to as the *Hopf Galois module structure of* $\mathcal{O}_L$. The main advantages of the introduction of Hopf Galois theory are:

- The class of Hopf Galois extensions enlarges the class of Galois extensions, in the sense that every Galois extension is Hopf Galois and there are Hopf Galois extensions that are not Galois. The Hopf Galois module structure of particular classes of Hopf Galois non-Galois extensions is studied for instance by Elder in the local case (see [Eld18]) and by Truman in the global case (see [Tru20]).
- A single extension may have different Hopf Galois structures, each of which gives rise to a different associated order of $\mathcal{O}_L$. Research has shown that there is not a general rule for the behaviour of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module as H runs through the Hopf Galois structures of L/K (see for example the papers [Byo02] and [Chi87] or the final comment of the book [Chi00]).

In this thesis, we enlarge what is known on the determination of the associated order and the Hopf Galois module structure of an extension of local or global fields. We establish a constructive method to compute a basis of the associated order in a Hopf Galois structure and give a necessary and sufficient condition for the freeness of the ring of integers as a module over that associated order. This method does not depend inherently in the ramification of the extension L/K, even on the nature of the fields: all we need is our fields to have rings of integers attached and $\mathcal{O}_K$ to be a PID. In that situation, $\mathcal{O}_L$ is $\mathcal{O}_K$-free. But more importantly, the property that ensures the validity of the method is that $\mathcal{O}_K$ is a Hermite ring in the sense of Kaplansky (see [Kap49]), and consequently we will say that these are **Hermite extensions**.

The idea behind the method is the same as in representation theory: instead of working with the elements of the Hopf algebra, whose structure is often tricky, we use the matrices representing them, and in that setting we have at our disposal the tools of linear algebra. More concretely, if L/K is H-Galois, the action of H on L induces a linear representation of H

$$\rho_H \colon H \longrightarrow \mathrm{End}_K(L)$$

that encodes full information about the action of H on L. Once we have fixed bases of H and L, we consider the canonical basis of $\mathrm{End}_K(L)$ (in its identification with a space of matrices) and we take the matrix of ρ_H as linear map (see Proposition 2.6). The key step is a reduction of this matrix to an $n \times n$ invertible matrix using only integral operations. Consequently, we call this method the *reduction method*. The characterization of the freeness also is closely related with the matrix of the action and depends on a single element of $\mathcal{O}_L$: for every $\beta \in \mathcal{O}_L$, we find a necessary and sufficient condition for β being a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module.

Content of the chapters

This thesis is organized as follows. The first chapter is a review of the main notions that will be needed later on and most of the concepts mentioned in this introduction are studied in more detail. Chapter 2 is the most important one and is devoted to the study of the reduction method in all its generality and the related concepts. Throughout the chapter we develop the example of the Hopf Galois non-Galois extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, taking the description of its unique Hopf Galois structure given in the paper [GP87]. We present the particularities obtained when the extension has an integral basis of eigenvectors of the action. Concretely, the associated order has a basis of pairwise orthogonal idempotents and normal integral basis generators are characterized. At the end of the chapter, we use the reduction method to study the Hopf Galois module structure of absolute extensions of degree 2 and 3.

The rest of the chapters consist essentially in applying the reduction method to different classes of extensions. In Chapter 3, we consider quartic Galois extensions. We determine all the Hopf Galois structures and apply the reduction method successively in the cases that the ground field is $\mathbb{Q}$ and $\mathbb{Q}_2$. In Chapter 4, we move on to separable extensions of degree p whose Galois closure has Galois group the dihedral group D_p of order $2p$. We describe the unique Hopf Galois structure and determine the matrix of the action. However, we are not able to perform the reduction in general, which leads us to consider particular cases. We provide a complete answer when the ground field is $\mathbb{Q}_3$ and $\mathbb{Q}_5$. We end the chapter by considering radical extensions of $\mathbb{Q}$.

At this point, to understand dihedral degree $2p$ extensions themselves we must make a parenthesis to study induced Hopf Galois structures of semidirect Galois extensions (that is, Galois extensions whose Galois group is a semidirect product), which is carried out in Chapter 5. Those are a special kind of Hopf Galois structures that can be seen as a tensor product of Hopf Galois structures in the factor extensions, whose Galois groups are those appearing in the semidirect product. Finally, in Chapter 6 we study dihedral degree $2p$ extensions with ground field $\mathbb{Q}_p$, by using the different ideas and results presented in Chapters 2, 4 and 5. We give complete answers for the cases $p = 3$ and $p = 5$.

Most of the contents in Chapters 2 and 5 (but not all of them) are based in papers [GR] of the author with Anna Rio. Namely, it contains the development of the reduction method and its application to induced Hopf Galois structures.

The computations that are sophisticated enough have been carried out with Maple. Most of the results are displayed in line with the development of this thesis. However, there are some that are considerably bulky and are shown in Appendix B.

Chapter 1

Preliminaries

1.1 Hopf algebras

Since we want to study the action of Hopf algebras on extensions of fields, we begin with a brief review of the main notions of Hopf algebras that are needed. A Hopf algebra is, roughly speaking, a vector space with algebra and coalgebra structures dual with each other (i.e a bialgebra), and a compatible coinverse operation. In this thesis we will work with Hopf algebras over fields, but they can be defined without difficulty over commutative rings with unity. The main reference for this part is [Und15, Chapter 3].

Definition 1.1. *Let R be a commutative ring with unity. An R-**Hopf algebra** is a* 6*-uple* $(H, m_R, \lambda_R, \Delta_R, \epsilon_R, \sigma_R)$ *where:*

1. *H is an R-module.*
2. *(H, m_H, λ_H) is an R-algebra, that is, $m_H \colon H \otimes_R H \longrightarrow H$ and $\lambda_H \colon R \longrightarrow H$ are R-linear maps that satisfy:*

   2.a. *[**Associative property**] Given $a, b, c \in H$,*

   $$m_H(m_H \otimes Id_H)(a \otimes b \otimes c) = m_H(Id_H \otimes m_H)(a \otimes b \otimes c).$$

   Equivalently, the following diagram is commutative:

   $$\begin{tikzcd}
   H \otimes H \otimes H \arrow[r, "Id_H \otimes m_H"] \arrow[d, "m_H \otimes Id_H"'] & H \otimes H \arrow[d, "m_H"] \\
   H \otimes H \arrow[r, "m_H"] & H
   \end{tikzcd}$$

   2.b. *[**Unit property**] Given $a \in H$ and $r \in R$,*

   $$m_H(\lambda_H \otimes \mathrm{Id}_H)(r \otimes a) = r\,a = m_H(\mathrm{Id}_H \otimes \lambda_H)(a \otimes r).$$

   Equivalently, the following diagrams are commutative:

   $$\begin{tikzcd}
   H \otimes R \arrow[r, "Id_H \otimes \lambda_H"] \arrow[d, "s_2"'] & H \otimes H \arrow[dl, "m_H"'] \\
   H & R \otimes H \arrow[l, "s_1"] \arrow[u, "\lambda_H \otimes Id_H"']
   \end{tikzcd}$$

where $s_1\colon R\otimes H \longrightarrow H$ and $s_2\colon H\otimes R \longrightarrow H$ are defined by $s_1(r\otimes a) = r\,a = s_2(a\otimes r)$.

The map m_H is called the ***multiplication map****, and λ_H is called the* ***unit map****.*

3. *(H,Δ_H,ϵ_H) is an R-coalgebra, that is, $\Delta_H\colon H \longrightarrow H\otimes H$ and $\epsilon_H\colon H \longrightarrow R$ are R-linear maps that satisfy:*

3.a. ***(Coassociative property)*** *There is a commutative diagram:*

$$\begin{tikzcd}
H \arrow[r, "\Delta_H"] \arrow[d, "\Delta_H"'] & H\otimes H \arrow[d, "Id_C\otimes\Delta_H"] \\
H\otimes H \arrow[r, "\Delta_H\otimes Id_H"] & H\otimes H\otimes H
\end{tikzcd}$$

Equivalently, for all $h\in H$,

$$(Id_H\otimes\Delta_H)\Delta_H(h) = (\Delta_H\otimes Id_H)\Delta_H(h).$$

3.b. ***(Counit properties)*** *The following diagrams are commutative:*

$$\begin{tikzcd}
H \arrow[r, "1\otimes -"] \arrow[d, "-\otimes 1"'] \arrow[dr, "\Delta_H"] & R\otimes H \\
H\otimes R & H\otimes H \arrow[l, "Id_H\otimes\epsilon_H"] \arrow[u, "\epsilon_H\otimes Id_H"']
\end{tikzcd}$$

Equivalently, for all $h\in H$,

$$(\epsilon_H\otimes Id_H)\Delta_H(h) = 1\otimes h,$$

$$(Id_H\otimes\epsilon_H)\Delta_H(h) = h\otimes 1.$$

The map Δ_H is called the ***comultiplication map*** *and ϵ_H is called the counit map.*

4. *$(H,m_H,\lambda_H,\Delta_H,\epsilon_H)$ is an R-bialgebra, that is, Δ_H and ϵ_H are homomorphisms of R-algebras.*

5. *$\sigma_H\colon H \longrightarrow H$ is an R-linear map satisfying the following property:*

$$m_H(\mathrm{Id}_H\otimes\sigma_H)\Delta_H(h) = \epsilon_H(h)\,1_H = m_H(\sigma_H\otimes Id_H)\Delta_H(h),\ h\in H.$$

Remark 1.2. *In the fourth point we ask $\Delta_H\colon H \longrightarrow H\otimes H$ to be an R-algebra homomorphism, that is, it may respect the R-algebra structures on H and $H\otimes H$. The R-algebra structure of $H\otimes H$ is given by*

$$m_{H\otimes H}((a\otimes b)\otimes(c\otimes d)) = (a\,c)\otimes(b\,d),$$

$$\lambda_{H\otimes H}(r) = \lambda_{H\otimes H}(r)\otimes 1_H.$$

An R-Hopf algebra is a ring with unity with the usual sum and product

$$a\,b := m_H(a \otimes b),$$

because of the associative and unit properties. However, this ring is not in general commutative.

Let us define $\tau\colon H \otimes_R H \longrightarrow H \otimes_R H$ as $\tau(a \otimes b) = b \otimes a$ for every $a \otimes b$.

Definition 1.3. *Let H be an R-Hopf algebra.*

1. *We say that H is **commutative** if $m_H \circ \tau = m_H$.*

2. *We say that H is **cocommutative** if $\Delta_H = \tau \circ \Delta_H$.*

The easiest example of an R-Hopf algebra is the ring R itself. Another example of R-Hopf algebra is the following:

Example 1.4. *Let G be a finite group and let R be a commutative ring with unity. Then, the group ring*

$$R[G] = \{\sum_{g \in G} a_g\, g \mid a_g \in R\}$$

is clearly an R-module. It is finitely generated because the elements of G form a system of generators, which is free by definition. Thus, $R[G]$ is R-free with basis G. Actually, it is an R-Hopf algebra with the maps

$$m_{R[G]}(g \otimes h) = g\,h,\ g, h \in G,$$

$$\lambda_{R[G]}(r) = r\,e_G,\ r \in R,$$

$$\Delta_{R[G]}(g) = g \otimes g,\ g \in G$$

$$\epsilon_{R[G]}(g) = 1,\ g \in G$$

$$\sigma_{R[G]}(g) = g^{-1},\ g \in G.$$

It is clearly cocommutative but it is commutative only if so is G.

Now, we introduce a notation for the image of any element of H by the comultiplication, called the **Sweedler's notation**. Given $h \in H$, we know that $\Delta_H(h) \in H \otimes_R H$, so it is a sum of elements of the form $h_{(1)} \otimes h_{(2)}$, where $h_{(1)}, h_{(2)} \in H$. We denote

$$\Delta_H(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}.$$

Keeping Sweedler's notation in mind, we make the following definition.

Definition 1.5. *Let H be an R-Hopf algebra and let A be an R-algebra which is also a left H-module with action denoted by $\cdot$. We say that A is a **left H-module algebra** if the following conditions are satisfied:*

1. *$h \cdot (a\,a') = \sum_{(h)} (h_{(1)} \cdot a)\,(h_{(2)} \cdot a')$ for all $h \in H$ and $a, a' \in A$.*

2. *$h \cdot 1_A = \epsilon_H(h)\,1_A$ for all $h \in H$.*

1.2 Hopf Galois structures

Let L/K be a finite extension of fields and let G be a group of K-automorphisms of L in a previously fixed algebraic closure $\overline{K}$ of K. The most usual definition of L/K being Galois with group G is that every K-embedding of L into $\overline{K}$ restricts to an element of G. If so, G is the set of all K-embeddings of L in $\overline{K}$, which coincides with the group $\mathrm{Aut}_K(L)$ of automorphisms of L that fix K. A Hopf Galois structure is an object that in some sense plays the role of the Galois group and when it exists the extension is called Hopf Galois. More accurately, in the case of the Galois group, this role depends on the K-group algebra $K[G]$ and its K-linear action on L, which endows L with left $K[G]$-module algebra structure (see [Und15, Proposition 4.5.1]). The definition of Hopf Galois structure arises naturally from the following characterization of Galois extensions:

Theorem 1.6. *Let G be a subgroup of $\mathrm{Aut}_K(L)$. Then, L/K is Galois with Galois group G if and only if the map $j\colon L\otimes_K K[G]\longrightarrow \mathrm{End}_K(L)$ defined as $j(x\otimes\sigma)(y)=x\sigma(y)$ for $\sigma\in G$ and extended by K-linearity is an isomorphism of K-vector spaces.*

A proof can be found in [Und15, Proposition 4.5.3]. Although in that statement the ground field is an extension of $\mathbb{Q}$, it is actually not used in the proof since it is based on the Dedekind independence theorem, which does not need the field L to be an extension of $\mathbb{Q}$.

As aforementioned, since the group G is finite, $K[G]$ is a finite dimensional cocommutative K-Hopf algebra. By replacing it with another Hopf algebra with similar properties, the definition of Hopf Galois structure follows.

Definition 1.7. *A Hopf Galois structure on L/K is a pair $(H,\cdot)$ where H is a finite dimensional cocommutative K-Hopf algebra and $\cdot\colon H\otimes_K L\longrightarrow L$ is a K-linear action that endows L with H-module algebra structure, such that the map*

$$\begin{array}{rccl} j\colon & L\otimes_K H & \longrightarrow & L \\ & x\otimes h & \longmapsto & j(x\otimes h)(y)=x(h\cdot y) \end{array}$$

is an isomorphism of K-vector spaces.

If $(H,\cdot)$ is a Hopf Galois structure of L/K and the action $\cdot$ is implicit in the context, we will also say that L/K is H-Galois. A Hopf Galois extension is an extension that admits some Hopf Galois structure. With this definition, every Galois extension is Hopf Galois, as $K[G]$ together with the classical Galois action extended by K-linearity is a Hopf Galois structure. This is called **the classical Galois structure**, denoted by H_c henceforth.

However, the converse does not hold in general: for instance, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is a Hopf Galois extension that is not Galois. This is an example of extensions that will be studied broadly later on in this thesis: the separable degree p extensions whose normal closure has Galois group isomorphic to D_p, the dihedral group of $2p$ elements, with p an odd prime number. Actually, that example is a particular case of Proposition 1.12 below.

There are also extensions that have several different Hopf Galois structures. For example the Galois closure of the previous one admits in total 5 Hopf Galois structures.

1.3 Greither-Pareigis theory

Finding and describing all Hopf Galois structures of a given extension may be an extremely difficult task, but if the extension is separable, Greither and Pareigis gave in their paper [GP87] a one-to-one correspondence between the Hopf Galois structures and a class of permutation subgroups, giving rise to the so called Greither-Pareigis theory.

1.3.1 The Greither-Pareigis theorem

Let L/K be a finite separable extension of fields. We call $\widetilde{L}$ the Galois closure of L/K, $G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$ and $X = G/G'$ the set of left cosets of G' in G. The coset of an element $g \in G$ is denoted by $\overline{g}$.

Definition 1.8. *The* ***left translation map*** *of G is the map $\lambda \colon G \longrightarrow \mathrm{Perm}(X)$ defined as $\lambda(\tau)(\overline{\sigma}) = \overline{\tau\sigma}$.*

Definition 1.9. *A subgroup N of $\mathrm{Perm}(X)$ is regular if it satisfies two of the following conditions (in which case, it also satisfies the third one):*

1. $|N| = |X|$.
2. *N acts transitively over X.*
3. *Given $x \in X$, the stabilizer of the action of N on x, $\mathrm{Sta}_N(x) = \{\eta \in N \mid \eta(x) = x\}$, is trivial.*

These are all the ingredients we need to give the full statement of the Greither-Pareigis theorem:

Theorem 1.10 (Greither-Pareigis)**.** *Let L/K be a finite separable extension and consider the previous notation. The Hopf Galois structures of L/K are in one-to-one correspondence with the regular subgroups of $\mathrm{Perm}(X)$ normalized by $\lambda(G)$.*

If N is such a subgroup, the corresponding Hopf Galois structure is given by

$$H := \widetilde{L}[N]^G = \{h \in L[N] \mid \sigma(h) = h \,\forall \sigma \in G\},$$

where G acts on $\widetilde{L}$ by means of the classical Galois action and on N as follows:

$$\sigma \cdot \eta = \lambda(\sigma)\eta\lambda(\sigma^{-1}),\, \sigma \in G,\, \eta \in N.$$

Note that this is actually an action closed on N because it is normalized by $\lambda(G)$. Regarding the action of H on L, if $h = \sum_{i=1}^{n} h_i\eta_i \in H$, then for every $x \in L$,

$$h \cdot x = \sum_{i=1}^{n} h_i \eta_i^{-1}(\overline{1_G})(x).$$

For the proof and related information, see [Chi00, Theorem 6.8].

1.3.2 Consequences

The appearance of the Greither-Pareigis theorem led to a number of results classifying Hopf Galois structures of many classes of extensions and in general allowed a deeper comprehension of Hopf Galois extensions.

The classical Galois structure and the canonical non-classical Galois structure

Let L/K be a Galois extension with Galois group G. In this case, the left translation map becomes $\lambda\colon G \longrightarrow \mathrm{Perm}(G)$ defined by $\lambda(\tau)(\sigma) = \tau\sigma$.

Definition 1.11. *The **right translation map** of G into $\mathrm{Perm}(G)$ is the map $\rho\colon G \longrightarrow \mathrm{Perm}(G)$ defined as $\rho(\tau)(\sigma) = \sigma\tau^{-1}$.*

Note that the definition of ρ is not correct if the extension is not Galois.

The Greither-Pareigis theorem in this case says that Hopf Galois structures of L/K are in one-to-one correspondence with regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$. But $\lambda(G)$ and $\rho(G)$ are themselves some such subgroups, so they give rise to Hopf Galois structures of L/K:

- The group $\rho(G)$ gives the classical Galois structure H_c (see [Chi00, Proposition 6.10]).
- The Hopf Galois structure given by $\lambda(G)$ is called **the canonical non-classical Hopf Galois structure**, denoted by H_λ.

It holds that $\lambda(G) = \rho(G)$ if and only if G is abelian (see [Chi00, Example 6.9]). Hence, they actually define the same Hopf Galois structure of L/K if and only if L/K is abelian.

A refinement of the Greither-Pareigis theorem: Byott's translation

When the degree of the extension is very low, explicit computations may be carried out so as to compute explicitly the Hopf Galois structures of the extension. For instance, if L/K is a separable extension of degree at most 4, then L/K is Hopf Galois (see [Chi00, Thoerem 6.13]).

The main disadvantage of the Greither-Pareigis theorem is that the complexity of the computation grows quickly with the degree of the extension. A refinement reversing the relationship between G and N was introduced by Byott, the so called Byott translation. We will not state the corresponding theorem here, but the reader can consult it for instance in [Chi00, Theorem 7.3]. Among its applications, it provides a formula for the number of Hopf Galois structures on a extensions in terms of G, G' and N (see [Byo96, Proposition 1]). Moreover, it can be used to prove easily the following:

Proposition 1.12. *Let L/K be a separable extension of fields with prime degree, let $\widetilde{L}$ be its normal closure and let $G = \mathrm{Gal}(\widetilde{L}/K)$. Then, L/K is Hopf Galois if and only if G is solvable.*

The proof can be found in [Chi00, Proposition 7.5]. In particular, if G is isomorphic to S_p or A_p with $p \geq 5$ prime, then L/K is not Hopf Galois. Hence, the first example of separable extension that is not Hopf Galois can be found at degree 5.

Almost classically Galois extensions

Let L/K be a separable extension and let $\widetilde{L}$, G, G' and X as usual. By the Greither-Pareigis theorem, Hopf Galois structures of L/K are in one-to-one correspondence with regular subgroups N of $\mathrm{Perm}(X)$ normalized by $\lambda(G)$. However, the theorem does not tell us whether $N \subset \lambda(G)$ or not. Actually, in practice we can find both situations. This distinction leads us to an important subclass of Hopf Galois extensions: the almost classically Galois extensions.

Theorem 1.13. *Let L/K be a separable extension. Then, the following are equivalent:*

1. *There is some Galois extension E/K such that $E \otimes_K L$ is a field that contains $\widetilde{L}$.*
2. *There is some Galois extension E/K such that $E \otimes_K L = \widetilde{L}$.*
3. *There is some normal complement J of G' in G.*
4. *There is a regular subgroup N of $\mathrm{Perm}(X)$ normalized by $\lambda(G)$ such that $N \subset \lambda(G)$.*

Proof. See [GP87, Proposition 4.1]. □

Definition 1.14. *Let L/K be a separable extension. We say that L/K is **almost classically Galois** if it satisfies some (any) of the equivalent conditions of Theorem 1.13. An extension E/K satisfying statements 1 or 2 is said to be a Galois complement.*

It is also possible to define what we understand by an almost classical Galois structure.

Definition 1.15. *Let $(H, \cdot)$ be a Hopf Galois structure of a separable extension L/K and let N be the regular subgroup of $\mathrm{Perm}(X)$ normalized by $\lambda(G)$. We say that $(H, \cdot)$ is an **almost classically Galois structure** if $N^{\mathrm{opp}} \subset \lambda(G)$.*

In this statement, N^{opp} is the centraliser of N in $\mathrm{Perm}(X)$, which is called the opposite group of N (see [GP87, Lemma 2.4.2.]). It can be identified with the group with the same underlying set as the group N and operation $ab := b \cdot_N a$, where $\cdot_N$ is the operation of N. The definition of almost classically Galois structure is correct because N is regular if and only if so is N^{opp}. The reason why we choose N^{opp} instead of N is that the Hopf algebra it provides is somewhat similar to $K[N]$ (see [GP87, Theorem 2.5] and the preceding remark).

As one may expect, L/K is almost classically Galois if and only if it has some almost classically Galois structure. Then, every almost classically Galois extension is Hopf Galois. The converse does not hold in general, but it is not trivial at all (see [GP87, Theorem 4.4] for a counterexample). Moreover, every Galois extension is almost classically Galois.

Byott's Uniqueness Theorem

Another important consequence is the Byott Uniqueness Theorem. A number $g \in \mathbb{Z}$ is said to be Burnside if g is coprime with $\varphi(g)$, where φ is the Euler function. The statement of the theorem is as follows:

Theorem 1.16 (Byott)**.** *Let L/K be a Galois extension and let G be its Galois group. Then, L/K has a unique Hopf Galois structure (the classical Galois structure) if and only if $|G|$ is a Burnside number.*

For a proof, see [Byo96, Theorem 1] or [Chi00, Theorem 8.1]. Actually, there is a version of the previous theorem for separable extensions that are not necessarily normal (see [Byo96, Theorem 2]):

Theorem 1.17. *Let L/K be a separable Hopf Galois extension of degree a Burnside number. Then, L/K admits a unique Hopf Galois structure. Moreover, this Hopf Galois structure is almost classically Galois.*

Examples of Burnside numbers are a prime number or pq for p and q primes such that $q < p$ and q does not divide $p-1$. Hence, for extensions of those degrees, there is a unique Hopf Galois structure, which is the classical one if the extension is Galois.

1.4 Extensions of number fields

In this section we recall briefly the most basic lines of the theory of number fields. The main reference is the book of Marcus [Mar77].

A **number field** is a finite extension of the field $\mathbb{Q}$ of rational numbers. Since $\mathbb{Q}$ is a perfect field, such an extension is always monogenic. The most common examples of number fields are the **quadratic fields**, those of degree 2, and the **cyclotomic fields**, generated by a primitive n-th root of unity, where $n \geq 1$.

An **algebraic integer** is a complex number which is root of a monic polynomial with integer coefficients (that is, a polynomial of $\mathbb{Z}[x]$). The **ring of integers** $\mathcal{O}_K$ of a number field K is the set of its algebraic integers, that is, $\mathcal{O}_K$ is the intersection of K with the set of all algebraic integers. It is a subring of K which is an integral domain, and K is its field of fractions. What is more, $\mathcal{O}_K$ is a **Dedekind domain**: an integral domain such that every ideal factorizes uniquely as a product of prime ideals.

In general, $\mathcal{O}_K$ is not a principal ideal domain, it is so if and only if it is a unique factorization domain. Let $\sim$ the relation on ideals of R such that $I \sim J$ if and only if there are $\alpha, \beta \in R$ such that $\alpha I = \beta J$ for every pair of ideals I and J of R. This is an equivalence relation, and the quotient set has group structure with the operation induced by the product of ideals. This is what we call the **ideal class group** of K. The class of principal ideals is the identity element. One of the main results in classical algebraic number theory is that the ideal class group is finite (see for example [Mar77, Chapter 5]). Its cardinal is called the **class number** of K. Hence, $\mathcal{O}_K$ is a PID if and only if it has class number 1.

An important notion concerning the arithmetic of a number field is its discriminant. Although it can be defined specifically for number fields, we give the general definition in [Chi00, Chapter 6]. Let R be a commutative ring and let A be an R-algebra which is finitely generated and free of rank n as an R-module. Given $x \in A$, let us denote $T_x \colon A \longrightarrow A$ the multiplication-by-a map and let $\mathrm{tr}(x)$ be its trace as linear map. If $\{x_1, ..., x_n\}$ is an R-basis of A, the **discriminant** of $(x_1, ..., x_n)$ is defined by

$$\mathrm{disc}(x_1, ..., x_n) = \det((\mathrm{tr}(x_i x_j))_{i,j=1}^n).$$

The ideal in R generated by $\mathrm{disc}(x_1, ..., x_n)$ is the **discriminant ideal** A. This definition is correct because such ideal is an invariant of R-bases of A (see [Chi00, Corollary 22.3]).

We are interested in extensions of number fields L/K rather than number fields themselves. Clearly, $\mathcal{O}_L$ has $\mathcal{O}_K$-module structure with the operation of L. It is finitely generated because L/K is finite, and torsion-free because it is contained in a field. Let us assume that in addition $\mathcal{O}_K$ is a principal ideal domain. Then, $\mathcal{O}_L$ is $\mathcal{O}_K$-free, and a basis of this module is called an **integral basis** of L. Moreover, the discriminant is an invariant of the integral bases of L, and then we can define the **discriminant of** L/K, denoted by $\mathrm{disc}(L/K)$ as the discriminant ideal of any of its integral bases. Another distinguished type of basis of L is a **power basis**: the one formed by the powers up to $[L : K]$ of a single element $\alpha \in L$. This is actually a K-basis of L whenever α is a primitive element of L/K.

Although there is a ramification theory for extensions of number fields, we will not deal with it in this thesis. The interested reader can consult [Mar77, Chapter 3].

1.5 Extensions of p-adic fields

Let p be a prime number. In this thesis, we will refer to a p-adic field as a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers. While number fields form a class of global fields (see [LL07, Chapter 25, Definition 2]), the class of p-adic fields is contained in the one of local fields (see [LL07, Chapter 25, F2]). Roughly speaking, the p-adic fields can be seen as a local analog of number fields.

If K is a p-adic field, the valuation ring or the ring of integers of K, denoted by $\mathcal{O}_K$, is the set of elements of K that are roots of monic polynomials with coefficients in $\mathbb{Z}_p$. In this case, $\mathcal{O}_K$ is a discrete valuation ring, that is, it has a unique prime ideal P, which subsequently is principal. In particular, $\mathcal{O}_K$ is always a PID. Any generator of P is called an **uniformising parameter** of K, denoted by π_K.

Every non-zero element of $\mathcal{O}_K$ is of the form $x = \pi^{v_K(x)}u$, where $u \in \mathcal{O}_K^*$ and $v_K(x) \in \mathbb{Z}_{\geq 0}$. Then we have a map v_K which can also be defined on the whole K by using that $K = \mathrm{Frac}(\mathcal{O}_K)$: if $a = \frac{x}{y} \in K$, $v_K(a) = v_K(x) - v_K(y)$. Defining $v_K(0) = \infty$, the map $v_K \colon K \longrightarrow \mathbb{Z} \cup \{\infty\}$ is a discrete valuation of K, the **π_K-adic valuation of** K. By construction, an element $a \in K$ belongs to $\mathcal{O}_K$ (resp. $\mathcal{O}_K^*$) if and only if $v_K(a) \geq 0$ (resp. $v_K(a) = 0$).

On the other hand, since P is the unique prime ideal, it is maximal, and so $k = \mathcal{O}_K/P$ is a finite field, called **the residue field of** K. If $K = \mathbb{Q}_p$, the ring of integers is $\mathbb{Z}_p$ and the uniformising parameter (up to multiplication by units) is p. The corresponding valuation v_p is called the **p-adic valuation**, and on $a \in \mathbb{Q}$ is defined as the power of p in the factorization of a (where we accept non-positive powers).

We review one of the most famous results concerning p-adic fields theory and with many applications, which is commonly known as Hensel's lemma.

Theorem 1.18 (Hensel's lemma). *Let K be a p-adic field and let $f \in \mathcal{O}_K[x]$. Let $\overline{f} \in k[x]$ be the reduction of f, that is, the polynomial whose coefficients are the classes of the coefficients of f modulo P. If $\overline{f}$ has a simple root $\theta \in k$, then there is a unique $a \in \mathcal{O}_K$ such that $f(a) = 0$ and $\overline{a} = \theta$.*

The statement is actually a bit more general (see [Con, Theorem 9.1]).

Let L/K be an extension of p-adic fields. Then the corresponding rings of integers form an extension $\mathcal{O}_L/\mathcal{O}_K$ of commutative rings, and in particular $\mathcal{O}_L$ is an

$\mathcal{O}_K$-module. It is again finitely generated and torsion-free, and now $\mathcal{O}_K$ is always a PID, so $\mathcal{O}_L$ is $\mathcal{O}_K$-free and its rank is the degree $[L : K]$ of the extension. Again, an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ is called an **integral basis** of L, and the **discriminant** of L/K, denoted by $\mathrm{disc}(L/K)$, is the discriminant of any of its integral bases. The number $c(L/K) = v_K(\mathrm{disc}(L/K))$ will be called the **discriminant exponent**. A **power basis** of an extension of p-adic fields has the analog definition as in the case of number fields. If $K = \mathbb{Q}_p$, a **Galois splitting model** of $L/\mathbb{Q}_p$ is an irreducible polynomial $f \in \mathbb{Q}[x]$ such that $L \cong \mathbb{Q}_p[x]/\langle f \rangle$, and the Galois group of f over $\mathbb{Q}_p$ is isomorphic to that of f over $\mathbb{Q}$. The Galois splitting models used in this thesis are taken from the web page [LMFDB]. There are examples of local fields that have no Galois splitting models (see the help page of [LMFDB]).

We now explore the ramification theory for extensions of local fields. For the ideal $\pi_K\mathcal{O}_L$ of $\mathcal{O}_L$, there is an integer $e(L/K) \in \mathbb{Z}_{\geq 1}$ such that $\pi_K\mathcal{O}_L = \pi_L^{e(L/K)}\mathcal{O}_L$. This number $e(L/K)$ is the **ramification index** of L/K. If l and k are the corresponding residue fields, then l/k is a finite extension of fields, whose degree $f(L/K) := [l : k]$ is called the **residue class degree** of L/K. By [LL07, Chapter 24, Theorem 1], $e(L/K)f(L/K) = n$.

Definition 1.19. *Let L/K be an extension of p-adic fields.*

1. *We say that L/K is **unramified** if $e(L/K) = 1$.*
2. *We say that L/K is **totally ramified** if $e(L/K) = [L : K]$.*
3. *We say that L/K is **tamely ramified** if $\gcd(e(L/K), p) = 1$. Otherwise, we will say that L/K is wildly ramified.*

For a p-adic field K, a monic polynomial $g(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathcal{O}_K[x]$ is called π_K**-Eisenstein** if $v_K(a_i) \geq 1$ for all $0 \leq i \leq n-1$ and $v_K(a_0) = 1$. If L/K is a totally ramified extension of p-adic fields, then $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. In order to find integral bases of L we have the following result at our disposal (see [FT92, Theorem 24]):

Theorem 1.20. *If $\alpha \in L$ is a primitive element of L/K which is also a root of some π_K-Eisenstein polynomial $g \in \mathcal{O}_K[x]$, then L/K is totally ramified and α is a uniformising parameter of L.*

Next, we recall the theory of higher ramification groups. The main reference for this part is [Ser, Chapter IV].

Definition 1.21. *Let L/K be a Galois extension of p-adic fields with Galois group G. For $i \geq -1$, the i-th ramification group of L/K is defined as $G_{-1} = G$ and*

$$G_i = \{\sigma \in G \,|\, \sigma(x) \equiv x \pmod{\pi_L^{i+1}} \text{ for all } x \in \mathcal{O}_L\}$$

for $i \geq 0$.

It is immediate that $G_i \supseteq G_{i+1}$ for every $i \geq -1$, and actually G_{i+1} is a normal subgroup of G_i. Moreover there exists $i_0 \geq 0$ such that G_i is trivial for all $i \geq i_0$ (see [Ser, Chapter IV, Proposition 1]). Then, the ramification groups of L/K form a filtration

$$G = G_{-1} \supset G_0 \supset G_1 \supset \cdots \supset \{1\},$$

which will be referred to as the chain of ramification groups of L/K in the sequel.

Definition 1.22. *A **ramification number** of L/K is an integer number $t \geq -1$ such that $G_t \neq G_{t+1}$. If the extension is cyclic of degree p, it is unique and denoted by $t(L/K)$.*

The group G_0 is also called the inertia group of L/K. We have that L/K is unramified (resp. totally ramified, resp. tamely ramified) if and only if $G_0 = \{1\}$ (resp. $G_0 = G$, resp. $G_1 = \{1\}$). This last property is due to the fact that G_1 is the p-Sylow subgroup of G_0 (see [Ser, Chapter IV, Corollaries 1 and 3]). It is a characterization of tamely ramified extensions, and it motivates the introduction of the following class of extensions, which will be very relevant later on:

Definition 1.23. *An extension L/K of p-adic fields is said to be **weakly ramified** if $G_2 = \{1\}$.*

To determine the chain of ramification groups of an extension in practice, what we will do is to determine the discriminant exponent $c(L/K)$ and then use the following result (see [Ser, Chapter IV, Proposition 4]):

Proposition 1.24. *With the previous notation,*

$$c(L/K) = f(L/K)\sum_{i=0}^{\infty}(|G_i| - 1)$$

1.6 Galois module structure of the algebraic integers

The starting point of Galois module theory is the normal basis theorem for Galois extensions.

Theorem 1.25 (Normal basis theorem)**.** *If L/K is a finite Galois extension of fields with Galois group G, then there is $\alpha \in L$ such that L has K-basis*

$$\{\sigma(\alpha) \mid \sigma \in G\}.$$

Proof. See, for example, [Coh07, Section 3.2]. □

A basis as in the previous statement is called a **normal basis** of L/K, and what the normal basis theorem means is that it always exists for an arbitrary extension of fields. If L/K is now a Galois extension of number or p-adic fields, Noether's theorem tells us whether $\mathcal{O}_L$ has some such basis.

Theorem 1.26 (Noether)**.** *If L/K is an extension of p-adic fields, then there is some $\alpha \in \mathcal{O}_L$ such that*

$$\{\sigma(\alpha) \mid \sigma \in G\}$$

is an integral basis of L if and only if L/K is tamely ramified.

In the literature, a basis as in the previous statement is called a normal integral basis. But in this thesis we will reserve that name for a more general concept, in the setting of Hopf Galois theory. As we know from the introduction, the idea is to replace $\mathcal{O}_K[G]$ with a more general object. These objects are $\mathcal{O}_K$-orders in $K[G]$ or a given Hopf Galois structure, and the general definition is as follows (see [Tru09, Definition 2.1.3.]):

Definition 1.27. *Let R be a Dedekind domain and let $K = \mathrm{Frac}(R)$ be the field of fractions of R. Let A be a finite dimensional K-algebra. An R-order in A is a subring $\mathfrak{A}$ in A such that:*

1. *The centre of $\mathfrak{A}$ contains R.*

2. *$\mathfrak{A}$ is finitely generated as an R-module.*

3. *$\mathfrak{A} \otimes_R K = A$.*

Now, the object we consider as ground ring for $\mathcal{O}_L$ is the following:

Definition 1.28. *Let L/K be an H-Galois extension of number or p-adic fields. The* ***associated order*** *of $\mathcal{O}_L$ in H is defined as*

$$\mathfrak{A}_H = \{h \in H \,|\, h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

The associated order is indeed an $\mathcal{O}_K$-order in H. The following proposition shows that the associated order is actually the right object to choose (see [Chi00, Proposition 12.5]):

Proposition 1.29. *If L/K is an H-Galois extension of number or p-adic fields and $\mathfrak{A}$ is an $\mathcal{O}_K$-order in H such that $\mathcal{O}_L$ is $\mathfrak{A}$-free, then $\mathfrak{A} = \mathfrak{A}_H$.*

If H is either the classical Galois structure of L/K or the unique Hopf Galois structure of L/K, we will denote $\mathfrak{A}_{L/K} = \mathfrak{A}_H$. Whenever $\mathcal{O}_K$ is a PID (which is the case if K is a p-adic field or a number field of class number 1), $\mathfrak{A}_H$ is $\mathcal{O}_K$-free of rank $[L : K]$. Hence, if $\mathcal{O}_L$ is $\mathfrak{A}_H$-free, it has rank one, as both of them are $\mathcal{O}_K$-free of the same rank. Consequently, if α generates $\mathcal{O}_L$ as $\mathfrak{A}_H$-module and $\{v_i\}_{i=1}^n$ is an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$,

$$\{v_1 \cdot \alpha, \dots v_n \cdot \alpha\}$$

is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$, which is what in this thesis will be called a **normal integral basis**. A free generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module like α will be called a **normal integral basis generator**. Its existence implies, obviously, that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

It does not hold in general that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free for a given Hopf Galois structure H. Nevertheless, there are a number of results finding conditions to imply or implied by the freeness. Concerning the classical Galois structure, one of the most celebrated is the following:

Theorem 1.30 (Leopoldt)**.** *If $L/\mathbb{Q}$ is an abelian extension of number fields, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free and a normal integral basis generator can be constructed explicitly.*

The local analog of Leopoldt's theorem also holds: for any abelian extension $L/\mathbb{Q}_p$ of p-adic fields, $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_p}$-free. Actually, Lettl proves in [Let98, Theorem 1] the analog result for the slightly more general class of extensions L/K of p-adic fields with $L/\mathbb{Q}_p$ abelian.

There are positive results due to Truman for the Hopf Galois module structure of $\mathcal{O}_L$ in the cases that L/K is an unramified or tamely ramified extension of p-adic fields.

Theorem 1.31. *Let L/K be a finite Hopf Galois unramified extension of p-adic fields, and let $H = L[N]^G$ be a Hopf Galois structure of L/K. Then, $\mathfrak{A}_H = \mathcal{O}_L[N]^G$ and $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.*

Proof. See [Tru09, Theorems 3.3.2 and 3.1.1]. □

Theorem 1.32. *Let L/K be an H-Galois tamely ramified Galois extension of p-adic fields and suppose that H is commutative. Then, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.*

Proof. See [Tru18, Theorem 4.6]. □

These and other results show that we have a better comprehension of tamely ramified extensions. For this reason, in this thesis we will prioritise the study of the wildly ramified ones.

Cyclic extensions of degree p

Let L/K be a cyclic extension of degree p of p-adic fields. By Byott Uniqueness Theorem, the classical Galois structure H_c is the unique Hopf Galois structure of L/K. A description of the associated order is given in the following (see [Fer74, Section 2.1 and Proposition 3]):

Proposition 1.33. *Let $G = \langle\sigma\rangle$ be the Galois group of L/K, let t be its ramification number and let $a = \mathrm{rem}(t, p)$ be the remainder of the Euclidean division of t by p. If $a = 0$, $\mathfrak{A}_{L/K}$ is the maximal $\mathcal{O}_K$-order in $K[G]$. Otherwise, a basis of $\mathfrak{A}_{L/K}$ is given by*

$$\left\{\frac{(\sigma - 1_G)^i}{\pi_L^{n_i}}\right\}_{i=0}^{p-1},$$

where $n_i = \min_{0\leq j\leq p-1-i}(\nu_{i+j} - \nu_j)$ and $\nu_i = \left[\frac{it+a}{p}\right]$ for all $0 \leq i \leq p-1$.

The problem of the $\mathfrak{A}_{L/K}$-freness of $\mathcal{O}_L$ was completely solved by M.J. Ferton (see for example [Fer74] or [Tho10, Theorem 3.4]):

Theorem 1.34. *Let L/K be a cyclic extension of degree p of p-adic fields, let $e = e(K/\mathbb{Q}_p)$, and let t be its ramification number. Call $a = \mathrm{rem}(t, p)$. Then:*

1. *If $t < \frac{pe}{p-1} - 1$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if $a|p-1$.*
2. *If $\frac{pe}{p-1} - 1 \leq t \leq \frac{pe}{p-1}$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free if and only if the length of the expansion of $\frac{t}{p}$ as continued fraction is at most 4.*

Chapter 2

The reduction method

The reduction method is the central tool of this thesis. For an H-Galois extension L/K of number or p-adic fields (with K of class number 1 if the extension is of number fields), it provides an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$ and gives a necessary and sufficient condition to determine whether or not a given element of $\mathcal{O}_L$ is a normal integral basis generator. In this chapter we develop the theory required to state the method and prove its validity.

We will work actually in a slightly more general situation. Let K be the field of fractions of a principal ideal domain $\mathcal{O}_K$. Let L be a separable extension of K and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L. Under these conditions, we will say that L/K is a **Hermite extension of fields** with rings of integers $\mathcal{O}_L/\mathcal{O}_K$. The notions concerning the associated order in Section 1.5 are valid in this case. Examples of Hermite extensions include extensions of p-adic fields and extensions of number fields where the ground field is of class number 1. The reason of this name is that in this case $\mathcal{O}_K$ is a Hermite ring in the sense of Kaplansky:

Definition 2.1. *A commutative ring R is Hermite if for every pair of elements $a, b \in R$ there is an unimodular matrix $Q \in \mathcal{M}_2(R)$ and an element $d \in R$ such that*

$$Q\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

This property is the key fact in order to establish the reduction method (see [Kap49, Theorem 3.5]).

Indeed, the idea behind the reduction method is that of the theory of linear representations: as the structure of a group (or more generally, an algebra) is in general not easy to determine, we embed it in a space of matrices, where we have the power of linear algebra at our disposal. Following this idea, for an H-Galois Hermite extension L/K of fields, we define the matrix of the action $M(H,L) \in \mathcal{M}_{n^2 \times n}(K)$, which encodes full information about the action (see Definition 2.4). But $M(H,L)$ can be used to test membership to $\mathfrak{A}_H$ for the elements of H (see Proposition 2.11). Then, $M(H,L)$ is reduced to a square $n \times n$ matrix and *preserving its integrality*, that is, by multiplication with a unimodular matrix, which is possible since $\mathcal{O}_K$ is a Hermite ring, and the inverse of the resulting matrix gives a basis of the associated order (see Theorem 2.25).

Using the matrix of the action, we are also able to give a characterization for the freeness of $\mathcal{O}_L$ in terms of the matrix of the action. This is not constructive, however, as it tells whether or not a given element β of $\mathcal{O}_L$ is normal integral basis generator. Then, in concrete examples we must find manually a concrete element that satisfies the required property.

2.1 Linear representation associated to a Hopf Galois structure

In this section we will see the action of a Hopf Galois structure as a linear representation of its Hopf algebra as endomorphisms of the top field fixing the ground field. Its definition generalizes the one of the representation of the Galois group of a Galois extension by automorphisms.

Namely, let L/K be a finite extension and let G be a group that acts on L by automorphisms. We look for an equivalent condition to L/K being Galois with Galois group G in such a way that this condition involves Hopf algebras. There is a natural group representation of G

$$\begin{array}{rccl} \rho_G\colon & G & \longrightarrow & \mathrm{Aut}_K(L) \\ & \sigma & \longmapsto & y \mapsto \sigma(y). \end{array}$$

Now, we can extend this map by K-linearity, and since linear combinations of automorphisms are in general endomorphisms, we obtain

$$\begin{array}{rccl} \rho_{K[G]}\colon & K[G] & \longrightarrow & \mathrm{End}_K(L) \\ & \sum_{\sigma\in G} a_\sigma\sigma & \longmapsto & y \mapsto \sum_{\sigma\in G} a_\sigma\sigma(y), \end{array}$$

which is a linear representation of the K-group algebra $K[G]$.

Let us consider the regular representation of L as K-vector space

$$\begin{array}{rccl} 1\colon & L & \longrightarrow & \mathrm{End}_K(L) \\ & x & \longmapsto & y \mapsto xy. \end{array}$$

Then, we can combine it with ρ_G to form a canonical map

$$(1,\rho_{K[G]})\colon L\otimes_K K[G] \longrightarrow \mathrm{End}_K(L)$$

defined by sending each $x\otimes\sigma$ to the endomorphism $y \longmapsto x\sigma(y)$ for $\sigma\in G$ and extended by K-linearity. But this map turns out to be the map j of Theorem 1.6, so L/K is Galois with group G if and only if $(1,\rho_{K[G]})$ is bijective. In such case, this representation involves also the classical Galois action in its definition.

Now, the K-group algebra $K[G]$ and the Galois action is nothing but a Hopf Galois structure of the Galois extension L/K, and as usual in Hopf Galois theory, we shall replace it by an arbitrary one. Let L/K be a finite extension and assume that H is a K-Hopf algebra that endows L with left H-module algebra structure. Similarly we have a linear representation

$$\begin{array}{rccl} \rho_H\colon & H & \longrightarrow & \mathrm{End}_K(L) \\ & h & \longmapsto & x \mapsto h\cdot x \end{array}$$

of the K-Hopf algebra H. Again, we can construct a canonical map

$$(1,\rho_H)\colon L\otimes_K H \longrightarrow \mathrm{End}_K(L)$$

defined by sending each $x\otimes h\in L\otimes_K H$ to the endomorphism $y\longmapsto x(h\cdot y)$ which is the map j of Definition 1.7. Then, L/K is H-Galois if and only if $(1,\rho_H)$ is bijective. In such case, ρ_H is an object that encodes both the K-Hopf algebra H and the Hopf action of H on L.

Example 2.2. We regard the introductory example of [GP87] with the perspective of linear representations. We consider the extension $\mathbb{Q}(\omega)/\mathbb{Q}$, where $\omega = \sqrt[3]{2}$. We call $L = \mathbb{Q}(\omega)$ By the reference above, this extension has a unique Hopf Galois structure, which is the K-Hopf algebra

$$H = \mathbb{Q}(c,s)/\langle 3s^2 + c^2 - 1_H, (2c+1_H)s, (2c+1_H)(c-1_H)\rangle$$

whose comultiplication and coinverse maps are given by

$$\Delta(c) = c \otimes c - 3s \otimes s, \quad \Delta(s) = c \otimes s + s \otimes c,$$

$$\epsilon(c) = 1_H, \quad \epsilon(s) = 0,$$

together with the action of H over L defined as

$$\begin{aligned} 1_H \cdot 1 = 1, \quad 1_H \cdot \omega = \omega, \quad 1_H \cdot \omega^2 = \omega^2, \\ c \cdot 1 = 1, \quad c \cdot \omega = -\frac{1}{2}\omega, \quad c \cdot \omega^2 = -\frac{1}{2}\omega^2, \\ s \cdot 1 = 0, \quad s \cdot \omega = \frac{1}{2}\omega, \quad s \cdot \omega^2 = -\frac{1}{2}\omega^2. \end{aligned} \tag{2.1}$$

This determines completely the action because a $\mathbb{Q}$-basis of H is given by $\{1_H, c, s\}$. Then, the linear representation that defines the Hopf Galois structure $(H, \cdot)$ is the map $\rho_H \colon H \longrightarrow \mathrm{End}_{\mathbb{Q}}(L)$ defined by $\rho_H(h)(\omega^i) = h \cdot \omega^i$ for every $h \in H$. Note that with this approach c and s are symbols while $\rho_H(c)$ and $\rho_H(s)$ are endomorphisms of L, which in [GP87] are called c and s. Thus, in this example we can see ρ_H as a representation of H as an algebra of endomorphisms. Since L/K is H-Galois, $(1, \rho_H) \colon L \otimes_{\mathbb{Q}} H \longrightarrow \mathrm{End}_{\mathbb{Q}}(L)$ is an isomorphism and in particular ρ_H is a monomorphism, so the Hopf Galois condition for $L/\mathbb{Q}$ means that we can identify uniquely the symbols with the endomorphisms by means of ρ_H.

2.2 From linear maps to matrices

Let L/K be a Hermite H-Galois extension. As the linear representation $\rho_H \colon H \longrightarrow \mathrm{End}_K(L)$ defines completely the Hopf Galois structure $(H, \cdot)$, we can use it to determine the associated order $\mathfrak{A}_H$. To this end, we fix an integral basis of L and by executing a change of bases of ρ_H as linear map, we transform a basis of H into a basis of $\mathfrak{A}_H$. This procedure is called the reduction method. In order to carry out this transformation, we work with the matrix of ρ_H, and this is what we call the matrix of the action.

Although the computation of the associated order only makes sense with Hermite extensions, the definition of matrix of the action is valid for extensions of arbitrary fields. Thus, we take L/K an H-Galois extension of fields. Let us fix a K-basis $W = \{w_i\}_{i=1}^n$ of H and a K-basis $B = \{\gamma_j\}_{j=1}^n$ of L. The matrix of the action is often deduced from a more tractable matrix, which we call the Gram matrix.

Definition 2.3. *The **Gram matrix** of the Hopf Galois structure H is defined as the matrix*

$$G(H_W, L_B) = \begin{pmatrix} w_1 \cdot \gamma_1 & w_1 \cdot \gamma_2 & \cdots & w_1 \cdot \gamma_n \\ w_2 \cdot \gamma_1 & w_2 \cdot \gamma_2 & \cdots & w_2 \cdot \gamma_n \\ \vdots & \vdots & \vdots & \vdots \\ w_n \cdot \gamma_1 & w_n \cdot \gamma_2 & \cdots & w_n \cdot \gamma_n \end{pmatrix} \in \mathcal{M}_n(L).$$

We have chosen this name in an analogy to the case of the Gram matrix of a scalar product. Of course, in this case the action of H on L is not a scalar product, but we extend the terminology to this situation. When the bases of H and L are implicit in the context, we will write $G(H,L)$ instead of $G(H_W, L_B)$.

The matrix of the action arises from replacing the entries of $G(H_W, L_B)$ by row vectors of coordinates and taking the transpose. Namely:

Definition 2.4. *Given $1 \leq j \leq n$, we denote*

$$M_j(H,L) = \begin{pmatrix} | & | & \dots & | \\ w_1 \cdot \gamma_j & w_2 \cdot \gamma_j & \dots & w_n \cdot \gamma_j \\ | & | & \dots & | \end{pmatrix} \in \mathcal{M}_{n\times n}(K),$$

*that is, $M_j(H,L)$ is the matrix whose i-th column is the column vector of the coordinates of $w_i \cdot \gamma_j$ with respect to the basis B. Then, the **matrix of the action** is defined as:*

$$M(H,L) = \left(\begin{array}{c} M_1(H,L) \\ \hline \cdots \\ \hline M_n(H,L) \end{array}\right) \in \mathcal{M}_{n^2\times n}(K).$$

As in the case of the Gram matrix, we will normally omit the explicit mention to the bases W and B. Let us fix a notation for the entries of $M(H,L)$. For each $1 \leq j \leq n$, the element $w_i \cdot \gamma_j$ belongs to L, so it has an expression as vector of coordinates with respect to the basis B

$$w_i \cdot \gamma_j = \sum_{k=1}^{n} m_{ij}^{(k)}(H,L)\gamma_k, \tag{2.2}$$

where $m_{ij}^{(k)}(H,L) \in K$ for every $1 \leq k \leq n$. Then, the j-th block of $M(H,L)$ is the matrix

$$M_j(H,L) = (m_{ij}^{(k)}(H,L))_{k,i=1}^{n},$$

where k increases from top to bottom and i does from left to right. Hence, $M(H,L)$ can be expressed as

$$M(H,L) = \left(\begin{array}{ccc} m_{11}^{(1)}(H,L) & \cdots & m_{n1}^{(1)}(H,L) \\ \vdots & \ddots & \vdots \\ m_{11}^{(n)}(H,L) & \cdots & m_{n1}^{(n)}(H,L) \\ \hline \vdots & \vdots & \vdots \\ \hline m_{1n}^{(1)}(H,L) & \cdots & m_{nn}^{(1)}(H,L) \\ \vdots & \ddots & \vdots \\ m_{1n}^{(n)}(H,L) & \cdots & m_{nn}^{(n)}(H,L) \end{array}\right).$$

Let us analyze what the definition of $M(H,L)$ means. The definition above focuses on the blocks of the matrix, but we can also look at its columns. Let us fix the canonical basis $\{E_{ij}\}_{i,j=1}^{n}$ of $\mathcal{M}_n(K)$, given by $E_{ij} = (\delta_{ik}\delta_{jl})_{k,l=1}^{n}$ for every $1 \leq i, j \leq n$, where δ_{ab} is the Kronecker delta. That is, E_{ij} is the matrix with 1 in its (i,j)-th entry and 0 in the other ones. We also fix the canonical basis $\{e_i\}_{i=1}^{n^2}$ of K^{n^2}. Let us define

$$\begin{array}{rccc} \varphi\colon & \mathcal{M}_n(K) & \longrightarrow & K^{n^2} \\ & E_{ij} & \longmapsto & e_{i+(j-1)n} \end{array}.$$

Since φ sends a basis to a basis, it is an isomorphism of K-vector spaces.

Proposition 2.5. *If we identify endomorphisms with their matrices, the matrix of the action may be described as*

$$M(H,L) = \begin{pmatrix} | & | & \cdots & | \\ \varphi(\rho_H(w_1)) & \varphi(\rho_H(w_2)) & \dots & \varphi(\rho_H(w_n)) \\ | & | & \cdots & | \end{pmatrix} \in \mathcal{M}_{n^2\times n}(K).$$

Proof. It is enough to check that for every $1 \le i \le n$ the matrix of $\rho_H(w_i)$ as endomorphism is $(m_{ij}^{(k)}(H,L))_{j,k=1}^n$, where j increases from top to bottom and k does from left to right. Indeed,

$$\rho_H(w_i)(\gamma_j) = w_i \cdot \gamma_j = \sum_{k=1}^n m_{ij}^{(k)}(H,L)\gamma_k,$$

so for every $1 \le k \le n$, the k-th column of the matrix $\rho_H(w_i)$ is

$$(m_{i1}^{(k)}(H,L) \quad \cdots \quad m_{in}^{(k)}(H,L))^t.$$

□

This suggests the interpretation of the matrix of the action as the matrix of the linear map ρ_H. Let $\Phi = \{\varphi_i\}_{i=1}^{n^2}$ defined as follows: For every $1 \le i \le n^2$, there are $1 \le k, j \le n$ such that $i = k + (j-1)n$. Then, let φ_i be the map that sends γ_j to γ_k and the other γ_l to 0. For simplicity, we call $\varphi_i = \varphi_{kj}$. Under this notation, $\varphi_{kj}(\gamma_l) = \delta_{jl}\gamma_k$, where δ_{jl} is the Kronecker delta. The matrix of φ_{kj} as linear map is the $n \times n$ matrix whose (k,j)-th element is 1 and the other ones are 0, that is, E_{kj}.

Proposition 2.6. *The matrix of the action $M(H_W, L_B)$ is the matrix of the linear map $\rho_H\colon H \longrightarrow \operatorname{End}_K(L)$ when we consider the basis W in H and the basis Φ in $\operatorname{End}_K(L)$.*

Proof. By definition, the i-th column of the matrix of ρ_H is the column vector of coordinates of $\rho_H(w_i)$ with respect to the basis Φ. Let us compute this vector. For every $1 \le l \le n$, we have

$$\left(\sum_{k,j=1}^n m_{ij}^{(k)}(H,L)\varphi_{kj}\right)(\gamma_l) = \sum_{k=1}^n m_{il}^{(k)}(H,L)\gamma_k = w_i \cdot \gamma_l = \rho_H(w_i)(\gamma_l).$$

Thus, we have the equality of endomorphisms

$$\rho_H(w_i) = \sum_{k,j=1}^n m_{ij}^{(k)}(H,L)\varphi_{kj}$$

for every $1 \le i \le n$.

Hence, the i-th column of the matrix of ρ_H is

$$\left(m_{i1}^{(1)}(H,L) \quad \cdots \quad m_{i1}^{(n)}(H,L) \quad \cdots \quad m_{in}^{(1)}(H,L) \quad \cdots \quad m_{in}^{(n)}(H,L)\right)^t,$$

which coincides with the i-th column of $M(H,L)$. □

Example 2.7. We consider the extension of Example 2.2. We fix the K-basis $\{1_H, c, s\}$ of H and the K-basis $\{1, \omega, \omega^2\}$ of L. With these choices, we can use the expressions in (2.1) to find that the Gram matrix of the Hopf Galois structure is

$$G(H,L) = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & -\frac{1}{2}\omega & -\frac{1}{2}\omega^2 \\ 0 & \frac{1}{2}\omega & -\frac{1}{2}\omega^2 \end{pmatrix}$$

and the matrix of the action of H on L is given by

$$M(H,L) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Identifying endomorphisms with their matrices,

$$\rho_H(1_H) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_H(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 \\ 0 & 0 & -\frac{1}{2} \end{pmatrix}, \quad \rho_H(s) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & -\frac{1}{2} \end{pmatrix},$$

and when we apply $\varphi \colon \mathcal{M}_3(\mathbb{Q}) \longrightarrow \mathbb{Q}^9$, we obtain indeed the columns of the matrix of the action.

The definition of $M(H,L)$ does not use the property that L/K is H-Galois. Actually, to define the matrix of the action it is enough to assume that L has left H-module structure. However, the H-Galois condition is used in the following:

Corollary 2.8. *The matrix $M(H,L)$ has rank n.*

Proof. Since L/K is H-Galois, by definition the map $(1, \rho_H) \colon L \otimes_K H \longrightarrow \mathrm{End}_K(L)$ is bijective. Moreover, the restriction of this map to H coincides with ρ_H. Hence, ρ_H is injective, and then its matrix as linear map, which is $M(H,L)$, has maximal rank n. □

2.2.1 Change of bases

Next, we consider the dependence of $M(H_W, L_B)$ on the K-bases of W and B of H and L. We will study successively the changes of the basis of H and the basis of L. There is also a formula for the simultaneous change of the two bases, but we will not make it explicit because it is obtained by composing the other two changes.

Change of the basis of H

It is the most simple to express and, for this reason, the first we work with. We consider K-bases $W = \{w_i\}_{i=1}^n$, $W' = \{w_i'\}_{i=1}^n$ of H and a K-basis $B = \{\gamma_j\}_{j=1}^n$ of L. We want to study the relation between the entries of the matrices $M(H_W, L_B)$ and $M(H_{W'}, L_B)$.

Proposition 2.9. *Let $P_W^{W'}$ be the matrix of change of bases from the basis W to the basis W'. Given $1 \leq j \leq n$,*

$$M_j(H_{W'}, L_B) = M_j(H_W, L_B)P_W^{W'}.$$

Proof. Let us fix $1 \leq i \leq n$. By definition of matrix of the action, we have

$$w_i' \cdot \gamma_j = \sum_{k=1}^{n} m_{ij}^{(k)}(H_{W'}, L_B)\gamma_k.$$

Now, call $P_W^{W'} = (a_{ij})_{i,j=1}^n$. Then,

$$w_i' = \sum_{l=1}^{n} a_{li} w_l,$$

so we compute

$$\begin{aligned} w_i' \cdot \gamma_j &= \sum_{l=1}^{n} a_{li} w_l \cdot \gamma_j \\ &= \sum_{l=1}^{n} a_{li} \sum_{k=1}^{n} m_{lj}^{(k)}(H_W, L_B)\gamma_k \\ &= \sum_{k=1}^{n} \left(\sum_{l=1}^{n} a_{li} m_{lj}^{(k)}(H_W, L_B) \right) \gamma_k. \end{aligned}$$

The uniqueness of coordinates yields

$$m_{ij}^{(k)}(H_{W'}, L_B) = \sum_{l=1}^{n} m_{lj}^{(k)}(H_W, L_B) a_{li}.$$

Since i and k are arbitrary, we obtain the desired expression. □

Change of the basis of L

When we change the basis of L, the situation is a bit trickier, since it affects not only the entries of the matrix but also the basis from which we write the vectors. However, we can still represent the relation with a matrix expression, in this case involving the columns of the matrices rather than the blocks. We consider a K-basis $W = \{w_i\}_{i=1}^n$ of H and K-bases $B = \{\gamma_j\}_{j=1}^n$ and $B' = \{\gamma_j'\}_{j=1}^n$ of L. Call $w_i(B)$ (resp. $w_i(B')$) the representing matrix of w_i by ρ_H when we consider matrices with coordinates with respect to B (resp. B'). Note that $w_i(B)$ (resp. $w_i(B')$) is the matrix of the linear map $\rho_H(w_i) \colon L \longrightarrow L$ where we fix the basis B (resp. B') in both domain and codomain. By the general change basis formula for linear maps, we have

$$w_i(B') = P^{-1} w_i(B) P,$$

where $P = P_B^{B'}$ is the matrix of change of bases from the basis B to the basis B'.

There is a more simple formula for the change of basis of L in which we use the Gram matrix instead of the matrix of the action, and this is the one that actually will be useful in practice.

Proposition 2.10. *With the previous notation,*

$$G(H, L_{B'}) = G(H, L_B)P_B^{B'},$$

where in the product of the right side member we consider $P_B^{B'}$ as a matrix with coefficients in L.

Proof. Let us write $P_B^{B'} = (d_{ij})_{i,j=1}^n$ and fix $1 \leq i, j \leq n$. Then, $\gamma_j' = \sum_{k=1}^n d_{kj}\gamma_k$, so the (i, j)-th entry of $G(H_W, L_{B'})$ can be described as

$$w_i \cdot \gamma_j' = \sum_{k=1}^n d_{kj} w_i \cdot \gamma_k.$$

For each k, $w_i \cdot \gamma_k$ is the (i, k)-th entry of $G(H_W, L_B)$ and d_{kj} is the (k, j)-th entry of $P_B^{B'}$. Therefore, the expression above is also the (i, j)-entry of $G(H, L_B)P_B^{B'}$, proving the statement. □

Although theoretically the problem is solved, in practice there is an extra step. If one knows $G(H, L_B)$ and applies the formula above, then one obtains the entries of $G(H, L_{B'})$ in terms of the basis B. However, in order to construct the matrix of the action $M(H, L_{B'})$, we need to write the entries of $G(H, L_{B'})$ in terms of the basis B'. Hence, we need to change each entry from B to B', for instance applying the matrix $P_{B'}^B$ to its vector of coordinates with respect to B.

2.3 Reducing the matrix of the action

Let L/K be an H-Galois Hermite extension. We can interpret the definition of $\mathfrak{A}_H$ in terms of ρ_H. Concretely, given $h \in H$, we know that $h \in \mathfrak{A}_H$ if and only if $h \cdot x \in \mathcal{O}_L$ for every $x \in \mathcal{O}_L$. This means that $h \in \mathfrak{A}_H$ if and only if the K-endomorphism $\rho_H(h) \colon L \longrightarrow L$ restricts well to $\mathcal{O}_L$, that is, $\rho_H(h) \in \mathrm{End}_{\mathcal{O}_K}(\mathcal{O}_L)$. Now, since $M(H, L)$ is the matrix of ρ_H, we can rewrite this condition in terms of coordinates. Let us fix again bases $W = \{w_i\}_{i=1}^n$ of H and $B = \{\gamma_j\}_{j=1}^n$ of L.

Proposition 2.11. *Assume that B is an integral basis of L. Given $h = \sum_{i=1}^n h_i w_i \in H$, $h \in \mathfrak{A}_H$ if and only if*

$$M(H, L)\begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} \in \mathcal{O}_K^{n^2}, \tag{2.3}$$

that is, $M(H, L)$ takes the column vector of the coordinates of h with respect to B to a vector of n^2 integer coordinates in K.

Remark 2.12. *Since L/K is a Hermite extension, $\mathcal{O}_K$ is a PID and then $\mathcal{O}_L$ is $\mathcal{O}_K$-free (see Section 1.5), so an integral basis exists.*

What Proposition 2.11 means is that $M(H, L)$ filters the elements of the associated order among the ones in H. Now, we regard condition (2.3) as a family of systems of n^2 linear equations, where the matrix of coefficients is $M(H, L)$, the indeterminates are the coordinates $h_1, ..., h_n$, and the independent terms run through $\mathcal{O}_K^{n^2}$. Under this interpretation, the elements of $\mathfrak{A}_H$ are the vectors $h \in H$ whose vector of coordinates $(h_1, ..., h_n)$ with respect to W is a solution of a system of equations as before with independent term a vector of integers in K.

2.3.1 Reduced matrices

To solve a system of equations as in (2.3), we can apply linear transformations in $M(H, L)$ to reduce it to an $n \times n$ matrix, which will be invertible since $M(H, L)$ has rank n. However, the independent term of the new system of equations should have integer components in K so that the reduced matrix also filters the elements of the associated order. Hence, we must use only elementary transformations f such that both f and f^{-1} preserve $\mathcal{O}_K$. Such transformations will be called **integral linear transformations**.

Even though we need transformations that preserve integrality, the matrix $M(H, L)$ does not have in general coefficients in $\mathcal{O}_K$. Both in theory and practice it will be more convenient to work with a matrix which plays the role of $M(H, L)$ but with integral coefficients. To this end, we introduce the notions of content and primitive part classically used for polynomials.

Definition 2.13. *Let $\mathcal{O}_K$ be a PID with fraction field K. Let $A \in \mathcal{M}_n(K)$.*

1. *The content of A is defined as $\operatorname{cont}(A) = \frac{d}{a}$, where $a \in \mathcal{O}_K$ is any element that satisfies $aA \in \mathcal{M}_n(\mathcal{O}_K)$ and d is the greatest common divisor of the coefficients of aA.*
2. *The primitive part of A is $pp(A) := \frac{A}{\operatorname{cont}(A)}$.*
3. *We say that A is primitive if $A = pp(A)$, that is, $\operatorname{cont}(A) = 1$.*

Remark 2.14. The definition of content does not depend on the choice of a. Indeed, since $\mathcal{O}_K$ is an UFD, fractions in K have a unique irreducible expression, up to units. Then, if l is the least common multiple of the denominators of the entries of A in irreducible form, $\frac{d}{a} = l$ independently on the choice of a.

In similarity with the case of polynomials, every matrix with coefficients in the fraction field of a unique factorization domain may be written as the product of its content and its primitive part. Moreover, the primitive part of a matrix in K has coefficients in $\mathcal{O}_K$. If $K = \mathbb{Q}$ (which is the fraction field of the principal ideal domain $\mathbb{Z}$), decomposing $M(H, L)$ as the product of its content and primitive part is to drop the common denominators of its entries out of $M(H, L)$.

Let us go back to the problem of reducing $M(H, L)$. The matrix associated to an integral linear transformation is an invertible element in $\mathcal{M}_n(\mathcal{O}_K)$ (i.e, an element of $\mathrm{GL}_n(\mathcal{O}_K)$). Such matrices are called unimodular. Hence, the concatenation of integral linear transformations may be represented by a product of elementary unimodular matrices, which is a unimodular matrix. Thus, we would like to find a unimodular matrix U such that $UM(H, L)$ is essentially a $n \times n$ matrix, meaning that all its $n \times n$ blocks are the 0 matrix except the first one. Actually, this is always possible.

Theorem 2.15. *Let $\mathcal{O}_K$ be a PID with fraction field K. Let $m \geq n$ and let $A \in \mathcal{M}_{m\times n}(K)$ be a matrix of rank n. Then there is a matrix $D \in \mathcal{M}_n(K)$ and a unimodular matrix $U \in \mathrm{GL}_m(\mathcal{O}_K)$ with the property that*

$$UA = \begin{pmatrix} D \\ O \end{pmatrix},$$

where O is the zero matrix of $\mathcal{M}_{(m-n)\times n}(K)$.

Proof. Since $\mathcal{O}_K$ is a PID, it is a Hermite ring, so we can apply [Kap49, Theorem 3.5] to $\mathrm{pp}(A) \in \mathcal{M}_{m\times n}(\mathcal{O}_K)$, giving the existence of a matrix $\Gamma \in \mathcal{M}_n(\mathcal{O}_K)$ and a unimodular matrix $U \in \mathrm{GL}_n(\mathcal{O}_K)$ such that

$$UA = \begin{pmatrix} \Gamma \\ \hline O \end{pmatrix}.$$

Then, U and $D = d\Gamma$ satisfy the equality of the statement. □

Remark 2.16. *The matrix given by [Kap49, Theorem 3.5] is triangular, but this fact is ignored in our exposition because it is completely useless for our purposes. Besides, changing conveniently the unimodular matrix U can give any type of square matrix D.*

Definition 2.17. *A matrix D as in the previous statement is called a* ***reduced matrix of*** *A.*

Clearly, a reduced matrix is not unique: left multiplication of a reduced matrix by any unimodular matrix gives another reduced matrix.

The utility of the reduced matrix to compute associated orders falls on the fact that it also tests membership of the associated order for elements in H. The key fact is that the linear transformations involved preserve $\mathcal{O}_K$, that is, the reducing matrix U is unimodular.

Corollary 2.18. *Assume that B is an integral basis and let D be a reduced matrix of $M(H,L)$. Given $h = \sum_{i=1}^n h_i w_i \in H$, $h \in \mathfrak{A}_H$ if and only if*

$$D \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} \in \mathcal{O}_K^n.$$

Proof. We know that $h \in \mathfrak{A}_H$ if and only if

$$M(H,L) \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} \in \mathcal{O}_K^{n^2}. \tag{2.4}$$

By the definition of reduced matrix, there is a unimodular matrix U such that

$$UM(H,L) = \begin{pmatrix} D \\ \hline O \end{pmatrix}.$$

Since U is unimodular, it sends $\mathcal{O}_K^{n^2}$ to itself. Thus, applying U to (2.4) yields that $h \in \mathfrak{A}_H$ if and only if

$$\begin{pmatrix} D \\ \hline O \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} \in \mathcal{O}_K^{n^2}.$$

This is clearly equivalent to the condition in the statement. □

2.3.2 The Hermite normal form

The definition of the Hermite normal form of a matrix is well known for matrices with coefficients in $\mathbb{Z}$. As we work with matrices with coefficients in an arbitrary PID, we must use a more general definition, given in [AW92, Chapter 5, Definition 2.8]. First we review a couple of notions.

Definition 2.19. *Let R be a PID.*

1. *A complete set of non-associates in R is a subset $P \subset R$ such that for every non-zero $a \in R$ there is a unique $b \in P$ and a unit $u \in R^*$ such that $b = au$ (that is, every element of R has a unique associate in P).*

2. *A complete set of residues modulo an element $a \in R$ is a subset of R that contains a unique element in each coset modulo a.*

Now, the Hermite normal form of a matrix with coefficients in a PID is defined as follows.

Definition 2.20. *Let R be a PID, P a complete set of non-associates in R, and for every $a \in R$, let $P(a)$ be a complete set of residues modulo a. Let $A = (a_{ij}) \in \mathcal{M}_{m\times n}(R)$ be a non-zero matrix. We will say that M is in Hermite normal form if there exists an integer $1 \leq r \leq m$ such that:*

1. *Given $1 \leq i \leq r$, the i-th row of M is non-zero, and given $r+1 \leq i \leq m$, the i-th row of M is zero.*

2. *There is a sequence of integer numbers $1 \leq n_1 < \cdots < n_r \leq m$ such that for every $1 \leq i \leq r$:*

   - *Given $j < n_i$, $a_{ij} = 0$.*
   - *$a_{i,n_i} \in P - \{0\}$.*
   - *Given $1 \leq j < i$, $a_{j,n_i} \in P(a_{i,n_i})$*

Example 2.21. 1. If $R = \mathbb{Z}$, a complete set of non-associates is $P = \mathbb{Z}_{\geq 0}$ and for every positive integer a, a complete set of residues modulo a is $\{x \in \mathbb{Z} \mid \lceil -\frac{|a|}{2} \rceil < x \leq \lfloor \frac{|a|}{2} \rfloor\}$.

2. If $R = \mathbb{Z}_p$ for a prime number p, a complete set of non-associates is $P = \{p^n\}_{n=0}^{\infty}$. If $m \geq n$ is of rank n and $A \in \mathcal{M}_{m\times n}(\mathcal{O}_K)$, the elements of the diagonal in the Hermite normal form are non-negative powers of p. If an element above the diagonal also belongs to $\mathbb{Q}$, we will choose the element in its coset whose usual absolute value is strictly less than $\frac{p}{2}$.

The following result assures the existence and the uniqueness of the Hermite normal form of a matrix.

Theorem 2.22 (Hermite normal form)**.** *Let R be a PID, let P be a complete set of non-associates in R, and for every $a \in R$, let $P(a)$ be a complete set of residues modulo a. Let $A \in \mathcal{M}_{m\times n}(R)$ a matrix of rank n. Then:*

1. *There exists an $m \times m$ unimodular matrix $U \in \mathrm{GL}_m(R)$, such that UA is a matrix in Hermite normal form. If in addition R is euclidean, U can be written as a product of elementary matrices with coefficients in R.*

2. *The Hermite normal form of A is unique.*

Proof. See [AW92, Chapter 5, Theorems 2.9 and 2.13]. □

Note that the Hermite normal form of a matrix is unique because of the choice of a complete set of residues modulo every element of the diagonal. If we do not take any such system, then there exist still echelon matrices that satisfy Definition 2.20 except the last point in 2. For simplicity, we shall admit all of them as Hermite normal forms of the original matrix. Consequently, we will usually think of *a Hermite normal form* of a given matrix. Another convention we will follow is that we will consider the Hermite normal form as the matrix resulting from deleting the zero rows from the original Hermite normal form.

We have defined the Hermite normal form of a matrix A when the coefficients in A belong to a PID. However, the matrix $M(H,L)$ has coefficients in K and they need not to lie in $\mathcal{O}_K$. To be able to talk about the Hermite normal form of $M(H,L)$, we use the content and the primitive part.

Definition 2.23. *Let $d = \operatorname{cont}(M(H,L))$ and $M = \operatorname{pp}(M(H,L))$. The Hermite normal form of $M(H,L)$ is defined as the matrix $d\Gamma$, where Γ is the Hermite normal form of M.*

Example 2.24. *Consider again Example 2.2. Since $\mathbb{Z}$ is a PID, $L/\mathbb{Q}$ is a Hermite extension. We computed $M(H,L)$ in Example 2.7. In this case, $\operatorname{cont}(M(H,L)) = \frac{1}{2}$ and*

$$\operatorname{pp}(M(H,L)) = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 2 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 2 & -1 & -1 \end{pmatrix}.$$

Now, $U\operatorname{pp}(M(H,L)) = \begin{pmatrix} \Gamma \\ O \end{pmatrix}$, where

$$U = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad \Gamma = \begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & -1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Then Γ is the Hermite normal form of the principal part of $M(H,L)$, and consequently, the Hermite normal form of $M(H,L)$ is

$$D = \frac{1}{2}\begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & -1 \\ 0 & 0 & 2 \end{pmatrix}.$$

This is a reduced matrix of $M(H,L)$. Another reduced matrix arises simply by deleting the zero rows of $M(H,L)$, that is,

$$D' = \frac{1}{2}\begin{pmatrix} 2 & 2 & 0 \\ 2 & -1 & 1 \\ 2 & -1 & -1 \end{pmatrix}.$$

2.4 Determination of a basis

Recall that an element $h = \sum_{i=1}^{n} h_i w_i \in H$ belongs to $\mathfrak{A}_H$ if and only if its vector of coordinates $(h_1, ..., h_n)$ with respect to W is a solution of any system of equations with matrix of coefficients $M(H,L)$ and independent term any vector with components in $\mathcal{O}_K$. If $U \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ is a unimodular matrix that reduces $M(H,L)$ to a reduced matrix D, then multiplication by U yields a system with only n equations and the same solutions. Moreover, the matrix of coefficients of this new system is D, which is invertible, and its inverse gives the solutions. Explicitly:

Theorem 2.25. *Let L/K be a degree n Hermite H-Galois extension of fields, $W = \{w_i\}_{i=1}^{n}$ a K-basis of H and $B = \{\gamma_j\}_{j=1}^{n}$ an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. Let D be a reduced matrix of $M(H,L)$ and call $D^{-1} = (d_{ij})_{i,j=1}^{n}$. The elements*

$$v_i = \sum_{l=1}^{n} d_{li} w_l,\ 1 \leq i \leq n$$

form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$. Moreover, if we identify each v_i with the column vector of its coordinates with respect to W, the action of this basis on $\mathcal{O}_L$ can be expressed as

$$v_i \cdot \gamma_j = M_j(H,L) v_i,$$

with coordinates with respect to B.

Proof. Let $h = \sum_{l=1}^{n} h_l w_l \in H$, with $h_i \in K$. By Corollary 2.18, $h \in \mathfrak{A}_H$ if and only if there exist elements $c_1, ..., c_n \in \mathcal{O}_K$ such that

$$D\begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

Multiplying by D^{-1} at both sides, this is equivalent to

$$\begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix} = \begin{pmatrix} d_{11} & \cdots & d_{1n} \\ \vdots & \ddots & \vdots \\ d_{n1} & \cdots & d_{nn} \end{pmatrix}\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix},$$

that is,

$$h_l = \sum_{i=1}^{n} d_{li} c_i,\ 1 \leq l \leq n.$$

Hence, $h \in \mathfrak{A}_H$ if and only if there exist $c_1, ..., c_n \in \mathcal{O}_K$ such that

$$h = \sum_{l=1}^{n}\sum_{i=1}^{n} d_{li} c_i w_l = \sum_{i=1}^{n} c_i \left(\sum_{l=1}^{n} d_{li} w_l\right) = \sum_{i=1} c_i v_i.$$

The last member clearly belongs to $\langle v_1, ..., v_n\rangle_{\mathcal{O}_K}$. Hence, $\{v_i\}_{i=1}^n$ is an $\mathcal{O}_K$-system of generators of $\mathfrak{A}_H$. Now, it is K-linearly independent because $\{w_i\}_{i=1}^n$ is a K-basis and D^{-1} is invertible, so it is also $\mathcal{O}_K$-linearly independent and hence an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

The action of this $\mathcal{O}_K$-basis on $\mathcal{O}_L$ is given by

$$v_i \cdot \gamma_j = \sum_{l=1}^n d_{li} w_l \cdot \gamma_j = \sum_{k=1}^n \left(\sum_{l=1}^n d_{li} m_{lj}^{(k)}(H, L) \right) \gamma_k.$$

□

The set $V = \{v_i\}_{i=1}^n$ determined in the previous theorem is in particular a K-basis of H, and the matrix D^{-1} is the matrix of the change of K-basis from W to V (in the notation of Proposition 2.9, $D^{-1} = P_W^V$). This is why its columns give the coordinates of the new basis with respect to W. So the reduction method finds a matrix of change of basis that carries W to a K-basis of H which in addition is an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

Example 2.26. In the situation of Example 2.2, we can apply Theorem 2.25 because $\{1, \omega, \omega^2\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_L$, as $\mathcal{O}_L = \mathbb{Z}[\omega]$.

The Hermite normal form of $M(H, L)$, computed in Example 2.24, has inverse

$$D^{-1} = \frac{1}{3}\begin{pmatrix} 3 & 1 & -1 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix}.$$

Then, by the theorem,

$$V = \left\{ \mathrm{Id}, \frac{\mathrm{Id} + 2c}{3}, \frac{-\mathrm{Id} + c + 3s}{3} \right\}$$

is a $\mathbb{Z}$-basis of $\mathfrak{A}_H$. Let us compute the action of this basis on $\mathcal{O}_L$. Obviously, $\mathrm{Id} \cdot \omega^i = \omega^i$ for $i \in \{1, 2, 3\}$. Regarding the other two elements,

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \implies \tfrac{\mathrm{Id}+2c}{3} \cdot 1 = 1,$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \implies \tfrac{\mathrm{Id}+2c}{3} \cdot \omega = 0,$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \implies \tfrac{\mathrm{Id}+2c}{3} \cdot \omega^2 = 0,$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} -\frac{1}{3} \\ \frac{1}{3} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \implies \tfrac{\mathrm{Id}+2c}{3} \cdot 1 = 0,$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} -\frac{1}{3} \\ \frac{1}{3} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \implies \tfrac{\mathrm{Id}+2c}{3} \cdot \omega = 0,$$

$$\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 1 & -\frac{1}{2} & -\frac{1}{2}\end{pmatrix}\begin{pmatrix}-\frac{1}{3}\\ \frac{1}{3}\\ 1\end{pmatrix} = \begin{pmatrix}0\\ 0\\ -1\end{pmatrix} \quad\implies\quad \tfrac{\mathrm{Id}+2c}{3}\cdot\omega^2 = -\omega^2.$$

Hence, the Gram matrix for this new basis is

$$G(H_V, L_B) = \begin{pmatrix}1 & \omega & \omega^2\\ 1 & 0 & 0\\ 0 & 0 & -\omega^2\end{pmatrix}.$$

On the other hand, the other reduced matrix in Example 2.24 gives rise to the basis

$$V' = \left\{\frac{\mathrm{Id}+2c}{3}, \frac{\mathrm{Id}-c+3s}{3}, \frac{\mathrm{Id}-c-3s}{3}\right\}.$$

The first element in this basis is the second element in V, and the third one is the negative of the third element in V, so we know how they act on $\mathcal{O}_L$. Let us compute the action of the remaining element:

$$\begin{pmatrix}1 & 1 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{3}\\ -\frac{1}{3}\\ 1\end{pmatrix} = \begin{pmatrix}0\\ 0\\ 0\end{pmatrix} \quad\implies\quad \tfrac{\mathrm{Id}-c+3s}{3}\cdot 1 = 0,$$

$$\begin{pmatrix}0 & 0 & 0\\ 1 & -\frac{1}{2} & \frac{1}{2}\\ 0 & 0 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{3}\\ -\frac{1}{3}\\ 1\end{pmatrix} = \begin{pmatrix}0\\ 1\\ 0\end{pmatrix} \quad\implies\quad \tfrac{\mathrm{Id}-c+3s}{3}\cdot \omega = \omega,$$

$$\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 1 & -\frac{1}{2} & -\frac{1}{2}\end{pmatrix}\begin{pmatrix}\frac{1}{3}\\ -\frac{1}{3}\\ 1\end{pmatrix} = \begin{pmatrix}0\\ 0\\ 0\end{pmatrix} \quad\implies\quad \tfrac{\mathrm{Id}-c+3s}{3}\cdot \omega^2 = 0.$$

Hence, the Gram matrix for this case is

$$G(H_{V'}, L_B) = \begin{pmatrix}1 & 0 & 0\\ 0 & \omega & 0\\ 0 & 0 & \omega^2\end{pmatrix}.$$

That is, the Gram matrix is diagonal with diagonal filled by the elements of the basis V'. In short, we say that the action of V' on L is diagonal. This implies that the elements of V' are pairwise orthogonal idempotents, as we prove below in a more general situation.

Proposition 2.27. *Let L/K be an H-Galois extension, $W = \{w_i\}_{i=1}^n$ a K-basis of H and $B = \{\gamma_j\}_{j=1}^n$ a K-basis of L. Assume that the action of W on L is diagonal. Then, the elements of W are pairwise orthogonal idempotents.*

Proof. Note that the action of W on L being diagonal means that $w_a \cdot \gamma_b = \delta_{ab}\gamma_b$ for every a and b. Let $1 \leq i, j \leq n$. Then, for every $1 \leq k \leq n$,

$$(w_i w_j)\cdot\gamma_k = w_i\cdot(w_j\cdot\gamma_k) = w_i\cdot(\delta_{jk}\gamma_k) = \delta_{jk}w_i\cdot\gamma_k = \delta_{ik}\delta_{jk}\gamma_k.$$

If $i = j$, this says that $w_i^2\cdot\gamma_k = \delta_{ik}\gamma_k = w_i\cdot\gamma_k$ for every k, and since ρ_H is injective (because L/K is H-Galois), $w_i^2 = w_i$. Otherwise, if $i \neq j$, $(w_i w_j)\cdot\gamma_k = 0$ for every k, so again the injectivity of ρ_H gives that $w_i w_j = 0$. □

In the situation of Proposition 2.27, B is a basis of eigenvectors of the action of H on L (see Section 2.6).

2.5 Freeness over the associated order

Let L/K be an H-Galois Hermite extension of fields. Let $W = \{w_i\}_{i=1}^n$ be a K-basis of H and $B = \{\gamma_j\}_{j=1}^n$ an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. In this section we discuss the problem of determining whether or not $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. For each element $\beta \in \mathcal{O}_L$, we will give a necessary and sufficient condition that tests if β is a normal integral basis generator of $\mathcal{O}_L$. The tool will be again the matrix of the action, or more precisely, the linear combination of its blocks with the coordinates of β with respect to B. This is what we will call the matrix associated to β.

2.5.1 Matrix associated to an element

Call $V = \{v_i\}_{i=1}^n$ an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$ computed by the reduction method. That is, if D is a reduced matrix of $M(H_W, L_B)$ and we call $D^{-1} = (d_{ij})_{i,j=1}^n$, then

$$v_i = \sum_{l=1}^n d_{li} w_l$$

for every $1 \leq i \leq n$.

Let $\beta \in \mathcal{O}_L$ be a potential $\mathfrak{A}_H$-generator of $\mathcal{O}_L$. Since ρ_H is injective, $\{\beta\}$ is linearly independent over $\mathfrak{A}_H$. Then, β is an $\mathfrak{A}_H$-free generator of $\mathcal{O}_L$ if and only if $\mathcal{O}_L = \mathfrak{A}_H \cdot \beta$. Thus, we want to determine a necessary and sufficient condition for the equality $\mathcal{O}_L = \mathfrak{A}_H \cdot \beta$ to hold. In general, $\mathfrak{A}_H \cdot \beta \subset \mathcal{O}_L$, and $\{v_i \cdot \beta\}_{i=1}^n$ is an $\mathcal{O}_K$-basis of $\mathfrak{A}_H \cdot \beta$. Then, the equality holds if and only if $\{v_i \cdot \beta\}_{i=1}^n$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Determining conditions under which the vectors $v_i \cdot \beta$ form a basis are closely related with the study of the matrix $M_\beta(H_V, L_B)$ whose columns are the coordinates of the elements $v_i \cdot \beta$ with respect to the basis B. Let us find its explicit form. We have

$$v_i \cdot \beta = v_i \cdot \left(\sum_{j=1}^n \beta_j \gamma_j\right) = \sum_{j=1}^n \beta_j v_i \cdot \gamma_j.$$

Recall that, by Theorem 2.25, the action of the basis V on $\mathcal{O}_L$ is given by the equalities $v_i \cdot \gamma_j = M_j(H_W, L_B) v_i$. Hence,

$$v_i \cdot \beta = \sum_{j=1}^n \beta_j M_j(H_W, L_B) v_i, \ 1 \leq i \leq n.$$

These n vectors are the columns of the matrix $M_\beta(H_V, L_B)$. Now, recall that the vectors v_i are the columns of the matrix D^{-1}. We obtain

$$M_\beta(H_V, L_B) = \sum_{j=1}^n \beta_j M_j(H_W, L_B) D^{-1}.$$

Finally, by Proposition 2.9, $M_j(H_V, L_B) = M_j(H_W, L_B) D^{-1}$ for every $1 \leq j \leq n$. Thus,

$$M_\beta(H_V, L_B) = \sum_{j=1}^n \beta_j M_j(H_V, L_B).$$

This leads us to introduce the following general notion.

Definition 2.28. *Let L/K be a degree n H-Galois extension of fields, $W = \{w_i\}_{i=1}^n$ a K-basis of H and $B = \{\gamma_j\}_{j=1}^n$ a K-basis of L. The associated matrix of an element $\beta = \sum_{j=1}^n \beta_j\gamma_j \in L$ with respect to the K-bases W and B is defined as the matrix whose columns are the coordinates of the elements $w_i \cdot \beta$ with respect to B, that is,*

$$M_\beta(H_W, L_B) := \sum_{j=1}^{n} \beta_j M_j(H_W, L_B).$$

There is a formula of change of basis for the matrix associated to an element which is a trivial consequence of the one in Proposition 2.9.

Proposition 2.29. *If W' is another K-basis of H, then*

$$M_\beta(H_{W'}, L_B) = M_\beta(H_W, L_B)P_W^{W'}.$$

2.5.2 Criteria for freeness

Next, we use the matrix $M_\beta(H_V, L_B)$ to characterize whether or not $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. We know that $\{v_i \cdot \beta\}_{i=1}^n$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ if and only if it is $\mathcal{O}_K$-linearly independent and an $\mathcal{O}_K$-system of generators. As $\mathfrak{A}_H$ acts on $\mathcal{O}_L$, it is immediate that $M_\beta(H_V, L_B) \in \mathcal{M}_n(\mathcal{O}_K)$. Standard linear algebra yields that the $\mathcal{O}_K$-linear independence of $\{v_i \cdot \beta\}_{i=1}^n$ is equivalent to the invertibility of the matrix $M_\beta(H_V, L_B)$ in $\mathcal{M}_n(K)$ (with the remark that in this case $\mathcal{O}_K$-linear independence is equivalent to K-linear independence), that is, $M_\beta(H_V, L_B) \in \mathrm{GL}_n(K)$. This condition means that the associated matrix has an inverse with entries in K, but not necessarily in $\mathcal{O}_K$. The condition of having integral entries turns out to be equivalent to the freeness of $\mathcal{O}_L$.

Corollary 2.30. *Let L/K be a degree n Hermite H-Galois extension. Let V be an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$ and B an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. An element $\beta \in \mathcal{O}_L$ generates $\mathcal{O}_L$ as $\mathfrak{A}_H$-module if and only if $M_\beta(H_V, L_B) \in \mathrm{GL}_n(\mathcal{O}_K)$.*

Proof. Suppose that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. Then, $B' := \{v_i \cdot \beta\}_{i=1}^n$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. As the matrix $M_\beta(H_V, L_B)$ is the matrix whose columns are the coordinates of $v_i \cdot \beta$ with respect to B, it is the change-basis matrix $P_B^{B'}$, and hence unimodular. Conversely, assume that $M_\beta(H_V, L_B) \in \mathrm{GL}_n(\mathcal{O}_K)$. Since B is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ and $v_i \cdot \beta = M_\beta(H_V, L_B) \cdot \gamma_i$ for every $1 \leq i \leq n$, $\{v_i \cdot \beta\}_{i=1}^n$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. □

Remark 2.31. The matrix $M_\beta(H_V, L_B)$ being unimodular means that its determinant is a unit of $\mathcal{O}_K$. This determinant is actually the generalized index $[\mathcal{O}_L : \mathfrak{A}_H \cdot \beta]$ (see [FT92, Section II.4] for a definition), and it is invertible if and only if the ideal it generates is trivial, that is, $\mathcal{O}_L = \mathfrak{A}_H \cdot \beta$, which is consistent with the previous result.

Example 2.32. Let us consider the extension $L/\mathbb{Q}$ of Example 2.2 and let $\beta = \beta_1 + \beta_2\omega + \beta_3\omega^2 \in \mathcal{O}_L$. In Example 2.26 we computed two bases V and V' of $\mathfrak{A}_H$ and the action of these bases on $\mathcal{O}_L$. Looking at the results obtained, we may write the matrices associated to β with respect to these bases:

$$M_\beta(H_V, L_B) = \begin{pmatrix} \beta_1 & \beta_1 & 0 \\ \beta_2 & 0 & 0 \\ \beta_3 & 0 & -\beta_3 \end{pmatrix}, \qquad M_\beta(H_{V'}, L_B) = \begin{pmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 \\ 0 & 0 & \beta_3 \end{pmatrix}.$$

The determinant of both matrices is $\beta_1\beta_2\beta_3$, which is an invertible element of $\mathbb{Z}$ if and only if all the β_i are 1 or -1. Then, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free and all possible generators are $\beta = \beta_1 + \beta_2\omega + \beta_3\omega^2$ with $\beta_i \in \{-1, 1\}$ for all $i \in \{1, 2, 3\}$.

A reformulation. The index of a Hopf Galois structure

Taking into account Proposition 2.29,

$$M_\beta(H_V, L_B) = M_\beta(H_W, L_B)P_W^V.$$

For an element $\beta \in \mathcal{O}_K$, let us denote $D_\beta(H_W, L_B) = \det(M_\beta(H_W, L_B))$. Then, the criterion of Corollary 2.30 is satisfied if and only if

$$D_\beta(H_W, L_B) \in \det(D)\mathcal{O}_K^*. \tag{2.5}$$

Now, assume that $\mathcal{O}_K$ is a Euclidean domain with Euclidean norm N_K. We also assume that N_K is either additive (i.e. $N_K(ab) = N_K(a) + N_K(b)$ for every non zero $a, b \in \mathcal{O}_L$) or multiplicative (i.e. $N_K(ab) = N_K(a)N_K(b)$ for every $a, b \in \mathcal{O}_L$). Given $u \in \mathcal{O}_K^*$, $N_K(u) = 0$ if N_K is additive and $N_K(u) = 1$ if N_K is multiplicative.

Example 2.33. The ring $\mathbb{Z}$ is an Euclidean domain with multiplicative Euclidean norm the usual absolute value $N_\mathbb{Q} = |\cdot|$. If p is a prime number, for a p-adic field K, $\mathcal{O}_K$ is an Euclidean domain with additive Euclidean norm the π_K-adic valuation v_K for an uniformising parameter π_K.

Under these considerations, (2.5) is equivalent to

$$N_K(D_\beta(H_W, L_B)) = N_K(\det(D)).$$

Proposition 2.34. *The number $N_K(\det(D))$ does not depend on the reduced matrix chosen.*

Proof. Let us call $M(H, L) = M(H_W, L_B)$ for convenience.

Since $M(H, L)$ has rank n, its Hermite normal form is $\begin{pmatrix} M \\ \hline O \end{pmatrix}$ for a certain matrix $M \in \mathrm{GL}_n(K)$ in echelon form. Let D be a reduced matrix of $M(H, L)$. By definition of reduced matrix, the matrices $M(H, L)$ and $\begin{pmatrix} D \\ \hline O \end{pmatrix}$ are equal up to left multiplication by a unimodular matrix (left equivalent according to [AW92, Definition 2.1]) and the Hermite normal form is unique (see [AW92, Theorem 2.13]), so they have the same Hermite normal form $\begin{pmatrix} M \\ \hline O \end{pmatrix}$.

We claim that M is the Hermite normal form of D. Indeed, if M' is the Hermite normal form of D, then there is a unimodular matrix $U \in \mathrm{GL}_n(\mathcal{O}_K)$ such that $UD = M'$. Then $\left(\begin{array}{c|c} U & 0 \\ \hline 0 & I_{n^2-n} \end{array}\right) \in \mathcal{M}_{n^2}(\mathcal{O}_K)$ is a unimodular matrix because its determinant is $\det(U) \in \mathcal{O}_K^*$, and satisfies

$$\left(\begin{array}{c|c} U & O' \\ \hline O & I_{n^2-n} \end{array}\right) \begin{pmatrix} D \\ \hline O \end{pmatrix} = \begin{pmatrix} M' \\ \hline O \end{pmatrix},$$

where O' is the zero matrix in $\mathcal{M}_{n\times(n^2-n)}(K)$. By the uniqueness of the Hermite normal form, $\begin{pmatrix} M \\ \hline O \end{pmatrix} = \begin{pmatrix} M' \\ \hline O \end{pmatrix}$, that is, $M = M'$. Moreover, we deduce that $UD = M$.

This proves that for every reduced matrix D there is a unimodular matrix carrying $\begin{pmatrix} D \\ O \end{pmatrix}$ to $\begin{pmatrix} M \\ O \end{pmatrix}$ that has its first $n \times n$ block U unimodular, and the equality $UD = M$ holds for this block. Then $N_K(\det(D)) = N_K(\det(M))$ for every reduced matrix D. □

This leads to the following definition:

Definition 2.35. *Let W be a K-basis of H. The index of the Hopf Galois structure $(H, \cdot)$ is defined as*

$$I_W(H, L) = N_K(\det(D)),$$

where D is a reduced matrix of $M(H, L)$.

Let us assume that N_K is additive (if it is multiplicative, we replace the additions by products). If W' is another K-basis of H, then

$$I_{W'}(H, L) = I_W(H, L) + N_K(\det(P_W^{W'})).$$

With this notation, we can rewrite Corollary 2.30 in a more convenient way, without requiring the basis V:

Proposition 2.36. *An element $\beta \in \mathcal{O}_L$ is an $\mathfrak{A}_H$-free generator of $\mathcal{O}_L$ if and only if*

$$N_K(D_\beta(H_W, L_B)) = I_W(H, L).$$

Note that this new condition is independent on the basis of H. Indeed, if W' is another K-basis of H, then $M_\beta(H_{W'}, L_B) = M_\beta(H_W, L_B) P_W^{W'}$, so

$$v_K(D_\beta(H_{W'}, L_B)) = N_K(D_\beta(H_W, L_B)) + N_K(\det(P_W^{W'})),$$

and joining this with the equality of indexes above, we obtain that $N_K(D_\beta(H_W, L_B)) = I_W(H, L)$ if and only if $N_K(D_\beta(H_{W'}, L_B)) = I_{W'}(H, L)$.

Example 2.37. We consider once again the extension $L/\mathbb{Q}$ in 2.2. The determinant of the reduced matrix D in Example 2.24 is $\frac{3}{2}$, which has absolute value $\frac{3}{2}$. Then, the index of the Hopf Galois structure of $L/\mathbb{Q}$ is $I(H, L) = \frac{3}{2}$. The matrix associated to β considering the basis W is

$$M_\beta(H_W, L_B) = \begin{pmatrix} \beta_1 & \beta_1 & 0 \\ \beta_2 & -\frac{\beta_2}{2} & \frac{\beta_2}{2} \\ \beta_3 & -\frac{\beta_3}{2} & -\frac{\beta_3}{2} \end{pmatrix},$$

with determinant $\frac{3\beta_1\beta_2\beta_3}{2}$. This coincides with $I_W(H, L)$ if and only if $\beta_1\beta_2\beta_3$ has absolute value 1, which recovers the conclusion that these are all the elements that can generate $\mathcal{O}_L$ as $\mathfrak{A}_H$-module.

2.6 Bases of eigenvectors

Although the reduction method works with every Hermite H-Galois extension L/K, reducing the matrix $M(H, L)$ may be a very difficult task, especially when the degree of the extension is big enough. However, for the extension in Example 2.2 we obtained a reduced matrix of $M(H, L)$ by only removing the zero rows. This happens because the action on the chosen basis of L gives a scalar multiple of the original element. In this section we study that property.

Definition 2.38. *Let L/K be an H-Galois extension and let us fix a K-basis $W = \{w_i\}_{i=1}^n$ of H and a K-basis $B = \{\gamma_j\}_{j=1}^n$ of L. We say that B is a* ***basis of eigenvectors*** *if for every $1 \leq i, j \leq n$ there exist elements $\lambda_{ij} \in K$ such that*

$$w_i \cdot \gamma_j = \lambda_{ij}\gamma_j.$$

The matrix

$$\Lambda = \begin{pmatrix} \lambda_{11} & \lambda_{21} & \cdots & \lambda_{n1} \\ \lambda_{12} & \lambda_{22} & \cdots & \lambda_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{1n} & \lambda_{2n} & \cdots & \lambda_{nn} \end{pmatrix}$$

is called the ***matrix of eigenvalues*** *with respect to W. We will also say that L/K has the* ***eigenvectors property*** *with respect to the Hopf Galois structure H.*

If B is a basis of eigenvectors, then the Gram matrix can be written as

$$G(H_W, L_B) = \begin{pmatrix} \lambda_{11}\gamma_1 & \lambda_{12}\gamma_2 & \cdots & \lambda_{1n}\gamma_n \\ \lambda_{21}\gamma_1 & \lambda_{22}\gamma_2 & \cdots & \lambda_{2n}\gamma_n \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n1}\gamma_1 & \lambda_{n2}\gamma_2 & \cdots & \lambda_{nn}\gamma_n \end{pmatrix}.$$

Moreover, the j-th block of the matrix of the action is the $n \times n$ matrix whose rows are all 0 except the j-th one, which is $(\lambda_{ij})_{i=1}^n$. Taking into account the expression (2.2), we deduce that

$$m_{ij}^{(k)}(H_W, L_B) = \delta_{jk}\lambda_{ij}$$

for every $1 \leq i, j, k \leq n$.

As the definition of the eigenvectors property for the basis B is written in terms of the basis of H, we need to prove that it actually does not depend on this choice.

Corollary 2.39. *Assume that there exist elements $\lambda_{ij} \in K$ such that $w_i \cdot \gamma_j = \lambda_{ij}\gamma_j$ for every $1 \leq i, j \leq n$ and let $W' = \{w_i'\}_{i=1}^n$ be another K-basis of H. Then, there exist $\lambda_{ij}' \in K$ such that $w_i' \cdot \gamma_j = \lambda_{ij}'\gamma_j$.*

Proof. Let us call $P_W^{W'} = (a_{ij})_{i,j=1}^n$. We know by Proposition 2.9 that $M_j(H_{W'}, L_B) = M_j(H_W, L_B)P_W^{W'}$ for all $1 \leq j \leq n$. Then, following the description of $M_j(H_W, L_B)$ above, we deduce that $w_i' \cdot \gamma_j = \left(\sum_{l=1}^n a_{li}\lambda_{lj}\right)\gamma_j$. Then, it is enough to take $\lambda_{ij}' = \sum_{l=1}^n a_{li}\lambda_{lj} \in K$. □

Note that the matrix of eigenvalues does depend on the basis of H (this is why in the definition we referred to it as the eigenvalues matrix with respect to the basis W). However, the previous proof yields easily that if Λ' is the eigenvalues matrix with respect to another basis W', then $\Lambda' = \Lambda P_W^{W'}$.

The most common situation is to work with a K-basis of L formed by the powers of a primitive element.

Definition 2.40. *Let L/K be a degree n H-Galois extension. Assume that L/K satisfies the eigenvector property with respect to H. A basis of eigenvectors of L/K is said to be* ***primitive*** *provided that it has the form $\{\alpha^j\}_{j=0}^{n-1}$ for some primitive element α of L/K.*

Example 2.41. *Let $L/\mathbb{Q}$ be the extension of Example 2.2. Then, $\{1, \omega, \omega^2\}$ is a primitive basis of eigenvectors of L, as can be observed from (2.1). The matrix of eigenvalues with the fixed bases is the matrix D' in Example 2.24.*

2.6.1 Associated order and freeness

Let us assume that L/K is Hermite and B is an integral basis of eigenvectors of L. Reducing the matrix $M(H, L)$ is trivial in this case, as we can permute its rows so as to place the zero ones at the bottom of the matrix. This shows that the eigenvalues matrix Λ is a reduced matrix of $M(H, L)$. Let us call $\Omega = (\omega_{ij})_{i,j=1}^n$ its inverse. Then $\mathfrak{A}_H$ has an $\mathcal{O}_K$-basis V given by the elements $v_i = \sum_{l=1}^n \omega_{li} w_l$, $1 \leq i \leq n$.

Now, we focus on the action of this basis on $\mathcal{O}_L$. In the case of Example 2.26 we proved that the action diagonalizes and by only using the definition of the action, we proved that the basis of the associated order is of pairwise orthogonal idempotents. This inspires the general result:

Proposition 2.42. *Let L/K be an H-Galois Hermite extension of fields and assume that $B = \{\gamma_j\}_{j=1}^n$ is an integral basis of eigenvectors of L. Let $V = \{v_i\}_{i=1}^n$ be the basis of $\mathfrak{A}_H$ obtained from the matrix of eigenvalues Λ. Then, the action of V on $\mathcal{O}_L$ is diagonal, so the elements of V are pairwise orthogonal idempotents.*

Proof. By Theorem 2.25, the coordinates of $v_i \cdot \gamma_j$ with respect to the basis B are given by the column vector obtained from the multiplication $M_j(H_W, L_B)\Omega$. Now, the unique non-zero row of $M_j(H_W, L_B)$ is the j-th one, which is by definition the j-th row of Λ. But Ω is the inverse of Λ, so the matrix-vector product above is actually the j-th vector of the canonical basis. This means that $v_i \cdot \gamma_j = \delta_{ij}\gamma_j$ for all $1 \leq i, j \leq n$, proving that the action is diagonal. □

Let us move on to the question of the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$. Given $\beta = \sum_{j=1}^n \beta_j \gamma_j$, the matrix associated to β with respect to the bases V and B is

$$M_\beta(H_V, L_B) = \begin{pmatrix} \beta_1 & 0 & \cdots & 0 \\ 0 & \beta_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \beta_n \end{pmatrix}.$$

The determinant of this matrix is $D_\beta(H_V, L_B) = \beta_1\beta_2 \cdots \beta_n$, and there are of course choices of β for which this product is in $\mathcal{O}_K^*$; for instance $\beta = \sum_{j=1}^n \gamma_j$. This proves:

Proposition 2.43. *Let L/K be a Hermite H-Galois extension and assume that $B = \{\gamma_j\}_{j=1}^n$ is an integral basis of eigenvectors of L. Then, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free and the elements that (individually) may generate $\mathcal{O}_L$ as $\mathfrak{A}_H$-module are the elements $\beta \in \mathcal{O}_L$ such that $\beta_1 \cdots \beta_n \in \mathcal{O}_K^*$.*

We summarize the results obtained in this part:

Theorem 2.44. *Let L/K be an H-Galois Hermite extension of fields. Assume that L/K admits some integral basis of eigenvectors $B = \{\gamma_j\}_{j=1}^n$ with respect to H. Then:*

1. *If $\Omega = (\omega_{ij})_{i,j=1}^n$ is the inverse of the eigenvalues matrix of B, then the elements*

$$v_i = \sum_{l=1}^n \omega_{li} w_l \; 1 \leq i \leq n$$

   form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

2. *The elements of the basis above are pairwise orthogonal idempotents.*

3. *$\mathcal{O}_L$ is $\mathfrak{A}_H$-free and the normal integral basis generators are the elements $\beta \in \mathcal{O}_L$ such that $\beta_1 \cdots \beta_n \in \mathcal{O}_K^*$.*

Example 2.45. Let L/K be a cyclic degree p extension of p-adic fields with Galois group $G = \langle \sigma \rangle$ and assume that K contains a primitive p-th root of unity ξ. Assume that there is a primitive element α of L/K such that $v_K(\alpha^p) = 1$, that is, L/K is of the first type among the three possible listed in [Chi00, Proposition 24.2]. By [Chi00, Proposition 24.3], $\mathfrak{A}_{L/K}$ is the maximal $\mathcal{O}_K$-order in $K[G]$ and $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free. We can reach the same conclusions by using the results established in this section. Indeed, we may assume without loss of generality that $\sigma(\alpha) = \xi\alpha$, so $\sigma(\alpha^j) = \xi^j\alpha^j$ for all j. Then, $B = \{\alpha^j\}_{j=0}^{p-1}$ is a basis of eigenvectors of the classical Galois structure, and it is integral because α is a root of a π_K-Eisenstein polynomial. The eigenvalues matrix is the Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \xi & \cdots & \xi^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{p-1} & \cdots & \xi^{(p-1)^2} \end{pmatrix},$$

with inverse

$$\frac{1}{p}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \xi^{-1} & \cdots & \xi^{-(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{-(p-1)} & \cdots & \xi^{-(p-1)^2} \end{pmatrix}.$$

By the second statement of Theorem 2.44, the elements $e_j = \frac{1}{p}\sum_{k=0}^{p-1}\xi^{-jk}\sigma^k$ form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$. Since this is a basis of primitive pairwise orthogonal idempotents, it gives the maximal $\mathcal{O}_K$-order in $K[G]$. On the other hand, Proposition 2.43 gives that $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

Remark 2.46. If we assume that L/K is of one of the other two types in [Chi00, Proposition 24.2], then for a primitive element α of L/K, the basis of its powers $\{\alpha^j\}_{j=1}^n$ is still a primitive basis of eigenvectors, but it is not integral, and then we cannot apply the results in this section. In fact, Theorem 2.44 does not hold because $\mathcal{O}_L$ is not in general $\mathfrak{A}_{L/K}$-free.

2.6.2 The eigenvectors property in the Galois case

By definition, the eigenvectors property is satisfied for a Hopf Galois extension L/K whenever we can find a K-basis of L formed by eigenvectors of the action of the Hopf Galois structure that we are considering. In this section, we will see the meaning of this property with the point of view of Galois theory. That is, we characterize the eigenvectors property for a Galois extension with respect to the classical Galois structure, what we call the **classical eigenvectors property**. Accordingly, a basis of eigenvectors with respect to the classical Galois structure will be called a **classical eigenvectors basis**. In Example 2.45 we showed that for a cyclic degree p extension the key property for the existence of such a basis was the fact that the primitive root ξ was in the ground field, that is, the extension was Kummer. Actually, this property characterizes the cyclic extensions with a classical basis of eigenvectors.

Proposition 2.47. *Let L/K be a Galois extension of degree n. Then, L/K has some classical primitive basis of eigenvectors if and only if L/K is cyclic and Kummer.*

Proof. Let us call $G = \mathrm{Gal}(L/K)$. Assume that there exists some primitive element α of L/K such that

$$\sigma(\alpha^i) = \lambda_{\sigma,i}\alpha^i,\ \sigma \in G,\ 0 \leq i \leq n-1,$$

where $\lambda_{\sigma,i} \in K$. Let $f = \mathrm{irr}(\alpha, X, K)$ be the minimal polynomial of α. Then,

$$f(X) = \prod_{\sigma\in G}(X - \sigma(\alpha)) = \prod_{\sigma\in G}(X - \lambda_{\sigma,1}\alpha).$$

Since α is a primitive element, all the $\sigma(\alpha)$ are distinct as σ runs through G, so the independent term of this polynomial is $(-1)^n\prod_{\sigma\in G}\lambda_{\sigma,1}\alpha^n$, which obviously belongs to K. Since the $\lambda_{\sigma,1}$ also do, we obtain that $\alpha^n \in K$. This says that $f(X) = X^n - \alpha^n$. Hence, if ξ is a primitive n-th root of unity, the roots of f are α, $\xi\alpha, ..., \xi^{n-1}\alpha$. By standard Galois theory, G permutes the roots of f, so for every $\sigma \in G$ there is a unique $0 \leq i_\sigma \leq n-1$ such that $\sigma(\alpha) = \xi^{i_\sigma}\alpha$. But by the hypothesis, $\sigma(\alpha) = \lambda_{\sigma,1}\alpha$. Hence, $\xi^{i_\sigma} = \lambda_{\sigma,1} \in K$ for every $\sigma \in G$. In particular, $\xi \in K$, so L/K is Kummer. Then, since the primitive element α of L/K is a root of f and this polynomial is of the form $f(X) = X^n - \alpha^n$, L/K is cyclic.

Conversely, assume that L/K is cyclic and Kummer. Then, L is the splitting field over K of a polynomial of the form $f(X) = X^n - \alpha^n$ for some primitive element α of L/K, whose roots are $\alpha, \xi\alpha, ..., \xi^{n-1}\alpha$. Since G permutes the roots of f, for every $\sigma \in G$ there is a unique $0 \leq i_\sigma \leq n-1$ such that $\sigma(\alpha) = \xi^{i_\sigma}\alpha$. Since L/K is Kummer, $\xi^{i_\sigma} \in K$ for all $\sigma \in G$. Then the basis of the powers of α is a classical primitive basis of eigenvectors. □

This result does not characterize completely the Galois extensions that satisfy the classical eigenvectors property, because there may be Galois extensions L/K with a basis of eigenvectors in which no element is primitive. However, we can consider the extensions generated by the elements of a basis, apply the previous result, and compare with the whole extension. In order to *lift* the eigenvectors property, we use the following lemma.

Lemma 2.48. *Let E/K and F/K be Galois extensions such that $E \cap F = K$ and let $L = EF$. If E/K and F/K satisfy the classical eigenvectors property , then so does L/K.*

Proof. Let $\{\alpha_i\}_{i=1}^r$ be a classical basis of eigenvectors of E and $\{z_j\}_{j=1}^u$ a classical basis of eigenvectors of F. Then $\{\alpha_i z_j\}_{i,j=1}^n$ is a K-basis of L. Since $E \cap F = K$, we have

$$G = \mathrm{Gal}(L/K) = \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K).$$

Hence, for every $\sigma\tau \in G$ and $1 \leq i \leq r$ and $1 \leq j \leq u$,

$$\sigma\tau(\alpha_i z_j) = \lambda_{\sigma i}^{(E)}\lambda_{\tau,j}^{(F)}\alpha_i z_j.$$

Then, $\{\alpha_i z_j\}$ is a classical eigenvectors basis of L/K. □

The following result proves the characterization that we wanted.

Theorem 2.49. *Let L/K be a Galois extension. Then, L/K satisfies the eigenvectors property with respect to the classical Galois structure if and only if L/K is a compositum of cyclic Kummer extensions.*

Proof. Assume that L/K satisfies the eigenvectors property with respect to the classical Galois structure. Let $\{\alpha_j\}_{j=1}^n$ be a K-basis of L such that

$$\sigma(\alpha_j) = \lambda_{\sigma,j}\alpha_j,\ 1 \leq j \leq n,\ \sigma \in G,$$

where $\lambda_{\sigma,j} \in K$. Thus, for every $1 \leq j \leq n$, the conjugates of α_j are scalar multiplies of α_j. Then, $K(\alpha_j)/K$ is a Galois extension that satisfies the eigenvectors property with respect to the classical Galois structure with a primitive eigenvector basis, the one generated by α_j. Therefore, by Proposition 2.47, $K(\alpha_j)/K$ is cyclic and Kummer for every $1 \leq j \leq n$.

Now, it is quite clear that $L = \prod_{j=1}^n K(\alpha_j)$. Indeed, the product is contained in L because $K(\alpha_j) \subset L$ for every $1 \leq j \leq n$, and for the other inclusion it is enough to notice that the product contains the K-basis $\{\alpha_1, ..., \alpha_n\}$ of L, and hence all elements of L. This proves that L/K is the compositum of cyclic Kummer extensions.

Conversely, assume that L/K is a composition of cyclic Kummer extensions. By Proposition 2.47, all of them satisfy the eigenvectors property with respect to the classical Galois structure and a primitive element. By the previous lemma, L/K satisfies the eigenvectors property with respect to the classical Galois structure. □

2.7 Absolute extensions of fields with low degree

The reduction method provides a way to determine effectively the associated order of a Hopf Galois structure and a necessary and sufficient condition for the existence of a normal basis generator. However, since it requires to know how the Hopf Galois structure acts on the ring of integers, it is difficult to carry out the explicit computations unless the degree of the extension is very low. In this section we study the most simple cases: extensions L/K of degree 2 and 3. Except for a particular case of quadratic extensions, we will take the ground field K to be $\mathbb{Q}$ or $\mathbb{Q}_p$ for some prime number p. We already know the answer for the question of the freeness: By Theorem 1.16, these extensions have the classical Galois structure as their unique Hopf Galois structure, and by Leopoldt's theorem in its local version, $\mathcal{O}_L$ is free over its associated order. We will reach the same conclusion using the criterion in Section 2.5 and compute a generator for each case.

2.7.1 Quadratic extensions

Let L/K be a separable Hermite quadratic extension of fields. Then, L/K is Galois with Galois group of the form $G = \langle\sigma\rangle$ and $\sigma^2 = 1$. For simplicity, let us assume that $\mathrm{char}(K) \neq 2$. Hence, we can write $L = K(z)$ where $z \in L - K$, $z^2 \in K$ and $\sigma(z) = -z$. The unique Hopf Galois structure of L/K is the classical Galois structure H_c. To apply the reduction method, we need a basis of H_c, an integral basis of L, and how H_c acts on this basis. The first one is immediate: the elements $\{\mathrm{Id}, \sigma\}$ of G form a K-basis of H_c. Since the extension is Hermite, there is an element $z \in \mathcal{O}_L$ such that $m := z^2 \in \mathcal{O}_K$. Then $\{1, z\}$ is a K-basis of L. Let us assume that it is also an integral basis.

Theorem 2.50. *Let L/K be a Hermite quadratic extension of fields with* $\mathrm{char}(K) \neq 2$ *such that $z = \sqrt{m}$, with $m \in K$, generates an integral basis of L. Then, $\mathfrak{A}_{L/K}$ has a basis of* *idempotents*

$$\left\{\frac{\mathrm{Id}+\sigma}{2}, \frac{\mathrm{Id}-\sigma}{2}\right\}$$

and $\mathcal{O}_L$ *is* $\mathfrak{A}_{L/K}$*-free with generator any element* $\beta = \beta_1 + \beta_2 z \in \mathcal{O}_L$ *such that* $\beta_1\beta_2 \in \mathcal{O}_K^*$. *In particular,* $1+z$ *is a generator.*

Proof. The hypothesis means that $\{1, z\}$ is an integral basis of eigenvectors, and since $\sigma(z) = -z$, the eigenvalues matrix is

$$\Lambda = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The columns of its inverse give the $\mathcal{O}_K$-basis of $\mathfrak{A}_{L/K}$

$$\left\{\frac{\mathrm{Id}+\sigma}{2}, \frac{\mathrm{Id}-\sigma}{2}\right\},$$

which by Proposition 2.42 is a basis of pairwise orthogonal idempotents. Regarding the freeness, Proposition 2.43 gives that $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free with generator any element $\beta_1 + \beta_2 z$ such that $\beta_1\beta_2 \in \mathcal{O}_K^*$. □

Remark 2.51. *If in addition* 2 *is an invertible element in* $\mathcal{O}_K$*, the same basis* $\{\mathrm{Id}, \sigma\}$ *of* H_c *is an* $\mathcal{O}_K$*-basis of* $\mathfrak{A}_{L/K}$*. That is,* $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$*. Note that this is the case if the ground field is* $\mathbb{Q}_p$ *with* p *an odd prime number, which is coherent with what we obtain if we apply Noether theorem, as such an extension is tamely ramified.*

If $\{1, z\}$ is not an integral basis, then a general description of $\mathcal{O}_L$ is not available and the behaviour depends on the nature of the fields.

With ground field $\mathbb{Q}$

If $L/\mathbb{Q}$ is a quadratic extension and $L = \mathbb{Q}(z)$ with $z^2 = m \in \mathbb{Z}$ square-free, it is a classical exercise in number theory to prove that an integral basis of L is given by $\{1, z\}$ if $m \equiv 2$ or $3 \pmod 4$ and $\{1, \frac{1+z}{2}\}$ if $m \equiv 1 \pmod 4$.

In the first case, $\{1, z\}$ is an integral basis and Theorem 2.50 gives the solution. Otherwise we have the Gram matrix

$$G(H_c, L) = \begin{pmatrix} 1 & \frac{1+z}{2} \\ 1 & 1 - \frac{1+z}{2} \end{pmatrix},$$

and hence

$$M(H_c, L) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 1 \\ 1 & -1 \end{pmatrix}.$$

Then, the reduced matrix D is the identity, so $\mathfrak{A}_{L/\mathbb{Q}} = \mathbb{Z}[G]$. Let $\beta = \beta_1 + \beta_2 z \in \mathcal{O}_L$. Then,

$$M_\beta(H_c, L) = \begin{pmatrix} \beta_1 & \beta_1 + \beta_2 \\ \beta_2 & -\beta_2 \end{pmatrix},$$

which has determinant

$$D_\beta(H_c, L) = -(2\beta_1 + \beta_2)\beta_2.$$

In this case $[H_c : L/\mathbb{Q}] = |\det(D)| = 1$. If $\beta = -1 + z$, then $D_\beta(H_c, L) = 1$ as well, so $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free with generator β.

With ground field $\mathbb{Q}_2$

Let $L/\mathbb{Q}_2$ be a quadratic extension. According to [Rio95, Section 2.4], L is the splitting field over $\mathbb{Q}_2$ of one of the polynomials

$$x^2+1, \quad x^2\pm 5, \quad x^2\pm 2, \quad x^2\pm 10.$$

Let us call f the polynomial of that list that indeed defines $L/\mathbb{Q}_2$.

The unique case in which the extension is unramified is when the defining polynomial is $f(x)=x^2-5$. In such case, $\mathfrak{A}_{L/\mathbb{Q}_2}=\mathbb{Z}_2[G]$ and $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

We study the rest of the cases. Let us assume that $f(x)=x^2+2a$ with $a\in\{1,-1,5,-5\}$. The roots of f are $z=\sqrt{2a}$ and $w=-\sqrt{2a}=-z$. Since f is 2-Eisenstein, $\{1,z\}$ is an integral basis of L, so it is enough to apply Theorem 2.50.

Otherwise, we suppose $f(x)=x^2+a$, $a\in\{1,5\}$. Then f is not 2-Eisenstein, but we can try to build a polynomial with such property defining the same extension. Indeed, we define

$$g(x)=f(x+1)=x^2+2x+a+1,$$

and $v_2(a+1)=1$, so g is 2-Eisenstein. The roots of this polynomial are

$$z=-1+\sqrt{-a}, \quad w=-1-\sqrt{-a}=-2-z.$$

Now, $\{1,z\}$ is an integral basis of $\mathcal{O}_L$ and

$$G(H_c,L)=\begin{pmatrix}1 & z\\ 1 & -2-z\end{pmatrix}.$$

Then, the matrix of the action is

$$M(H_c,L)=\begin{pmatrix}1 & 1\\ 0 & 0\\ 0 & -2\\ 1 & -1\end{pmatrix},$$

which has Hermite normal form $D=\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}$. Then, $\mathfrak{A}_{L/\mathbb{Q}_2}$ has basis

$$\left\{\mathrm{Id}, \frac{-\mathrm{Id}+\sigma}{2}\right\}.$$

Let $\beta=\beta_1+\beta_2 z\in\mathcal{O}_L$. Then,

$$D_\beta(H_c,L)=\begin{pmatrix}\beta_1 & \beta_1-2\beta_2\\ \beta_2 & -\beta_2\end{pmatrix},$$

which has determinant

$$D_\beta(H_c,L)=2(-\beta_1+\beta_2)\beta_2.$$

Then, we have that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_2}$-free and $\beta=z$ is a generator.

2.7.2 Cubic cyclic extensions

If L/K is a degree 3 extension of fields, then it is not necessarily Galois: its Galois closure $\widetilde{L}$ may have Galois group C_3 or D_3 over K. In this chapter we explore the first of these cases (the other one being treated in Chapter 4).

Thus, let us assume that L/K is a cyclic degree 3 extension of fields and let $G = \mathrm{Gal}(L/K)$. The classical Galois structure is the unique Hopf Galois structure and a basis of the Hopf algebra is given by the Galois group $G = \langle\sigma\rangle$, $\sigma^3 = \mathrm{Id}$. As in the quadratic case, the form of an integral basis of L depends strongly on the nature of the fields.

With ground field $\mathbb{Q}$

If $L/\mathbb{Q}$ is a cyclic cubic extension, then we have at our disposal a complete description of L and an integral basis.

Theorem 2.52. *1. There exists a unique pair of integers $(e, u) \in \mathbb{Z}^2$ such that $e = \frac{u^2+3v^2}{4}$ is for a certain $v \in \mathbb{Z}$ a product of distinct primes congruent to 1 modulo 3, $u \equiv 2 \pmod 3$ and $L = \mathbb{Q}(\alpha)$ where α is a root of the polynomial*

$$f(x) = x^3 - 3ex - eu.$$

2. The other two roots of f are

$$\sigma(\alpha) = -\frac{2e}{v} - \frac{u+v}{2v}\alpha + \frac{1}{v}\alpha^2,$$

$$\sigma^2(\alpha) = \frac{2e}{v} + \frac{u-v}{2v}\alpha - \frac{1}{v}\alpha^2.$$

3. If $3 \nmid v$, then $\{1, \alpha, \sigma(\alpha)\}$ is an integral basis of L and $\mathrm{disc}(L/K) = (9e)^2$. Otherwise, for $\alpha' = \frac{\alpha+1}{3}$, $\{1, \alpha', \sigma(\alpha')\}$ is an integral basis of L and $\mathrm{disc}(L/K) = e^2$.

Proof. The statement above is a summary of the results in [Coh93, Section 6.4.2]. □

Let us assume that $3 \nmid v$. Fixing in L the integral basis $\{1, \alpha, \sigma(\alpha)\}$, we have

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha & \sigma(\alpha) \\ 1 & \sigma(\alpha) & \sigma^2(\alpha) \\ 1 & \sigma^2(\alpha) & \alpha \end{pmatrix}.$$

We need the coordinates of $\sigma^2(\alpha)$ with respect to the integral basis. Of the two equalities in the second part of the previous theorem, the first one is equivalent to $\alpha^2 = 2e + \frac{u+v}{2}\alpha + v\sigma(\alpha)$, and replacing this in the left side member of the second, we obtain

$$\begin{aligned}\sigma^2(\alpha) &= \frac{2e}{v} + \frac{u-v}{2v}\alpha - \frac{2e}{v} - \frac{u+v}{2v}\alpha - \sigma(\alpha) \\ &= -\alpha - \sigma(\alpha).\end{aligned}$$

Then,

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha & \sigma(\alpha) \\ 1 & \sigma(\alpha) & -\alpha - \sigma(\alpha) \\ 1 & -\alpha - \sigma(\alpha) & \alpha \end{pmatrix}.$$

The Hermite normal form of $M(H_c, L)$ is

$$D = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 3 \end{pmatrix},$$

whence

$$\left\{ \mathrm{Id}, \sigma, \frac{\mathrm{Id} + \sigma + \sigma^2}{3} \right\}$$

is a $\mathbb{Z}$-basis of $\mathfrak{A}_{L/\mathbb{Q}}$. On the other hand, given $\beta = \beta_1 + \beta_2\alpha + \beta_3\sigma(\alpha) \in \mathcal{O}_L$, we have

$$D_\beta(H_c, L) = 3\beta_1(\beta_2^2 - \beta_2\beta_3 + \beta_3^2).$$

If $\beta = 1 + \alpha$, the determinant is 3, which coincides with the absolute value of the determinant of D. Then, $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free with generator β.

Assume that $3|v$. In this case, the integral basis is $\{1, \alpha', \sigma(\alpha')\}$ where $\alpha' = \frac{1+\alpha}{3}$, and the Gram matrix is

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha' & \sigma(\alpha') \\ 1 & \sigma(\alpha') & \sigma^2(\alpha') \\ 1 & \sigma^2(\alpha') & \alpha' \end{pmatrix},$$

so now we have to determine the coordinates of $\sigma^2(\alpha')$ in terms of the aforementioned basis. We have:

$$\begin{aligned} \sigma^2(\alpha') &= \sigma^2\left(\frac{1+\alpha}{3}\right) \\ &= \frac{1 - \alpha - \sigma(\alpha)}{3} \\ &= \frac{1}{3} - \frac{1}{3}\alpha - \frac{1}{3}\sigma(\alpha). \end{aligned}$$

To obtain the coordinates with respect to $\{1, \alpha', \sigma(\alpha')\}$, we replace $\alpha = 3\alpha' - 1$ in the expression above:

$$\sigma^2(\alpha') = \frac{1}{3} - \frac{1}{3}(3\alpha' - 1) - \frac{1}{3}\sigma(3\alpha' - 1) = 1 - \alpha' - \sigma(\alpha').$$

Then,

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha' & \sigma(\alpha') \\ 1 & \sigma(\alpha') & 1 - \alpha' - \sigma(\alpha') \\ 1 & 1 - \alpha' - \sigma(\alpha') & \alpha' \end{pmatrix}.$$

In this case we obtain the 3×3 identity matrix as the Hermite normal form D of $M(H_c, L)$. Thus, $\mathfrak{A}_{L/\mathbb{Q}} = \mathbb{Z}[G]$. On the other hand, for $\beta = \beta_1 + \beta_2\alpha' + \beta_3\sigma(\alpha') \in \mathcal{O}_L$, we have

$$D_\beta(H_c, L) = (\beta_2^2 - \beta_2\beta_3 + \beta_3^2)(3\beta_1 + \beta_2 + \beta_3),$$

and for $\beta = \alpha'$ the determinant is 1, which coincides with the absolute value of $\det(D)$. Hence, $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free with generator β.

With ground field $\mathbb{Q}_3$

Let us study the cyclic degree 3 extensions of $\mathbb{Q}_3$. Although this case is actually solved with the result of Bertrandias and Ferton, we will also apply the reduction method in order to compare the results obtained.

First, if $L/\mathbb{Q}_3$ is a cyclic degree 3 extension, then L is defined by one of the polynomials

$$x^3 - x + 1, \quad x^3 - 3x^2 + 3, \quad x^3 - 3x^2 + 12, \quad x^3 - 3x^2 + 21.$$

These polynomials have been taken from [LMFDB, p-adic field 3.3.0.1, p-adic field 3.3.4.2, p-adic field 3.3.4.3, p-adic field 3.3.4.1], respectively. For the first polynomial, $L/\mathbb{Q}_3$ is unramified. Then, for this case, $\mathfrak{A}_{L/\mathbb{Q}_3} = \mathbb{Z}[G]$ and $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_3}$-free.

For the other polynomials, $L/\mathbb{Q}_3$ is totally ramified. All of these are 3-Eisenstein, so a root of the aforementioned polynomials generates an integral power basis of L. Let f be one of those polynomials. Then, $\mathrm{disc}(L/\mathbb{Q}_3) = \mathrm{disc}(f)$. For $a \in \{1, 4, 7\}$,

$$\mathrm{disc}(x^3 - 3x^2 + 3a) = 3^4(4a - 3a^2),$$

so $v_3(\mathrm{disc}(L/\mathbb{Q}_3)) = 4$. From $4 = \sum_{i=0}^{\infty}(|G_i| - 1)$ it follows that $|G_0| = |G_1| = 3$ and $|G_i| = 1$ for all $i > 1$, so $t = 1$. We apply Theorem 1.34 with $K = \mathbb{Q}_3$: we have that $\frac{3}{2} - 1 = \frac{1}{2} < t$ and the expansion of $\frac{1}{3}$ as continued fraction is trivial, so $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_3}$-free for all cases. Moreover, by Proposition 1.33, $\mathfrak{A}_{L/\mathbb{Q}_3}$ has $\mathbb{Z}_3$-basis

$$\left\{ \mathrm{Id}, -\mathrm{Id} + \sigma, \frac{\mathrm{Id} - 2\sigma + \sigma^2}{3} \right\}. \tag{2.6}$$

Let us check that we obtain the same conclusions by applying the reduction method. First we determine the Gram matrix with respect to an integral basis of L.

Let f be one of the polynomials above and fix a root α of f, which gives rise to a power integral basis. In order to determine the action of the Galois group on this basis, we have to deal with the conjugates of α and their powers. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f, where, for instance, $\alpha_1 = \alpha$. By reordering these roots or replacing σ by σ^2, we can assume that σ induces the permutation $(\alpha_1, \alpha_2, \alpha_3)$. There is a quadratic polynomial $f_1 \in L[x]$ such that $f(x) = (x - \alpha)f_1(x)$, and in practice f_1 can be determined by using for instance Ruffini algorithm. Then, α_2 and α_3 are roots of a quadratic polynomial and consequently can be expressed explicitly in terms of α.

There are two possible obstacles:

- The appearance of the square root of an element of L, i.e. a linear combination of the powers of α. But since the degree of the extension is very low, it can be solved easily with some mathematical computation software.
- There is no factorization of f as the one above with coefficients in $\mathbb{Q}(\alpha)$, that is, the coefficients of the corresponding linear combinations of the powers of α could be 3-adic numbers that are not rational. In that case, we replace f

by a polynomial that generates the same extension and factorizes with coefficients in $\mathbb{Q}$, for example its Galois splitting model. If that polynomial is not 3-Eisenstein, we cannot use Theorem 1.20 to assure whether or not some of its roots give rise to an integral basis. Then, what we do is either to prove it in some other way or to carry out a change of variables so that the factorization property is preserved and obtain a 3-Eisenstein polynomial.

First, we consider the unramified case, i.e. $f(x) = x^3 - x + 1$. In this case, if $f_1(x) = \frac{f(x)}{x-\alpha}$, then this polynomial does not have coefficients in $\mathbb{Q}(\alpha)$. Then, we replace f by its Galois splitting model $g(x) = x^3 + x^2 - 2x - 1$ (see [LMFDB, p-adic field 3.3.0.1]).

We claim that a root α of g generates a power integral basis of L, that is, that the $\mathbb{Z}_3$-algebras $\mathcal{O}_L$ and $\mathbb{Z}_3[\alpha]$ coincide. We have trivially that $\mathbb{Z}_3[\alpha] \subset \mathcal{O}_L$. We will prove that their discriminant ideals (in the sense of the definition given in Section 1.4) coincide. By [Chi00, Corollary 22.4], this will imply that the equality follows. Again by [LMFDB, p-adic field 3.3.0.1], the discriminant exponent of L is 0, so $\operatorname{disc}(\mathcal{O}_L) = \mathbb{Z}_3$. On the other hand, $\operatorname{disc}(g) = 49 \in \mathbb{Z}_3^*$, so the ideal it generates is $\operatorname{disc}(\mathbb{Z}_3[\alpha]) = \mathbb{Z}_3$, so we have the equality.

By Ruffini algorithm, we find that

$$g(x) = (x - \alpha)(x^2 + (\alpha+1)x + \alpha^2 + \alpha - 2),$$

so the two conjugates of α are roots of the quadratic polynomial. Its discriminant is $-3\alpha^2 - 2\alpha + 9$. Solving a system of three equations with three indeterminates, one finds that

$$\sqrt{-3\alpha^2 - 2\alpha + 9} = 2\alpha^2 + \alpha - 3,$$

with the sign chosen by convenience. Hence, the conjugates of α are

$$\begin{aligned} \alpha_2 &= \frac{-(\alpha+1) + 2\alpha^2 + \alpha - 3}{2} = \frac{2\alpha^2 - 4}{2} = \alpha^2 - 2, \\ \alpha_3 &= \frac{-(\alpha+1) - 2\alpha^2 - \alpha + 3}{2} = \frac{-2\alpha^2 - 2\alpha + 2}{2} = -\alpha^2 - \alpha + 1. \end{aligned}$$

Thus, the Gram matrix of the action is

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \alpha_3 & \alpha_3^2 \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & -2+\alpha^2 & 3-\alpha-\alpha^2 \\ 1 & 1-\alpha-\alpha^2 & 2+\alpha \end{pmatrix}.$$

Then, the matrix of the action is

$$M(H, L) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -2 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 3 & 2 \\ 0 & -1 & 1 \\ 1 & -1 & 0 \end{pmatrix}.$$

The Hermite normal form of this matrix is the identity matrix of order 3, proving that $\{1, \sigma, \sigma^2\}$ is an $\mathbb{Z}_3$-basis of $\mathfrak{A}_{L/\mathbb{Q}_3}$, that is, $\mathfrak{A}_H = \mathbb{Z}_3[G]$. With respect to the freeness, given $\beta = \beta_1 + \beta_2\alpha + \beta_3\alpha^2$, the matrix associated to β is

$$M_\beta(H_c, L) = \begin{pmatrix} \beta_1 & \beta_1 - 2\beta_2 + 3\beta_3 & \beta_1 + \beta_2 + 2\beta_3 \\ \beta_2 & -\beta_3 & -\beta_2 + \beta_3 \\ \beta_3 & \beta_2 - \beta_3 & -\beta_2 \end{pmatrix},$$

with determinant

$$D_\beta(H_c, L) = (\beta_2^2 - \beta_2\beta_3 + \beta_3^2)(3\beta_1 - \beta_2 + 5\beta_3).$$

In particular, if $\beta = -1 + \alpha^2$, then $D_\beta(H_c, L) = 2 \in \mathbb{Z}_3^*$, so $v_3(D_\beta(H_c, L)) = 0$ for this specific β. On the other hand, since the Hermite normal form is the identity, the index of the classical Galois structure is $I(H_c, L) = 0$. Then, by Proposition 2.36, $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_3}$-free with generator $-1 + \alpha^2$.

Next, we move on to the totally ramified cases. Let us assume that $f(x) = x^3 - 3x^2 + 3$. In this case

$$f(x) = (x - \alpha)(x^2 + (\alpha - 3)x + \alpha^2 - 3\alpha).$$

Solving the corresponding quadratic equation:

$$\alpha_2 = 3 + \alpha - \alpha^2, \quad \alpha_3 = -2\alpha + \alpha^2.$$

Now, the action of G on the power basis generated by α gives the Gram matrix

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & 3 + \alpha - \alpha^2 & 6 + 3\alpha - 2\alpha^2 \\ 1 & -2\alpha + \alpha^2 & 3 - 3\alpha + \alpha^2 \end{pmatrix}.$$

Now, suppose that $f(x) = x^3 - 3x^2 + 12$. As in the unramified case, the polynomial $f_1(x) = \frac{f(x)}{x-\alpha}$ does not have coefficients in $\mathbb{Q}(\alpha)$. Then, we first replace f by its Galois splitting model $x^3 - 21x + 35$ (see [LMFDB, p-adic field 3.3.4.3]), and then make the change of variable $x \mapsto x + 1$, obtaining the polynomial

$$g(x) = x^3 + 3x^2 - 18x + 15.$$

This is 3-Eisenstein and also factors with coefficients in $\mathbb{Q}$. Thus, let us take α to be a root of g. The other two roots of g are

$$\alpha_2 = -12 + 4\alpha + \alpha^2, \quad \alpha_3 = 9 - 5\alpha - \alpha^2.$$

Then, the Gram matrix in this case is

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & -12 + 4\alpha + \alpha^2 & 69 - 21\alpha - 5\alpha^2 \\ 1 & 9 - 5\alpha - \alpha^2 & -24 + 21\alpha + 4\alpha^2 \end{pmatrix}.$$

Finally, let us take $f(x) = x^3 - 3x^2 + 21$. For this polynomial, we again replace f by its Galois splitting model $x^3 - 21x - 28$ (see [LMFDB, p-adic field 3.3.4.1]), and after that we make the change $x \mapsto x + 1$, obtaining

$$g(x) = x^3 + 3x^2 - 18x - 48.$$

If α is a root of g, the other two roots are

$$\alpha_2 = \frac{-18-\alpha+\alpha^2}{2}, \quad \alpha_3 = \frac{12-\alpha-\alpha^2}{2}.$$

The Gram matrix in this case is

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \frac{-18-\alpha+\alpha^2}{2} & \frac{42-3\alpha-\alpha^2}{2} \\ 1 & \frac{12-\alpha-\alpha^2}{2} & \frac{48+3\alpha-\alpha^2}{2} \end{pmatrix}.$$

Now, we proceed to study the Hopf Galois module structure of $\mathcal{O}_L$. The Hermite normal form of $M(H_c, L)$ in the three cases is

$$D = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 3 \end{pmatrix}.$$

The inverse of this matrix gives the basis of $\mathfrak{A}_{L/\mathbb{Q}_3}$

$$\left\{ \mathrm{Id}, \sigma, \frac{\mathrm{Id}+\sigma+\sigma^2}{3} \right\}.$$

Note that this is coherent with the basis in (2.6) as the corresponding change of basis has determinant in $\mathbb{Z}_3^*$.

Let us study the existence of a normal integral basis generator. In this case, the index of the Hopf Galois structure is $I(H_c, L) = 1$. We proceed as usual: we try to find some $\beta = \sum_{i=1}^3 \beta_i \alpha^{i-1} \in \mathcal{O}_L$ for which $v_3(D_\beta(H_c, L)) = 1$.

For the polynomial $f(x) = x^3 - 3x^2 + 3$,

$$M_\beta(H_c, L) = \begin{pmatrix} \beta_1 & 6\beta_3 + 3\beta_2 + \beta_1 & 3\beta_3 + \beta_1 \\ \beta_2 & 3\beta_3 + \beta_2 & -3\beta_3 - 2\beta_2 \\ \beta_3 & -2\beta_3 - \beta_2 & \beta_3 + \beta_2 \end{pmatrix}.$$

which has determinant

$$D_\beta(H_c, L) = -3\left(\beta_2{}^2 + 3\beta_3\beta_2 + 3\beta_3{}^2\right)(\beta_1 + \beta_2 + 3\beta_3).$$

In particular, for $\beta = \alpha$, the previous determinant has 3-adic valuation 1. Then, $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_3}$-free and that $\beta = \alpha$ is a generator.

If $f(x) = x^3 - 3x^2 + 12$,

$$M_\beta(H_c, L) = \begin{pmatrix} \beta_1 & 69\beta_3 - 12\beta_2 + \beta_1 & -24\beta_3 + 9\beta_2 + \beta_1 \\ \beta_2 & -21\beta_3 + 4\beta_2 & 21\beta_3 - 5\beta_2 \\ \beta_3 & -5\beta_3 + \beta_2 & 4\beta_3 - \beta_2 \end{pmatrix},$$

which has determinant

$$D_\beta(H_c, L) = 3\left(\beta_2{}^2 - 9\beta_3\beta_2 + 21\beta_3{}^2\right)(\beta_1 - \beta_2 + 15\beta_3).$$

We obtain again that $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free and $\beta = \alpha$ is a generator.

Finally, for $f(x) = x^3 - 3x^2 + 21$, we have

$$M_\beta(H_c, L) = \begin{pmatrix} \beta_1 & 21\,\beta_3 - 9\,\beta_2 + \beta_1 & 24\,\beta_3 + 6\,\beta_2 + \beta_1 \\ \beta_2 & -\frac{3}{2}\,\beta_3 - \beta_2/2 & \frac{3}{2}\,\beta_3 - \beta_2/2 \\ \beta_3 & -\beta_{\frac{3}{2}} + \beta_2/2 & -\beta_{\frac{3}{2}} - \beta_2/2 \end{pmatrix},$$

and the determinant is

$$D_\beta(H_c, L) = \frac{3}{2}\,\left({\beta_2}^2 + 3\,{\beta_3}^2\right)(\beta_1 - \beta_2 + 15\,\beta_3)\,.$$

From this we deduce once again that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \alpha$.

Chapter 3

Quartic Galois extensions

We have just seen how the reduction method is well suited for absolute extensions of degree 2 and 3 of number or p-adic fields, in the sense that it provides a basis of the associated order as well as an answer to the question of the freeness of the ring of integers and, if it exists, the construction of a normal integral basis. In this chapter we move forward in this classification and consider extensions of degree 4.

Now, the situation is far more complicated. To start, there are two possibilities for the Galois group: it may be the cyclic group C_4 of order 4 or the Klein group $C_2 \times C_2$ (in this last case, it is also said that the extension is elementary abelian). Consequently, according to the terminology of Greither-Pareigis theory, Hopf Galois structures of L/K can be of type C_4 (cyclic Hopf Galois structures) or of type $C_2 \times C_2$ (elementary abelian Hopf Galois structures). In the first section of this chapter we will use Greither-Pareigis theorem to check that there are indeed Hopf Galois structures of both types, and we will determine a basis of the corresponding Hopf algebra for each case.

Once all Hopf Galois structures are determined, we will move to the context of absolute extensions of number or p-adic fields in order to study the Hopf Galois module structure of the ring of integers. In the global setting, we will consider successively cyclic and elementary abelian extensions of $\mathbb{Q}$. In the local case, we are done for tamely ramified extensions. Indeed, since order 4 groups are always abelian, Hopf algebras in Hopf Galois structures are commutative and then we can apply Theorem 1.32, which gives that the ring of integers is indeed free over the associated order at each Hopf Galois structure. For this reason, we will focus on the wild case, i.e, we choose the ground field to be $\mathbb{Q}_2$.

By Leopoldt's theorem, there is always freeness over the associated order in the classical Galois structure. Our computations will show that this result is not valid in non-classical Hopf Galois structures of biquadratic extensions of $\mathbb{Q}$. Actually, this had been shown by Truman for the tame case (see [Tru12]). We will see that our criteria match with his result and obtain similar conditions for the wild cases.

3.1 Determination of the Hopf Galois structures

The description of the Hopf Galois structures of L/K was carried out by Byott in [Byo02, Theorem 2.5] in the more general context of Galois extensions of degree p^2. We follow his approach for $p = 2$. Namely, let $T = \langle \tau \rangle$ be an order 2 subgroup of G and let $\sigma \in G - T$ such that $\sigma^2 = 1_G$ if $G \cong C_2 \times C_2$ and $\sigma^2 = \tau$ otherwise. Then, we have a presentation of G as follows:

$$G = \langle \sigma, \tau \,|\, \tau^2 = 1_G, \sigma\tau = \tau\sigma, \sigma^2 = \gamma \rangle, \tag{3.1}$$

where $\gamma = 1_G$ if $G \cong C_2 \times C_2$ and $\gamma = \tau$ otherwise.

Theorem 3.1. *The regular subgroups of* $\mathrm{Perm}(G)$ *normalized by* $\lambda(G)$ *are those of the form*

$$N_{T,d} = \langle \mu, \eta_d \rangle,$$

where $d \in \{0,1\}$, $T = \langle \tau \rangle$ runs through the order 2 subgroups of G and, fixing a presentation of G as in 3.1,

$$\mu(\sigma^k\tau^l) = \sigma^k\tau^{l-1},$$
$$\eta_d(\sigma^k\tau^l) = \sigma^{k-1}\tau^{l+(k-1)d}.$$

The action of G on the previous automorphisms is given by

$$g(\mu) = \mu \text{ for all } g \in G, \quad \sigma(\eta_d) = \mu^d\eta_d, \quad \tau(\eta_d) = \eta_d.$$

It follows immediately from the theorem that $\mu = \lambda(\tau) = (1_G, \tau)(\sigma, \sigma\tau)$. As for the other generator, we have at each case:

$$\eta_{T,0} = \begin{cases} (1_G, \sigma\tau, \tau, \sigma) & \text{if } G \cong C_4 \\ (1_G, \sigma)(\tau, \sigma\tau) & \text{if } G \cong C_2 \times C_2 \end{cases},$$
$$\eta_{T,1} = \begin{cases} (1_G, \sigma)(\tau, \sigma\tau) & \text{if } G \cong C_4 \\ (1_G, \sigma\tau, \tau, \sigma) & \text{if } G \cong C_2 \times C_2 \end{cases}.$$

Note that $\eta_{T,0} = \lambda(\sigma^{-1})$ regardless of the structure of G. We also deduce

$$\eta_{T,0}^2 = \begin{cases} \mu & \text{if } G \cong C_4 \\ \mathrm{Id} & \text{if } G \cong C_2 \times C_2 \end{cases},$$
$$\eta_{T,1}^2 = \begin{cases} \mathrm{Id} & \text{if } G \cong C_4 \\ \mu & \text{if } G \cong C_2 \times C_2 \end{cases}.$$

That is, if $G \cong C_4$, $N_{T,0} \cong C_4$ and $N_{T,1} \cong C_2 \times C_2$, and otherwise, $N_{T,0} \cong C_2 \times C_2$ and $N_{T,1} \cong C_4$.

Let us fix a presentation of the Galois group

$$G = \langle \sigma, \tau \,|\, \tau^2 = 1_G, \sigma\tau = \tau\sigma, \sigma^2 = \gamma \rangle$$

with γ as before, and define $T = \langle \tau \rangle$, so that by choosing σ we have a presentation as in (3.1). If $G \cong C_4$, L/K has two Hopf Galois structures: the classical one, which is given by $N_{T,0}$, and a non-classical Hopf Galois structure given by $N_{T,1}$.

Otherwise, if $G \cong C_2 \times C_2$, there are two Hopf Galois structures apart from those, which arise from replacing $T_1 := T$ by $T_2 := \langle \sigma \rangle$ and σ by τ for one of them, and T_1 by $T_3 := \langle \sigma\tau \rangle$ for the other one. Let us determine the corresponding permutation subgroups $N_{T_i,1}$ for $i \in \{2,3\}$. For $i = 2$, $N_{T_2,1} = \langle \mu_2, \eta_{T_2,1} \rangle$. Following the definition,

$$\mu_2(\sigma^k\tau^l) = \sigma^{k-1}\tau^l,$$

whence $\mu_2 = \lambda(\sigma)$. On the other hand,

$$\eta_{T_2,1}(\sigma^k\tau^l) = \sigma^{k+l-1}\tau^{l-1},$$

so $\eta_{T_2,1} = (1_G, \sigma\tau, \sigma, \tau)$. Finally, for $i = 3$, we have $N_{T_3,1} = \langle \mu_3, \eta_{T_3,1} \rangle$. We compute the generators:

$$\begin{aligned} \mu_3(\sigma^k\tau^l) &= \mu_3(\sigma^{k-l}(\sigma\tau)^l) \\ &= \sigma^{k-l}(\sigma\tau)^{l-1} \\ &= \sigma^{k-1}\tau^{l-1}, \\ \eta_{T_3,1}(\sigma^k\tau^l) &= \eta_{T_3,1}(\sigma^{k-l}(\sigma\tau)^l) \\ &= \sigma^{k-l-1}(\sigma\tau)^{l+k-l-1} \\ &= \sigma^{-l+2(k-1)}\tau^{k-1} = \sigma^l\tau^{k-1}. \end{aligned}$$

We deduce that $\mu_3 = \lambda(\sigma\tau) = (1, \sigma\tau)(\sigma, \tau)$ and $\eta_{T_3,1} = (1_G, \tau, \sigma\tau, \sigma)$.

Once the permutation subgroups are computed, we determine the corresponding Hopf algebras of those Hopf Galois structures by using Greither-Pareigis theorem. We know that the Hopf algebra of the classical Galois structure is the K-group algebra $H_c = K[G]$. Regarding the non-classical Hopf Galois structures (the unique one if G is cyclic), we must determine the action of G on the previous automorphisms. Following the last part of the statement of Theorem 3.1, we have

$$g(\mu) = \mu, \quad g(\eta_{T,0}) = \eta_{T,0}$$

for every $g \in G$, and also $\sigma(\eta_{T,1}) = \mu\eta_{T,1}$. At this point, we must separate cases.

3.1.1 Case 1: G is cyclic

The Hopf Galois structure given by $N := N_{T,1}$ is the unique non-classical one. Let $x \in H = L[N]^G$, so there are $x_i \in L$ such that

$$x = x_1\mathrm{Id} + x_2\mu + x_3\eta_{T,1} + x_4\mu\eta_{T,1}.$$

From the equality

$$\sigma(x) = x$$

it follows that $\sigma(x_i) = x_i$ for $i \in \{1,2\}$, so $x_1, x_2 \in K$, and also $\sigma(x_3) = x_4$ and $\sigma(x_4) = x_3$. This implies that $\sigma^2(x_3) = x_3$, so $x_3 \in E := L^{\langle\sigma^2\rangle}$, the unique quadratic subextension of L/K. Let $z \in L$ such that $z \notin K$ and $z^2 \in K$. Then $x_3 = x_3^{(1)} + x_3^{(2)}z$ and $x_4 = x_3^{(1)} - x_3^{(2)}z$ for some $x_3^{(j)} \in K$. Thus,

$$x = x_1\mathrm{Id} + x_2\mu + x_3^{(1)}(\eta_{T,1} + \mu\eta_{T,1}) + x_3^{(2)}z(\eta_{T,1} - \mu\eta_{T,1}).$$

Then, x belongs to the space generated by

$$\{\mathrm{Id}, \mu, \eta_{T,1} + \mu\eta_{T,1}, z(\eta_{T,1} - \mu\eta_{T,1})\}.$$

Since this space is contained in H and with the same dimension, they coincide. Hence, we have:

Proposition 3.2. *A cyclic quartic extension L/K has two Hopf Galois structures: the classical Galois structure H_c of type C_4 and a non-classical Hopf Galois structure H of type $C_2 \times C_2$ with K-basis*

$$\{\mathrm{Id}, \mu, \eta_{T,1} + \mu\eta_{T,1}, z(\eta_{T,1} - \mu\eta_{T,1})\},$$

where z is the square root of a non-square element in K.

3.1.2 Case 2: G is elementary abelian

In this case we have three non-classical Hopf Galois structures, given by $N_i = \langle \mu_i, \eta_{T_i,1}\rangle$ for $i \in \{1,2,3\}$, where we call $\mu_1 = \mu$. Let us determine the corresponding Hopf algebras.

For $i = 1$, we know that $\eta_{T_1,1} = (1_G, \sigma\tau, \tau, \sigma)$, $\sigma(\eta_{T_1,1}) = \mu_1\eta_{T_1,1}$ and $\tau(\eta_{T_1,1}) = \eta_{T_1,1}$. We proceed as in the previous case: Let $x = x_1\mathrm{Id} + x_2\mu_1 + x_3\eta_{T_1,1} + x_4\mu_1\eta_{T_1,1} \in H_1 = L[N_1]^G$, and from $\sigma(x) = x$ we deduce that $x_1, x_2 \in K$ and the equalities $\sigma(x_3) = x_4$ and $\sigma(x_4) = x_3$. Now, we have also that $\tau(x) = x$ with τ fixing $\eta_{T_1,1}$, whence $x_3, x_4 \in E_1 := L^{\langle\tau\rangle}$. Let $z \in E_1$ such that $z^2 \in K$ and $E_1 = K(z)$, and let $x_3^{(1)}, x_3^{(2)} \in K$ such that $x_3 = x_3^{(1)} + x_3^{(2)}z$. Then $x_4 = x_3^{(1)} - x_3^{(2)}z$, and we deduce as in the previous case that a basis of H_1 is

$$\{\mathrm{Id}, \mu_1, \eta_{T,1} + \mu_1\eta_{T_1,1}, z(\eta_{T,1} - \mu_1\eta_{T_1,1})\}.$$

We move on to the case when $i = 2$. Then $\sigma(\eta_{T_2,1}) = \eta_{T_2,1}$ and $\tau(\eta_{T_2,1}) = \mu_2\eta_{T_2,1}$. Then, for $H_2 = L[N_2]^G$ we obtain the same basis

$$\{\mathrm{Id}, \mu_2, \eta_{T_2,1} + \mu_2\eta_{T_2,1}, z(\eta_{T_2,1} - \mu_2\eta_{T_2,1})\},$$

with the difference that now $z \in E_2 := L^{\langle\sigma\rangle}$.

Finally, let us assume that $i = 3$, in which case $\sigma(\eta_{T_3,1}) = \tau(\eta_{T_3,1}) = \mu_3\eta_{T_3,1}$, so $\sigma\tau(\eta_{T_3,1}) = \eta_{T_3,1}$. Then a basis of $H_3 = L[N_3]^G$ is

$$\{\mathrm{Id}, \mu_3, \eta_{T_3,1} + \mu_3\eta_{T_3,1}, z(\eta_{T_3,1} - \mu_3\eta_{T_3,1})\},$$

with $z \in E_3 := L^{\langle\sigma\tau\rangle}$.

The preceding paragraphs prove the following:

Proposition 3.3. *Let L/K be a quartic elementary abelian extension with Galois group G and let E_1/K, E_2/K and E_3/K be its quadratic subextensions. The Hopf Galois structures of L/K are the classical one H_c, of type $C_2 \times C_2$, and three non-classical Hopf Galois structures $\{H_i\}_{i=1}^3$ of type C_4 such that for every $1 \leq i \leq 3$, the K-basis of H_i is*

$$\{\mathrm{Id}, \mu_i, \eta_{T_i,1} + \mu_i\eta_{T_i,1}, z_i(\eta_{T_i,1} - \mu_i\eta_{T_i,1})\},$$

where $z_i \in E_i - K$ and $z_i^2 \in K$.

3.2 Cyclic quartic extensions of $\mathbb{Q}$

Let $L/\mathbb{Q}$ be a Galois quartic extension of number fields.

By [Har+87, Theorem 1], $L/\mathbb{Q}$ is a cyclic quartic extension if and only if

$$L = \mathbb{Q}(\sqrt{a(d + b\sqrt{d})}),$$

where:

- $a \in \mathbb{Z}$ is odd square-free and $b \in \mathbb{Z}_{>0}$.
- $d = b^2 + c^2$ for some $c \in \mathbb{Z}_{>0}$ and d is square-free.

- $\gcd(a,d)=1$.

There is a result that gives explicitly an integral basis of L (see [HW90]):

Theorem 3.4. *Let $L/\mathbb{Q}$ be a cyclic quartic extension and let $a,b,c,d\in\mathbb{Z}$ as above. Define $z=\sqrt{a(d+b\sqrt{d})}$ and $w=\sqrt{a(d-b\sqrt{d})}$. Then, an integral basis of K is given as follows:*

1. *If $d\equiv 0\,(\operatorname{mod}2)$,*
$$B=\{1,\sqrt{d},z,w\}.$$
2. *If $d\equiv 1\,(\operatorname{mod}2)$ and $b\equiv 1\,(\operatorname{mod}2)$,*
$$B=\left\{1,\frac{1+\sqrt{d}}{2},z,w\right\}.$$
3. *If $d\equiv 1\,(\operatorname{mod}2)$, $b\equiv 0(\operatorname{mod}2)$ and $a+b\equiv 3\,(\operatorname{mod}4)$,*
$$B=\left\{1,\frac{1+\sqrt{d}}{2},\frac{z+w}{2},\frac{z-w}{2}\right\}.$$
4. *If $d\equiv 1\,(\operatorname{mod}2)$, $b\equiv 0(\operatorname{mod}2)$, $a+b\equiv 1\,(\operatorname{mod}4)$ and $a\equiv c\,(\operatorname{mod}4)$,*
$$B=\left\{1,\frac{1+\sqrt{d}}{2},\frac{1+\sqrt{d}+z+w}{4},\frac{1-\sqrt{d}+z-w}{4}\right\}.$$
5. *If $d\equiv 1\,(\operatorname{mod}2)$, $b\equiv 0(\operatorname{mod}2)$, $a+b\equiv 1\,(\operatorname{mod}4)$ and $a\equiv -c\,(\operatorname{mod}4)$,*
$$B=\left\{1,\frac{1+\sqrt{d}}{2},\frac{1+\sqrt{d}+z-w}{4},\frac{1-\sqrt{d}+z+w}{4}\right\}.$$

We know that in this case $L/\mathbb{Q}$ has two Hopf Galois structures. In the classical one, we fix the basis $\{1_G,\sigma,\sigma^2,\sigma^3\}$, where we choose $\sigma=(z,w,-z,-w)$. With regard to the non-classical one, we need to choose an element δ in the unique quadratic subextension of $L/\mathbb{Q}$, which is $\mathbb{Q}(\sqrt{d})$. Let us choose $\delta=\sqrt{d}$. Hence, the non-classical Hopf Galois structure $H_{T,1}$ has $\mathbb{Q}$-basis

$$\left\{\mathrm{Id},\mu,\eta_{T,1}+\mu\eta_{T,1},\sqrt{d}(\eta_{T,1}-\mu\eta_{T,1})\right\},$$

where $\mu=\lambda(\sigma^2)$ and $\eta_{T,1}=\lambda(\sigma)$. We call these elements w_1, w_2, w_3 and w_4, respectively.

For both Hopf Galois structures, in order to compute the Gram matrix in each case we proceed as follows: we compute the matrix $G(H,L_{B_c})$ where

$$B_c=\{1,\sqrt{d},z,w\},$$

and then we carry out the computation $G(H,L_B)=G(H,L_{B_c})P_{B_c}^{B}$, where B is the integral basis in Theorem 3.4. From now on, we call $B_c=\{e_1,e_2,e_3,e_4\}$ and $B=\{\gamma_1,\gamma_2,\gamma_3,\gamma_4\}$.

3.2.1 The classical Galois structure

Let us consider first the classical Galois structure H_c, whose action is easier to determine. The aforementioned Gram matrix is

$$G(H_c, L_{B_c}) = \begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ e_1 & -e_2 & e_4 & -e_3 \\ e_1 & e_2 & -e_3 & -e_4 \\ e_1 & -e_2 & -e_4 & e_3 \end{pmatrix}.$$

Case 1: $d \equiv 0 \pmod 2$

The integral basis B in L is the basis B_c, meaning that $\gamma_i = e_i$ for all i, and so

$$G(H_c, L_B) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & -\gamma_2 & \gamma_4 & -\gamma_3 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ \gamma_1 & -\gamma_2 & -\gamma_4 & \gamma_3 \end{pmatrix}.$$

The Hermite normal form of $M(H,L)$ is

$$D(H,L) = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix},$$

so $\mathfrak{A}_{L/\mathbb{Q}}$ has $\mathbb{Z}$-basis

$$\left\{1_G, \sigma, \frac{-1_G + \tau}{2}, \frac{-1_G + \sigma - \tau + \sigma\tau}{4}\right\}.$$

On the other hand, we have that

$$D_\beta(H_c, L) = -8\beta_1\beta_2(\beta_3^2 + \beta_4^2),$$

so $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free with generator $\beta = \gamma_1 + \gamma_2 + \gamma_3$.

Case 2: $d \equiv 1 \pmod 2$ **and** $b \equiv 1 \pmod 2$

The integral basis is formed by

$$\gamma_1 = e_1, \quad \gamma_2 = \frac{e_1 + e_2}{2}, \quad \gamma_3 = e_3, \quad \gamma_4 = e_4,$$

and then the matrix of the change of basis is

$$P_{B_c}^B = \begin{pmatrix} 1 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then, we compute

$$G(H_c, L_B) = G(H_c, L_{B_c})P_{B_c}^B = \begin{pmatrix} e_1 & \frac{e_1+e_2}{2} & e_3 & e_4 \\ e_1 & \frac{e_1-e_2}{2} & e_4 & -e_3 \\ e_1 & \frac{e_1+e_2}{2} & -e_3 & -e_4 \\ e_1 & \frac{e_1-e_2}{2} & -e_4 & e_3 \end{pmatrix}.$$

Now we must find the coordinates of the entries with respect to the basis B. To this end, for each entry we apply the matrix $P_B^{B_c}$ on the column vector of its coordinates with respect to B_c. On this way, we obtain

$$G(H_c, L_B) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & \gamma_4 & -\gamma_3 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & -\gamma_4 & \gamma_3 \end{pmatrix}.$$

The Hermite normal form of $M(H_c, L_B)$ is

$$D = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

which gives the basis of $\mathfrak{A}_{L/\mathbb{Q}}$

$$\left\{ 1_G, \sigma, \frac{-1_G + \sigma^2}{2}, \frac{-\sigma + \sigma^3}{2} \right\}.$$

Regarding the freeness, the matrix of the action is

$$M_\beta(H_c, L) = \begin{pmatrix} \beta_1 & \beta_1 + \beta_2 & \beta_1 & \beta_1 + \beta_2 \\ \beta_2 & -\beta_2 & \beta_2 & -\beta_2 \\ \beta_3 & -\beta_4 & -\beta_3 & \beta_4 \\ \beta_4 & \beta_3 & -\beta_4 & -\beta_3 \end{pmatrix},$$

with determinant $D_\beta(H_c, L) = -4\beta_2(\beta_3^2 + \beta_4^2)(2\beta_1 + \beta_2)$. For instance, $\beta = \gamma_1 - \gamma_2 + \gamma_3$ is a normal integral basis generator. We proceed in the same way for the rest of the cases.

Case 3: $d \equiv 1 \pmod 2$**,** $b \equiv 0 \pmod 2$ **and** $a + b \equiv 3 \pmod 4$

We have the integral basis B formed by

$$\gamma_1 = e_1, \quad \gamma_2 = \frac{e_1 + e_2}{2}, \quad \gamma_3 = \frac{e_3 + e_4}{2}, \quad \gamma_4 = \frac{e_3 - e_4}{2},$$

giving the change basis matrix

$$P_{B_c}^B = \begin{pmatrix} 1 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Then, the Gram matrix is

$$G(H_c, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & -\gamma_4 & \gamma_3 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & \gamma_4 & -\gamma_3 \end{pmatrix}.$$

The Hermite normal form of $M(H_c, L)$ is exactly the same as the one in the previous case, so we obtain again the basis of $\mathfrak{A}_{L/\mathbb{Q}}$

$$\left\{ 1_G, \sigma, \frac{-1_G + \sigma}{2}, \frac{-\sigma + \sigma^3}{2} \right\}.$$

On the other hand, for $\beta \in \mathcal{O}_L$, we have again $D_\beta(H_c, L) = -4\beta_2(\beta_3^2+\beta_4^2)(2\beta_1+\beta_2)$, so again $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free and $\beta = \gamma_1 - \gamma_2 + \gamma_3$ is a normal integral basis generator of $\mathcal{O}_L$.

Case 4: $d \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, $a+b \equiv 1 \pmod 4$ **and** $a \equiv c \pmod 4$

The elements of B are

$$\gamma_1 = e_1, \quad \gamma_2 = \frac{e_1+e_2}{2}, \quad \gamma_3 = \frac{e_1+e_2+e_3+e_4}{4}, \quad \gamma = \frac{e_1-e_2+e_3-e_4}{4},$$

and

$$G(H_c, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1-\gamma_2 & \gamma_1-\gamma_2-\gamma_4 & \gamma_3 \\ \gamma_1 & \gamma_2 & \gamma_2-\gamma_3 & \gamma_1-\gamma_2-\gamma_4 \\ \gamma_1 & \gamma_1-\gamma_2 & \gamma_4 & \gamma_2-\gamma_3 \end{pmatrix}.$$

The Hermite normal form of $M(H_c, L)$ in this case is the identity matrix, meaning that $\mathfrak{A}_{L/\mathbb{Q}} = \mathbb{Z}[G]$. Given $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L) = (\beta_3^2+\beta_4^2)(2\beta_2+\beta_3-\beta_4)(4\beta_1+2\beta_2+\beta_3+\beta_4),$$

and for $\beta = \gamma_2 - \gamma_3$ it equals 1, proving that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free with that β as generator.

Case 5: $d \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, $a+b \equiv 1 \pmod 4$ **and** $a \equiv -c \pmod 4$

The elements

$$\gamma_1 = e_1, \quad \gamma_2 = \frac{e_1+e_2}{2}, \quad \gamma_3 = \frac{e_1+e_2+e_3-e_4}{4}, \quad \gamma = \frac{e_1-e_2+e_3+e_4}{4}$$

form the integral basis B and

$$G(H_c, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1-\gamma_2 & \gamma_4 & \gamma_2-\gamma_3 \\ \gamma_1 & \gamma_2 & \gamma_2-\gamma_3 & \gamma_1-\gamma_2-\gamma_4 \\ \gamma_1 & \gamma_1-\gamma_2 & \gamma_1-\gamma_2-\gamma_4 & \gamma_3 \end{pmatrix}.$$

As in the previous case, the Hermite normal form of $M(H_c, L)$ is the identity matrix, so $\mathfrak{A}_{L/\mathbb{Q}} = \mathbb{Z}[G]$. On the other hand, given $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L) = -\left({\beta_3}^2+{\beta_4}^2\right)(2\,\beta_2+\beta_3-\beta_4)(4\,\beta_1+2\,\beta_2+\beta_3+\beta_4).$$

For $\beta_1 = \beta_4 = 0$, $\beta_2 = 1$ and $\beta_3 = -1$, this is -1. We deduce that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free with generator $\beta = \gamma_2 - \gamma_3$.

3.2.2 Non-classical Hopf Galois structure

Let us move on to the non-classical Hopf Galois structure $H := H_{T,1}$. The Gram matrix where in L we fix the basis B_c is

$$G(H, L_{B_c}) = \begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ e_1 & e_2 & -e_3 & -e_4 \\ 2e_1 & -2e_2 & 0 & 0 \\ 0 & 0 & 2w\sqrt{d} & -2z\sqrt{d} \end{pmatrix}.$$

Now, a difficulty arises: at this point, we are not able to write some of the entries in terms of B_c because products of the basic elements have appeared in the previous expressions. To solve it, we find the coordinates of those elements with respect to the basis $B_z = \{1, z, z^2, z^3\}$, and then we change to B_c.

We first determine the matrix of the change of basis from B_z to B_c. It can be easily seen that the irreducible polynomial of z is

$$f(x) = x^4 - 2adx^2 + a^2c^2d.$$

We have that $zw = ac\sqrt{d}$ (note that if $a < 0$ we choose $\sqrt{-n} = i\sqrt{n}$ in the positive imaginary axis). Operating, one determines

$$\frac{1}{z} = -\frac{1}{a^2c^2d}z^3 + \frac{2}{ac^2}z,$$

$$\sqrt{d} = \frac{1}{ab}z^2 - \frac{d}{b},$$

$$w = \frac{1}{abc}z^3 - \frac{b^2+d}{bc}z.$$

Then,

$$P_{B_z}^{B_c} = \begin{pmatrix} 1 & -\frac{d}{b} & 0 & 0 \\ 0 & 0 & 1 & -\frac{b^2+d}{bc} \\ 0 & \frac{1}{ab} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{abc} \end{pmatrix}.$$

Then, we compute

$$z\sqrt{d} = \frac{1}{ab}z^3 - \frac{d}{b}z,$$

$$w\sqrt{d} = -\frac{1}{ac}z^3 + \frac{2d}{c}z.$$

Applying $P_{B_c}^{B_z}$, we change back the coordinates to the basis B_c, obtaining

$$2w\sqrt{d} = 2ce_3 - 2be_4,$$

$$-2z\sqrt{d} = 2be_3 + 2ce_4$$

Then, the Gram matrix we had set at the beginning of this part becomes

$$G(H, L_{B_c}) = \begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ e_1 & e_2 & -e_3 & -e_4 \\ 2e_1 & -2e_2 & 0 & 0 \\ 0 & 0 & 2ce_3 - 2be_4 & 2be_3 + 2ce_4 \end{pmatrix}.$$

Case 1: $d \equiv 0 \pmod 2$

Since $\gamma_i = e_i$ for all i, the Gram matrix is

$$G(H, L_B) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ 2\gamma_1 & -2\gamma_2 & 0 & 0 \\ 0 & 0 & 2c\gamma_3 - 2b\gamma_4 & 2b\gamma_3 + 2c\gamma_4 \end{pmatrix}.$$

Using the matrix (B.1), we can reduce the matrix $M(H,L)$ to

$$\begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & -2c \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix}.$$

This is almost the Hermite normal form of $M(H,L)$, with the exception that $-c$ does not need to be in the fixed complete set of residues modulo b. Concretely, the Hermite normal form is

$$D(H,L) = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 2r \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix},$$

where $r \equiv -c \pmod{b}$ and $\lceil -\frac{|b|}{2} \rceil < r \leq \lfloor \frac{|b|}{2} \rfloor$. We deduce that $\mathfrak{A}_H$ has a $\mathbb{Z}$-basis given by the elements

$$\left\{ w_1, \frac{-w_1 + w_2}{2}, \frac{-w_1 - w_2 + w_3}{4}, \frac{rw_1 - rw_2 + w_4}{2b} \right\}.$$

Moreover, $I(H,L) = 16b$.

For an element $\beta \in \mathcal{O}_L$, we have that

$$D_\beta(H,L) = 16b\beta_1\beta_2(\beta_3^2 + \beta_4^2).$$

Then, we have that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_1 + \gamma_2 + \gamma_3$.

Example 3.5. Let $L = \mathbb{Q}(\sqrt{10 + \sqrt{10}})$, which gives $a = b = 1$, $c = 3$ and $d = 10$. Since d is even, the integral basis is formed by

$$\gamma_1 = 1, \quad \gamma_2 = \sqrt{10}, \quad \gamma_3 = z, \quad \gamma_4 = w,$$

where $z = \sqrt{10 + \sqrt{10}}$ and $w = \sqrt{10 - \sqrt{10}}$. The Hermite normal form is in this case

$$D(H,L) = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Hence, $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$\left\{ w_1, \frac{-w_1 + w_2}{2}, \frac{-w_1 - w_2 + w_3}{4}, \frac{w_4}{2} \right\}.$$

Example 3.6. Let $L = \mathbb{Q}(\sqrt{58 + 3\sqrt{58}})$, which gives $a = 1$, $b = 3$, $c = 7$ and $d = 58$. Then d is even and square-free, and $d = b^2 + c^2$. In this case, the Hermite normal form is

$$D(H,L) = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & -2 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix}.$$

Therefore, $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$\left\{ w_1, \frac{-w_1 + w_2}{2}, \frac{-w_1 - w_2 + w_3}{4}, \frac{-w_1 + w_2 + w_4}{6} \right\}.$$

Case 2: $d \equiv 1 \pmod 2$ **and** $b \equiv 1 \pmod 2$

We obtain

$$G(H,L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ 2\gamma_1 & 2\gamma_1 - 2\gamma_2 & 0 & 0 \\ 0 & 0 & c\gamma_3 - b\gamma_4 & b\gamma_3 + c\gamma_4 \end{pmatrix}.$$

In this case, the Hermite normal form is

$$D(H,L) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & -2c \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix},$$

with the exception that $-c$ does not need to be in the fixed complete set of residues modulo b. The unimodular matrix we have used is (B.2). Then, $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$\Big\{w_1, \frac{-w_1 + w_2}{2}, \frac{w_3}{2}, \frac{rw_1 - rw_2 + w_4}{2b}\Big\},$$

where r is the corresponding class of $-c$ modulo b. Moreover, we see that $I(H,L) = 8b$.

Let us study the freeness of $\mathcal{O}_L$. For $\beta \in \mathcal{O}_L$,

$$D_\beta(H,L) = 8b\beta_2(\beta_3^2 + \beta_4^2)(2\beta_1 + \beta_2).$$

Let $\beta = \gamma_2 + \gamma_3$. Then, for this β, $D_\beta(H,L) = 8b$, proving that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

Example 3.7. Let $L = \mathbb{Q}(\sqrt{5+\sqrt{5}})$, which gives $a = b = 1$, $c = 2$ and $d = 5$. Then b and d are both odd, so the integral basis is formed by

$$\gamma_1 = 1, \quad \gamma_2 = \frac{1+\sqrt{5}}{2}, \quad \gamma_3 = z, \quad \gamma_4 = w,$$

where $z = \sqrt{5+\sqrt{5}}$ and $w = \sqrt{5-\sqrt{5}}$. In this case, the Hermite normal form is

$$D(H,L) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

so $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$\Big\{w_1, \frac{-w_1 + w_2}{2}, \frac{w_3}{2}, \frac{w_4}{2}\Big\}.$$

Example 3.8. Let $L = \mathbb{Q}(\sqrt{109+3\sqrt{109}})$, which gives $a = 1$, $b = 3$, $c = 10$ and $d = 109$. In this case the Hermite normal form is

$$D(H,L) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & -2 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix},$$

which gives the $\mathbb{Z}$-basis of $\mathfrak{A}_H$

$$\Big\{w_1, \frac{-w_1 + w_2}{2}, \frac{w_3}{2}, \frac{-w_1 + w_2 + w_4}{6}\Big\}.$$

Case 3: $d \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$ **and** $a+b \equiv 3 \pmod 4$

The Gram matrix is

$$G(H,L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ 2\gamma_1 & 2\gamma_1 - 2\gamma_2 & 0 & 0 \\ 0 & 0 & 2c\gamma_3 + 2b\gamma_4 & -2b\gamma_3 + 2c\gamma_4 \end{pmatrix}.$$

In this case, we have used the unimodular matrix (B.3) and obtained exactly the same Hermite normal form as in the previous case, so the basis is also the same and $I(H,L) = 8b$.

Moving on to the freeness, for $\beta \in \mathcal{O}_L$ we have

$$D_\beta(H,L) = -8b\beta_2(\beta_3^2 + \beta_4^2)(2\beta_1 + \beta_2).$$

This is just the negative of the value of $D_\beta(H,L)$ obtained in the previous case, and since $I(H,L)$ is the same, we have that again $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_2 + \gamma_3$.

Example 3.9. Let $L = \mathbb{Q}(\sqrt{5+2\sqrt{5}})$. In this case, $a = c = 1$, $b = 2$ and $d = 5$, and the integral basis is as above. The Hermite normal form of $M(H,L)$ is

$$D(H,L) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix},$$

so $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$\left\{ w_1, \frac{-w_1 + w_2}{2}, \frac{w_3}{2}, \frac{w_1 - w_2 + w_4}{4} \right\}.$$

Example 3.10. Let $L = \mathbb{Q}(\sqrt{109 + 10\sqrt{109}})$. Then $L/\mathbb{Q}$ is on this case for $a = 1$, $b = 10$, $c = 3$ and $d = 109$. In this case, the Hermite normal form is

$$D(H,L) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & -6 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 20 \end{pmatrix},$$

giving the $\mathbb{Z}$-basis of $\mathfrak{A}_H$

$$\left\{ w_1, \frac{-w_1 + w_2}{2}, \frac{w_3}{2}, \frac{-3w_1 + 3w_2 + w_4}{20} \right\}.$$

Case 4: $d \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, $a + b \equiv 1 \pmod 4$ **and** $a \equiv c \pmod 4$

The Gram matrix is

$$G(H,L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_2 & \gamma_2 - \gamma_3 & \gamma_1 - \gamma_2 - \gamma_4 \\ 2\gamma_1 & 2\gamma_1 - 2\gamma_2 & \gamma_1 - \gamma_2 & \gamma_2 \\ 0 & 0 & h & h' \end{pmatrix},$$

where

$$h = -b\gamma_1 + (b-c)\gamma_2 + 2c\gamma_3 + 2b\gamma_4,$$

$$h' = -c\gamma_1 + (b+c)\gamma_2 - 2b\gamma_3 + 2c\gamma_4.$$

In this case, by using the matrix (B.4) we obtain as Hermite normal form of $M(H,L)$

$$D(H,L) = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & -c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 2b \end{pmatrix}.$$

We see that $I(H,L) = 2b$.

Regarding the freeness, for $\beta \in \mathcal{O}_L$,

$$-2b(\beta_3^2 + \beta_4^2)(2\beta_2 + \beta_3 - \beta_4)(4\beta_1 + 2\beta_2 + \beta_3 + \beta_4).$$

Let $\beta = \gamma_2 - \gamma_3$. Then, $D_\beta(H,L) = -2b$, so $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

Example 3.11. Let $L = \mathbb{Q}(\sqrt{39+6\sqrt{13}})$. This is of the usual form with $a = c = 3$, $b = 2$ and $d = 13$. The Hermite normal form is in this case

$$D(H,L) = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Then, the $\mathbb{Z}$-basis of $\mathfrak{A}_H$ is

$$\left\{ w_1, w_2, w_3, \frac{w_1 - w_2 - 2w_3 + w_4}{4} \right\}$$

Case 5: $d \equiv 1 \pmod 2$**,** $b \equiv 0 \pmod 2$**,** $a + b \equiv 1 \pmod 4$ **and** $a \equiv -c \pmod 4$

The Gram matrix is

$$G(H,L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_2 & \gamma_2 - \gamma_3 & \gamma_1 - \gamma_2 - \gamma_4 \\ 2\gamma_1 & 2\gamma_1 - 2\gamma_2 & \gamma_1 - \gamma_2 & \gamma_2 \\ 0 & 0 & h & h' \end{pmatrix},$$

where

$$h = b\gamma_1 - (b+c)\gamma_2 + 2c\gamma_3 - 2b\gamma_4,$$
$$h' = -c\gamma_1 + (-b+c)\gamma_2 + 2b\gamma_3 + 2c\gamma_4.$$

Using the matrix (B.5), we find that the Hermite normal form is the same as in Case 4, so again $I(H,L) = 2b$.

For $\beta \in \mathcal{O}_L$,

$$D_\beta(H,L) = 2b(\beta_3^2 + \beta_4^2)(2\beta_2 + \beta_3 - \beta_4)(4\beta_1 + 2\beta_2 + \beta_3 + \beta_4).$$

This is just the same as in the previous case up to sign. Then, once again $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_2 - \gamma_3$.

Example 3.12. Let $L = \mathbb{Q}(\sqrt{15+6\sqrt{5}})$, which has $a = 3$, $b = 2$, $c = 1$ and $d = 5$. For these values, a, b, c and d satisfy the congruences of the last case. Then, the Hermite normal form of $M(H, L)$ is

$$D(H,L) = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Then, $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$\left\{w_1, w_2, w_3, \frac{-w_1+w_2-2w_3+w_4}{4}\right\}.$$

3.2.3 Summary of results

Theorem 3.13. *Let $L/\mathbb{Q}$ be a cyclic quartic extension and adopt the notation of Theorem 3.4.*

1. *(Case 1) If $d \equiv 0 \pmod 2$:*

   (i) In the classical Galois structure, $\mathfrak{A}_{L/\mathbb{Q}}$ has $\mathbb{Z}$-basis

   $$\left\{1_G, \sigma, \frac{-1_G+\tau}{2}, \frac{-1_G+\sigma-\tau+\sigma\tau}{4}\right\}.$$

   (ii) The associated order $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

   $$\left\{w_1, \frac{-w_1+w_2}{2}, \frac{-w_1-w_2+w_3}{4}, \frac{rw_1-rw_2+w_4}{2b}\right\},$$

   where r is the class of $-c$ mod b.

   (iii) The element $\beta = \gamma_1+\gamma_2+\gamma_3$ is a free generator of $\mathcal{O}_L$ as both $\mathfrak{A}_{L/\mathbb{Q}}$-module and $\mathfrak{A}_H$-module.

2. *(Cases 2 and 3) If $d \equiv 1 \pmod 2$ and $a+b \equiv 3 \pmod 4$:*

   (i) In the classical Galois structure, $\mathfrak{A}_{L/\mathbb{Q}}$ has $\mathbb{Z}$-basis

   $$\left\{1_G, \sigma, \frac{-1_G+\tau}{2}, \frac{-\sigma+\sigma\tau}{2}\right\}.$$

   (ii) The associated order $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

   $$\left\{w_1, \frac{-w_1+w_2}{2}, \frac{w_3}{2}, \frac{rw_1-rw_2+w_4}{2b}\right\},$$

   where r is the class of $-c$ mod b.

   (iii) The element $\beta = \gamma_2+\gamma_3$ is a free generator of $\mathcal{O}_L$ as both $\mathfrak{A}_{L/\mathbb{Q}}$-module and $\mathfrak{A}_H$-module.

3. *(Cases 4 and 5) If $d \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, $a+b \equiv 1 \pmod 4$:*

   (i) In the classical Galois structure, $\mathfrak{A}_{L/\mathbb{Q}} = \mathbb{Z}[G]$.

   (ii) The associated order $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

   $$\left\{w_1, w_2, w_3, \frac{-sw_1+sw_2-w_3+w_4}{2b}\right\},$$

   where s is the class of c mod $2b$.

   (iii) The element $\beta = \gamma_2-\gamma_3$ is a free generator of $\mathcal{O}_L$ as both $\mathfrak{A}_{L/\mathbb{Q}}$-module and $\mathfrak{A}_H$-module.

3.3 Biquadratic extensions of $\mathbb{Q}$

If G is elementary abelian, $L/\mathbb{Q}$ is a biquadratic extension, so there exist different square-free integers $m, n \in \mathbb{Z}$ such that $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Let $k = \frac{mn}{d^2}$, where $d = \gcd(m, n)$. The following result gives an integral basis of $L/\mathbb{Q}$ in terms of m, n and k (see [Mar77, Exercise 2.43]).

Proposition 3.14. *An integral basis B of $L/\mathbb{Q}$ is given as follows:*

1. *If $m \equiv 3 \pmod 4$ and $n, k \equiv 2 (\mathrm{mod}\, 4)$,*
$$B = \left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}.$$
2. *If $m \equiv 1 \pmod 4$ and $n, k \equiv 2$ or $3 \pmod 4$,*
$$B = \left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}.$$
3. *If $m, n, k \equiv 1 \pmod 4$,*
$$B = \left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right\}.$$

Remark 3.15. In [Tru12, Proposition 2.1], Truman shows that a biquadratic extension $\mathbb{Q}(\sqrt{m}, \sqrt{n})/\mathbb{Q}$ is tamely ramified if and only if $m, n \equiv 1 \pmod 4$, which corresponds to our case 3. Thus, cases 1 and 2 correspond to wildly ramified biquadratic extensions.

Note that the previous cases cover all possible situations because m, n and k can be exchanged conveniently. Keeping the notation of Section 3.1, let E_1, E_2 and E_3 the quadratic subextensions of $L/\mathbb{Q}$. We can assume without loss of generality that $E_1 = \mathbb{Q}(\sqrt{m})$ and $E_2 = \mathbb{Q}(\sqrt{n})$, otherwise we would exchange m and n. Then, $E_3 = \mathbb{Q}(\sqrt{k})$.

We translate the strategy and the notation of the case $G \cong C_4$ to this one: for each Hopf Galois structure H of $L/\mathbb{Q}$ we first compute the Gram matrix $G(H, L_{B_c})$ where in L we fix the basis $B_c = \{1, \sqrt{m}, \sqrt{n}, \sqrt{k}\}$, and then change to an integral basis B of Proposition 3.14. We call $B_c = \{e_1, e_2, e_3, e_4\}$ and $B = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$. When we multiply the square roots with each other, we can replace them with their respective conjugates if necessary, so that the following relations always hold:

$$\sqrt{m}\sqrt{k} = \frac{m}{d}\sqrt{n}, \quad \sqrt{n}\sqrt{k} = \frac{n}{d}\sqrt{m}, \quad \sqrt{m}\sqrt{n} = d\sqrt{k}.$$

3.3.1 Classical Galois structure

As in the case $G \cong C_4$, let us begin with the classical Galois structure H_c. We fix the basis $\{1_G, \sigma, \tau, \sigma\tau\}$. Since

$$\begin{aligned} \sigma(\sqrt{m}) &= -\sqrt{m}, \quad \sigma(\sqrt{n}) = \sqrt{n}, \quad \sigma(\sqrt{k}) = -\sqrt{k}, \\ \tau(\sqrt{m}) &= \sqrt{m}, \quad \tau(\sqrt{n}) = -\sqrt{n}, \quad \tau(\sqrt{k}) = -\sqrt{k}, \\ \sigma\tau(\sqrt{m}) &= -\sqrt{m}, \quad \sigma\tau(\sqrt{n}) = -\sqrt{n}, \quad \sigma\tau(\sqrt{k}) = \sqrt{k}, \end{aligned}$$

we have

$$G(H_c, L_{B_c}) = \begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ e_1 & -e_2 & e_3 & -e_4 \\ e_1 & e_2 & -e_3 & -e_4 \\ e_1 & -e_2 & -e_3 & e_4 \end{pmatrix}.$$

Case 1: $m \equiv 3 \pmod 4$ **and** $n, k \equiv 2 (\mathrm{mod}\, 4)$

The integral basis B has elements

$$\gamma_1 = e_1, \quad \gamma_2 = e_2, \quad \gamma_3 = e_3, \quad \gamma_4 = \frac{e_3 + e_4}{2},$$

and the Gram matrix is

$$G(H_c, L_B) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & -\gamma_2 & \gamma_3 & \gamma_3 - \gamma_4 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ \gamma_1 & -\gamma_2 & -\gamma_3 & -\gamma_3 + \gamma_4 \end{pmatrix}.$$

The Hermite normal form of $M(H_c, L_B)$ is

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

This gives the basis of $\mathfrak{A}_{L/\mathbb{Q}}$

$$\left\{ 1_G, \sigma, \frac{-1_G + \sigma}{2}, \frac{-1_G + \sigma - \tau + \sigma\tau}{4} \right\}.$$

Given $\beta \in \mathcal{O}_L$, $D_\beta(H_c, L_B) = 8\beta_1\beta_2\beta_4(2\beta_3 + \beta_4)$. If we choose $\beta_1 = \beta_2 = \beta_4 = 1$ and $\beta_3 = 0$, then $D_\beta(H_c, L_B) = 8$, giving that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free with generator

$$\beta = \gamma_1 + \gamma_2 + \gamma_4.$$

Case 2: $m \equiv 1 \pmod 4$ **and** $n, k \equiv 2$ **or** $3 \pmod 4$

We have

$$\gamma_1 = e_1, \quad \gamma_2 = \frac{e_1 + e_2}{2}, \quad \gamma_3 = e_3, \quad \gamma_4 = \frac{e_3 + e_4}{2},$$

and then

$$G(H_c, L_B) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & \gamma_3 & \gamma_3 - \gamma_4 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & -\gamma_3 & -\gamma_3 + \gamma_4 \end{pmatrix}.$$

The Hermite normal form of $M(H_c, L_B)$ is

$$D = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

We deduce that $\mathfrak{A}_{L/\mathbb{Q}}$ has $\mathbb{Z}$-basis

$$\left\{1_G, \sigma, \frac{-1_G+\tau}{2}, \frac{-\sigma+\sigma\tau}{2}\right\}.$$

Given $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L_B) = 4\beta_2\beta_4(2\beta_3+\beta_4)(2\beta_1+\beta_2).$$

In particular, if $\beta = \gamma_2 + \gamma_4$, then $|D_\beta(H_c, L_B)| = 4 = |\det(D)|$, so $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free with generator β.

Case 3**:** $m, n, k \equiv 1 \pmod 4$

The integral basis B is formed by

$$\gamma_1 = e_1, \quad \gamma_2 = \frac{e_1+e_2}{2}, \quad \gamma_3 = \frac{e_1+e_3}{2}, \quad \gamma_4 = \frac{1}{4}e_1 + \frac{1}{4}e_2 + \frac{m}{4d}e_3 + \frac{1}{4}e_4,$$

and then

$$G(H_c, L_B) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1-\gamma_2 & \gamma_3 & \frac{d-m}{2d}\gamma_1 + \frac{m}{d}\gamma_3 - \gamma_4 \\ \gamma_1 & \gamma_2 & \gamma_1-\gamma_3 & \gamma_2-\gamma_4 \\ \gamma_1 & \gamma_1-\gamma_2 & \gamma_1-\gamma_3 & \frac{d+m}{2d}\gamma_1 - \gamma_2 - \frac{m}{d}\gamma_3 + \gamma_4 \end{pmatrix}.$$

By applying the unimodular matrix (B.12), we can reduce the matrix of the action $M(H_c, L_B)$ to the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \\ 0 & \frac{d+m}{2d} & 0 & \frac{d-m}{2d} \end{pmatrix}.$$

Since $m \equiv 1 \pmod 4$, m is odd, and since it is divisible by d, d is also odd. Hence $d+m$ is even. On the other hand, it is clearly divisible by d. Since d and 2 are coprime, $2d$ divides $d+m$; in other words, $\frac{d+m}{2d} \in \mathbb{Z}$. Subtracting $\frac{d+m}{2d} \in \mathbb{Z}$ times the second row to the fifth row and changing sign of the fifth row gives the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & \frac{m}{d} \end{pmatrix}.$$

Now, $\frac{m}{d}$ is odd because it divides m, so we easily arrive to the identity matrix

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

as Hermite normal form. Then, $I(H_c, L) = 1$ and $\mathfrak{A}_{L/\mathbb{Q}} = \mathbb{Z}[G]$. On the other hand, for $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L) = \beta_4(2\beta_2+\beta_4)(4\beta_1+2\beta_2+2\beta_3+\beta_4)\left(2\beta_3 + \frac{m}{d}\beta_4\right).$$

If $\frac{m}{d} \equiv 1 \pmod 4$, we choose

$$\beta_1 = \frac{1}{4}\left(-1+\frac{m}{d}\right), \quad \beta_2 = 0, \quad \beta_3 = -\frac{1}{2}\left(1+\frac{m}{d}\right), \quad \beta_4 = 1$$

and then $D_\beta(H_c, L) = 1$. Otherwise, if $\frac{m}{d} \equiv 3 \pmod 4$, the choice

$$\beta_1 = \frac{1}{4}\left(1+\frac{m}{d}\right), \quad \beta_2 = 0, \quad \beta_3 = -\frac{1}{2}\left(1+\frac{m}{d}\right), \quad \beta_4 = 1$$

gives $D_\beta(H_c, L) = -1$. Then, a normal integral basis generator is generated by

$$\beta = \begin{cases} \frac{1}{4}\left(-1+\frac{m}{d}\right)\gamma_1 - \frac{1}{2}\left(1+\frac{m}{d}\right)\gamma_3 + \gamma_4 & \text{if } \frac{m}{d} \equiv 1 \pmod 4, \\ \frac{1}{4}\left(1+\frac{m}{d}\right)\gamma_1 - \frac{1}{2}\left(1+\frac{m}{d}\right)\gamma_3 + \gamma_4 & \text{if } \frac{m}{d} \equiv 3 \pmod 4. \end{cases}$$

3.3.2 Non-classical Hopf Galois structures

Now, we study the non-classical Hopf Galois structures $H_i := H_{T_i,1}$. We have seen that they have bases

$$\left\{\mathrm{Id}, \mu_1, \eta_{T_1,1} + \mu_1\eta_{T_1,1}, \sqrt{m}(\eta_{T_1,1} - \mu_1\eta_{T_1,1})\right\},$$
$$\left\{\mathrm{Id}, \mu_2, \eta_{T_2,1} + \mu_2\eta_{T_2,1}, \sqrt{n}(\eta_{T_2,1} - \mu_2\eta_{T_2,1})\right\},$$
$$\left\{\mathrm{Id}, \mu_3, \eta_{T_3,1} + \mu_3\eta_{T_3,1}, \sqrt{k}(\eta_{T_3,1} - \mu_3\eta_{T_3,1})\right\},$$

respectively. We call them $\{u_i\}_{i=1}^4$, $\{v_i\}_{i=1}^4$ and $\{w_i\}_{i=1}^4$, respectively.

Case 1: $m \equiv 3 \pmod 4$ **and** $n, k \equiv 2 \pmod 4$

The Gram matrices are

$$G(H_1, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ 2\gamma_1 & -2\gamma_2 & 0 & 0 \\ 0 & 0 & -2d\gamma_3 + 4d\gamma_4 & (-\frac{m}{d} - d)\gamma_3 + 2d\gamma_4 \end{pmatrix},$$

$$G(H_2, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & -\gamma_2 & \gamma_3 & \gamma_3 - \gamma_4 \\ 2\gamma_1 & 0 & -2\gamma_3 & -\gamma_3 \\ 0 & -2d\gamma_3 + 4d\gamma_4 & 0 & -\frac{n}{d}\gamma_2 \end{pmatrix},$$

$$G(H_3, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & -\gamma_2 & -\gamma_3 & -\gamma_3 + \gamma_4 \\ 2\gamma_1 & 0 & 0 & \gamma_3 - 2\gamma_4 \\ 0 & -\frac{2m}{d}\gamma_3 & \frac{2n}{d}\gamma_2 & \frac{n}{d}\gamma_2 \end{pmatrix}.$$

Let us find the Hermite normal form of the corresponding matrices of the action.

We start with H_1. By means of the unimodular matrix (B.6), $M(H_1, L)$ can be reduced to

$$\begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 2d \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & d + \frac{m}{d} \\ 0 & 0 & 0 & 4d \end{pmatrix}.$$

In the last two rows of the matrix above, we can carry out Euclid's algorithm with $d+\frac{m}{d}$ and $4d$, until leaving $g=\gcd(d+\frac{m}{d},4d)$ in one row and 0 in the other. We claim that $g=4$. Indeed, since $m\equiv 3\,(\mathrm{mod}\,4)$ and $m=d\frac{m}{d}$, one of d and $\frac{m}{d}$ is 3 mod 4 and the other one is 1 mod 4. Then, 4 divides $d+\frac{m}{d}$. Now, assume that p is an odd prime dividing both $d+\frac{m}{d}$ and $4d$. The latter condition implies that p divides d, and then the former gives that p divides $\frac{m}{d}$. But since m is square-free, d and $\frac{m}{d}$ are coprime, so $\frac{m}{d}$ cannot be divisible by p. This proves that $g=4$ as claimed. Finally, we reduce the non-zero entry above this one. Since d is odd, $2d\equiv 2\,(\mathrm{mod}\,4)$, so we subtract $\frac{2d-2}{4}$ times the fourth row from the second one and obtain a 2 in the last entry of the second row. Thus, $M(H_1,L)$ has Hermite normal form

$$D(H_1,L)=\begin{pmatrix}1&1&2&0\\0&2&2&2\\0&0&4&0\\0&0&0&4\end{pmatrix}.$$

This leads to the index $I(H_1,L)=32$. Moreover, $\mathfrak{A}_{H_1}$ has $\mathbb{Z}$-basis

$$\Big\{u_1,\frac{-u_1+u_2}{2},\frac{-u_1-u_2+u_3}{4},\frac{u_1-u_2+u_4}{4}\Big\}.$$

For H_2, we can use the unimodular matrix (B.7) to reduce $M(H_2,L)$ to

$$\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&\frac{n}{d}\\0&0&0&-2d\end{pmatrix}.$$

To simplify the last two rows, we compute the greatest common divisor of $\frac{n}{d}$ and $2d$. Since $n\equiv 2\,(\mathrm{mod}\,4)$, $\frac{n}{d}\equiv 2\,(\mathrm{mod}\,4)$. Then, $\gcd(2d,\frac{n}{d})=2\gcd(d,\frac{n}{d})$. Now, since n is square-free and d is a divisor of n, the primes of the factorization of d are among the primes of the factorization of n and appear only once, so d and $\frac{n}{d}$ are coprime. Thus, $\gcd(2d,\frac{n}{d})=2$. Then, the Hermite normal form is

$$D(H_2,L)=\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&2\end{pmatrix}.$$

Then, the index of H_2 is $I(H_2,L)=8$ and $\mathcal{O}_L$ has $\mathbb{Z}$-basis

$$\Big\{v_1,\frac{-v_1+v_2}{2},\frac{-v_1-v_2+v_3}{4},\frac{v_4}{2}\Big\}.$$

For the third non-classical Hopf Galois structure, we may reduce $M(H_3,L)$ to the matrix

$$\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&\frac{n}{d}\\0&0&0&2\frac{m}{d}\end{pmatrix},$$

in this case using the matrix (B.8). Let us compute the greatest common divisor g of $\frac{n}{d}$ and $2\frac{m}{d}$. Since $m\equiv 3\,(\mathrm{mod}\,4)$, $\frac{m}{d}$ is odd, so $2\frac{m}{d}\equiv 2\,(\mathrm{mod}\,4)$. On the other hand, we know yet that $\frac{n}{d} \equiv 2 \pmod 4$. Then, $g = 2\gcd(\frac{m}{d}, \frac{n}{d}) = 2$, since d is the greatest common divisor of m and n. Therefore, the Hermite normal form is

$$D(H_3, L) = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

whence $I(H_3, L) = 8$ and $\mathfrak{A}_{H_2}$ has $\mathbb{Z}$-basis

$$\left\{w_1, \frac{-w_1 + w_2}{2}, \frac{-w_1 - w_2 + w_3}{4}, \frac{w_4}{2}\right\}.$$

Now, we study the freeness of $\mathcal{O}_L$ over its associated orders in H_1, H_2 and H_3. Given $\beta \in \mathcal{O}_L$,

$$D_\beta(H_1, L) = -32\beta_1\beta_2\left(d\beta_3^2 + d\beta_3\beta_4 + \frac{1}{4}\left(d + \frac{m}{d}\right)\beta_4^2\right),$$

$$D_\beta(H_2, L) = 8\beta_1(2\beta_3 + \beta_4)\left(2d\beta_2^2 + \frac{n}{2d}\beta_4^2\right),$$

$$D_\beta(H_3, L) = 8\beta_1\beta_4\left(2\frac{m}{d}\beta_2^2 + 2\frac{n}{d}\beta_3^2 + 2\frac{n}{d}\beta_3\beta_4 + \frac{n}{2d}\beta_4^2\right).$$

Proposition 3.16. *For $i \in \{1, 2, 3\}$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free if and only if there exist integers $a, b \in \mathbb{Z}$ such that:*

1. *$a^2 + mb^2 = \pm 4d$, if $i = 1$.*
2. *$a^2 + nb^2 = \pm 2d$, if $i = 2$.*
3. *$a^2 + kb^2 = \pm 2\frac{n}{d}$, if $i = 3$.*

If that is the case, then a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_{H_i}$-module is

$$\beta = \begin{cases} \gamma_1 + \gamma_2 + \frac{a-db}{2d}\gamma_3 + b\gamma_4 & \text{if } i = 1 \\ \gamma_1 + \frac{a}{2d}\gamma_2 + \frac{1-b}{2}\gamma_3 + b\gamma_4 & \text{if } i = 2 \\ \gamma_1 + \frac{b}{2}\gamma_2 + \frac{ad-n}{2n}\gamma_3 + \gamma_4 & \text{if } i = 3 \end{cases}$$

Proof. 1. We know that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if there is some $\beta \in \mathcal{O}_L$ such that $|D_\beta(H_1, L)| = 32$, that is,

$$\beta_1\beta_2\left(d\beta_3^2 + d\beta_3\beta_4 + \frac{1}{4}\left(d + \frac{m}{d}\right)\beta_4^2\right) = \pm 1,$$

which at the same time is equivalent to each factor being either 1 or -1. We can always choose $\beta_1, \beta_2 \in \{-1, 1\}$, so the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$ is equivalent to the existence of $\beta_3, \beta_4 \in \mathbb{Z}$ such that

$$d\beta_3^2 + d\beta_3\beta_4 + \frac{1}{4}\left(d + \frac{m}{d}\right)\beta_4^2 = s,$$

where $s \in \{-1, 1\}$ (we will alternatively use this notation for ±1). Now, we regard this equality as a quadratic equation in β_3 with parameter β_4, whose solutions are

$$\beta_3 = \frac{-d\beta_4 \pm \sqrt{\Delta}}{2d},$$

where Δ is the discriminant of the equation. Now, it has an integral solution if and only if Δ is a square and $2d$ divides at least one of $-d\beta_4 \pm \sqrt{\Delta}$. Now, it is easy to check that $\Delta = 4(-m\beta_4^2 + 4ds)$.

Assume that there are integers a and b as in the statement. Choosing $\beta_4 = b$, it turns out that $\Delta = 4a^2$, which is a square, and $-db + \sqrt{\Delta} = -db + 2a$. Note that since $a^2 + mb^2 = 4ds$ and d divides mb^2, it also divides a^2, whence d divides a because it is square-free. Thus, $-db + 2a$ is divisible by both 2 and d, hence by $2d$. Conversely, if $\mathcal{O}_L$ is $\mathfrak{A}_H$-free, this means that there are $\beta_3, \beta_4 \in \mathbb{Z}$ such that

$$d\beta_3^2 + d\beta_3\beta_4 + \frac{1}{4}\left(d + \frac{m}{d}\right)\beta_4^2 = s,$$

and then $\beta_3 = \frac{-d\beta_4 \pm \sqrt{-m\beta_4^2 + 4ds}}{2d} \in \mathbb{Z}$, so $a = \sqrt{-m\beta_4^2 + 4ds}$ and $b = \beta_4$ satisfy the condition of the statement.

2. The argument is essentially the same as in 1. In this case, the equation we must consider is

$$2d\beta_2^2 + \frac{n}{2d}\beta_4^2 = s,$$

with unknown β_2 and parameter β_4. Then, the discriminant is $\Delta = 4(-n\beta_4^2 + 2ds)$, and the solutions are $\beta_2 = \pm\frac{\sqrt{\Delta}}{4d}$. Thus, the existence of a and b satisfying $a^2 + nb^2 = 2ds$ is equivalent to Δ being a square with $\beta_4 = \pm b$. Namely $\Delta = 4(-nb^2 + 2ds) = 4a^2$, whence it must be $\beta_2 = \frac{a}{2d}$. This is an integer number: since $a^2 + nb^2 = 2ds$ and $2d$ divides n, $2d$ divides a^2, so $2d$ being square-free implies that $2d$ divides a. Moreover, $\beta_4 = \pm b$ must accomplish $2\beta_3 + \beta_4 = \pm 1$ for $\beta_3 \in \mathbb{Z}$. This is always possible because b is odd. Indeed, since $a^2 + nb^2 = 2ds$ and a is even, taking mod 4 gives $2b^2 \equiv 2 \pmod{4}$, whence b is odd.

3. Here the situation is slightly different. Now, the equation involved is

$$2\frac{n}{d}\beta_3^2 + 2\frac{n}{d}\beta_3\beta_4 + 2\frac{m}{d}\beta_2^2 + \frac{n}{2d}\beta_4^2 = s,$$

with unknown β_3 and parameter β_2. Since β_4 is a factor of $D_\beta(H_3, L)$, it must be $\beta_4 \in \{-1, 1\}$, and we may assume that $\beta_4 = 1$. Then, the quadratic equation has solutions

$$\beta_3 = \frac{-2\frac{n}{d} \pm \sqrt{\Delta}}{4\frac{n}{d}},$$

where

$$\Delta = 4\left(-4k\beta_2^2 + 2\frac{n}{d}s\right).$$

Then, there are a and b as in the statement if and only if Δ is a square with $\beta_2 = \pm\frac{b}{2}$. This value of β_2 actually corresponds to an integer number. Indeed, the equality $a^2 + kb^2 = 2\frac{n}{d}s$ implies that a is even because so are k and $2\frac{n}{d}s$, and then taking classes mod 4 gives that $2b^2 \equiv 0 \pmod{4}$, whence b is even. On the other hand, we then have

$$\beta_3 = \frac{-2\frac{n}{d} \pm 2a}{4\frac{n}{d}} = \frac{-n \pm ad}{2n},$$

which belongs to $\mathbb{Z}$ if and only if $\frac{n}{d}$ divides a. But this is ensured by the equality $a^2 + kb^2 = 2\frac{n}{d}s$, as $\frac{n}{d}$ divides k, hence a^2, and hence a because $\frac{n}{d}$ is square-free.

The factors of $D_\beta(H_3, L)$ other than the quadratic equation do not add any restriction.

□

Remark 3.17. The conditions obtained in Proposition 3.16 refer to the solvability in $\mathbb{Z}$ of equations of the form $x^2 - Dy^2 = N$, which is known as the generalized Pell equation or the Pell-Fermat equation. The equations of this type have been widely studied and algorithms of resolution have been developed (see for example [Coh07, Section 6.3.5]). This problem could also be approached by applying the general theory for the equation $ax^2 + bxy + cy^2 = N$ (see [Mat02]) to the quadratic factor of each $D_\beta(H_i, L)$.

Remark 3.18. Note that the quadratic factor of $D_\beta(H_3, L)$ is actually $2\frac{m}{d}\beta_2^2 + \frac{n}{2d}(2\beta_3 + \beta_4)^2$. Since $n \equiv k \equiv 2 \pmod 4$, we can exchange them in Proposition 3.16, which amounts to exchange H_2 and H_3. By the original result, we have that $\mathcal{O}_L$ is $\mathfrak{A}_{H_2}$-free if and only if the last factor $2d\beta_2^2 + \frac{n}{2d}\beta_4^2$ of $D_\beta(H_2, L)$ has some root as polynomial in β_2 with β_4 odd. Once we have exchanged m and n, the freeness of $\mathcal{O}_L$ as $\mathfrak{A}_{H_2}$-module is given by the third statement. Now, if we exchange m and n in the last factor of $D_\beta(H_3, L)$, this also exchanges d and $\frac{m}{d}$. We then obtain $2d\beta_2^2 + \frac{n}{2d}(2\beta_3 + \beta_4)^2$, recovering the last factor of $D_\beta(H_2, L)$ (or more precisely, we obtain the same equation in β_2), and our result is coherent. Moreover, if we exchange m and n in the Pell equations themselves, we deduce that the equation $x^2 + ny^2 = \pm 2d$ has some solution if and only if so has the equation $x^2 + ny^2 = \pm 2\frac{n}{d}$.

The equations in Proposition 3.16 may have infinitely many solutions if m, n or k are negative. In the following result we explore the situation when they are positive.

Proposition 3.19. *Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ be a biquadratic extension of $\mathbb{Q}$ with $m \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$. Call $d = \gcd(m, n)$, $k = \frac{mn}{d^2}$.*

1. *If $m > 0$, $\mathcal{O}_L$ is not $\mathfrak{A}_{H_1}$-free unless m and n are coprime, (in which case $\beta = \gamma_1 + \gamma_2 + \gamma_3$ is a generator) or $m = 3$ and n is divisible by 3 (in which case a generator is $\beta = \gamma_1 + \gamma_2 - \gamma_3 + 2\gamma_4$).*

2. *If $n > 0$ (resp. $k > 0$), then $\mathcal{O}_L$ is not $\mathfrak{A}_{H_2}$-free (resp. not $\mathfrak{A}_{H_3}$-free) unless $n = 2d$.*

Proof. 1. Let us suppose that there are $a, b \in \mathbb{Z}$ such that $a^2 + mb^2 = 4d$ (the minus sign cannot occur under these hypotheses). Since a and b are raised to the square, their signs do not matter, so we can assume without loss of generality that $a, b \geq 0$. From the equation we have that $4d - mb^2$ is a square, and in particular it is non-negative, that is $mb^2 \leq 4d$. Now, since d is square-free, $4d$ is not a square unless m and n are coprime, in which case $a^2 + mb^2 = 4$. Then, $(a, b) = (2, 0)$ or $(a, b) = (1, 1)$ and $m = 3$. Assume that m and n are not coprime, i.e. $d > 1$. Then $b \neq 0$, and the previous inequality $mb^2 \leq 4d$ gives $m \leq 4d$. Since d is a divisor of m and m is odd, it must be $m = qd$ with $q \in \{1, 3\}$. Then, $4d - mb^2 = (4 - qb^2)d$ must be a square. In particular, $4 - qb^2 \geq 0$, whence $b = 1$. Therefore, $(4 - q)d$ must be a square. For $q = 3$, this is d, which is not a square. Otherwise, for $q = 1$, $3d$ is a square if and only if $d = 3$. Then $m = 3$, and the equation $a^2 + 3b^2 = 12$ only has solutions $(a, b) = (0, 2)$ and $(a, b) = (3, 1)$. Finally, since $d = m = 3$ and d is the greatest common divisor of m and n, n must be divisible by 3.

2. If $n > 0$ and there are $a, b \in \mathbb{Z}$ such that $a^2 + nb^2 = 2d$, then $2d - nb^2$ is a square, and since $2d$ is square-free, $n \leq 2d$. Since d is odd and divisor of n

and $n \equiv 2 \pmod 4$, it must be $n = 2d$. Thus, $a^2 + 2db^2 = 2d$ is only satisfied for $(a,b) = (0,1)$. As for k, if there are $a, b \in \mathbb{Z}$ such that $a^2 + kb^2 = 2\frac{n}{d}$ and $2\frac{n}{d}$ is not a square, then we argue as before to obtain that $k = \frac{n}{d}$ or $k = 2\frac{n}{d}$. Both of them are impossible, the former because $a^2 + \frac{n}{d}b^2 = 2\frac{n}{d}$ has no integral solutions, and the latter because $2\frac{n}{d} \equiv 0 \pmod 4$. Hence $2\frac{n}{d}$ is a square, which implies $\frac{n}{d} = 2$, that is, $n = 2d$, and it must be $(a,b) = (2,0)$.

□

Corollary 3.20. *The unique totally real biquadratic extension $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ of $\mathbb{Q}$ with $m \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$ for which $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free for all $i \in \{1,2,3\}$ is $L = \mathbb{Q}(\sqrt{3}, \sqrt{2})$.*

Proof. Since $L/\mathbb{Q}$ is totally real, $m, n, k > 0$. By Proposition 3.19, $\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free only for m and n coprime or $m = 3$ and n divisible by 3. Now, $\mathcal{O}_L$ is $\mathfrak{A}_{H_2}$-free and $\mathfrak{A}_{H_3}$-free only for $n = 2d$, which in the first case gives $(m,n) = (3,2)$, and in the second one, $(m,n) = (3,6)$. But in this last case $k = 2$, so both refer to the same extension. □

Case 2: $m \equiv 1 \pmod 4$ and $n, k \equiv 2$ or $3 \pmod 4$

We have the Gram matrices:

$$G(H_1, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_2 & -\gamma_3 & -\gamma_4 \\ 2\gamma_1 & 2\gamma_1 - 2\gamma_2 & 0 & 0 \\ 0 & 0 & -2d\gamma_3 + 4d\gamma_4 & (-\frac{m}{d} - d)\gamma_3 + 2d\gamma_4 \end{pmatrix},$$

$$G(H_2, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & \gamma_3 & \gamma_3 - \gamma_4 \\ 2\gamma_1 & \gamma_1 & -2\gamma_3 & -\gamma_3 \\ 0 & -d\gamma_3 + 2d\gamma_4 & 0 & \frac{n}{d}\gamma_1 - \frac{2n}{d}\gamma_2 \end{pmatrix},$$

$$G(H_3, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & -\gamma_3 & -\gamma_3 + \gamma_4 \\ 2\gamma_1 & \gamma_1 & 0 & \gamma_3 - 2\gamma_4 \\ 0 & -\frac{m}{d}\gamma_3 & -\frac{2m}{d}\gamma_1 + \frac{4m}{d}\gamma_2 & -\frac{m}{d}\gamma_1 + \frac{2m}{d}\gamma_2 \end{pmatrix}.$$

Let us find the Hermite normal forms. For H_1, we may reduce the matrix of the action to

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 2d \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & \frac{m}{d} + d \\ 0 & 0 & 0 & 4d \end{pmatrix},$$

using the matrix (B.9). Again, we carry out Euclid's algorithm in the last two rows so as to leave 0 in one and the greatest common divisor of $\frac{m}{d} + d$ and $4d$ in the other. In this case, we have that $m = d\frac{m}{d} \equiv 1 \pmod 4$, so $d \equiv \frac{m}{d} \pmod 4$, and then $d + \frac{m}{d} \equiv 2 \pmod 4$. Thus, 2 is the greatest power of 2 dividing both $\frac{m}{d} + d$ and $4d$. Reasoning as in the previous case, the aforementioned greatest common divisor is 2. Therefore, the Hermite normal form in this case is

$$D(H_1, L) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

so $I(H_1, L) = 8$ and $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$\Big\{u_1, \frac{-u_1+u_2}{2}, \frac{u_3}{2}, \frac{u_4}{2}\Big\}.$$

For H_2, we can use (B.10) to reduce $M(H_2, L)$ to

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & \frac{n}{d} \\ 0 & 0 & 0 & d \end{pmatrix}.$$

Since n is square-free and d is a divisor of n, d and $\frac{n}{d}$ are coprime, so the Hermite normal form is

$$D(H_2, L) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

whence $I(H_3, L) = 2$. Moreover, $\mathcal{O}_L$ has $\mathfrak{A}_{H_2}$-basis

$$\Big\{v_1, v_2, \frac{-v_1-v_2+v_3}{2}, v_4\Big\}.$$

Finally, for H_3, we reduce $M(H_3, L)$ by means of (B.11) to the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & \frac{m}{d} \\ 0 & 0 & 0 & \frac{n}{d} \end{pmatrix}.$$

Clearly, $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$, so the Hermite normal form of $M(H_3, L)$ is

$$D(H_3, L) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then, $I(H_3, L) = 2$ and $\mathcal{O}_L$ has $\mathfrak{A}_{H_3}$-basis

$$\Big\{w_1, w_2, \frac{-w_1-w_2+w_3}{2}, w_4\Big\}.$$

Let us study the freeness. Given $\beta \in \mathcal{O}_L$,

$$D_\beta(H_1, L) = -8\beta_2(2\beta_1+\beta_2)\left(2d\beta_3^2 + 2d\beta_3\beta_4 + \frac{1}{2}\left(d + \frac{m}{d}\right)\beta_4^2\right),$$

$$D_\beta(H_2, L) = 4(2\beta_1+\beta_2)(2\beta_3+\beta_4)\left(d\beta_2^2 + \frac{n}{d}\beta_4^2\right),$$

$$D_\beta(H_3, L) = 4\beta_4(2\beta_1+\beta_2)\left(\frac{m}{d}\beta_2^2 + 4\frac{n}{d}\beta_3^2 + 4\frac{n}{d}\beta_3\beta_4 + \frac{n}{d}\beta_4^2\right).$$

We see that 4 divides $D_\beta(H_i, L)$ for $i \in \{2,3\}$ while $I(H_i, L) = 2$ for $i \in \{1,2\}$. Hence, $\mathcal{O}_L$ is neither $\mathfrak{A}_{H_2}$-free nor $\mathfrak{A}_{H_3}$-free. As for H_1, we have:

Proposition 3.21. *$\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free if and only if there exist integers $a, b \in \mathbb{Z}$ such that $a^2 + mb^2 = \pm 2d$. If it is so, a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_{H_1}$-module is*

$$\beta = \gamma_1 - \gamma_2 + \frac{a - db}{2d}\gamma_3 + b\gamma_4.$$

Proof. The proof follows the same procedure as in Proposition 3.16. In this case, the equation we consider is

$$2d\beta_3^2 + 2d\beta_3\beta_4 + \frac{1}{2}\left(d + \frac{m}{d}\right)\beta_4^2 = s,\, s \in \{-1, 1\},$$

with unknown β_3 and parameter β_4. The discriminant of the equation is $\Delta = 4(-\beta_4^2 m + 2ds)$, so this being a square is equivalent to the existence of a and b as in the statement with $\beta_4 = b$. Then, the solutions of the equation are $\beta_3 = \frac{-db \pm a}{2d}$. We can choose without loss of generality the plus sign. Let us check that this is actually an integer number. Indeed, from the equation $a^2 + mb^2 = 2ds$ we deduce that d divides a, and on the other hand taking classes mod 4 gives $a^2 + b^2 \equiv 2 \pmod{4}$ (since d must be odd because so is m), whence $a^2 \equiv b^2 \equiv 1 \pmod{4}$, so a and b are odd. Hence, $-db + a$ is even, which proves that it is divisible by $2d$. Finally, we are free to choose $\beta_1, \beta_2 \in \mathbb{Z}$ such that $\beta_2 = \pm 1$ and $2\beta_1 + \beta_2 = \pm 1$. □

Corollary 3.22. *If $m > 0$, $\mathcal{O}_L$ is not $\mathfrak{A}_{H_1}$-free.*

Proof. We follow the same strategy as in Proposition 3.19. Assume that there are integers $a, b \in \mathbb{Z}$ such that $a^2 + mb^2 = 2d$. Then it must be $m \leq 2d$, and since m is odd, necessarily $m = d$. But then we have $a^2 + db^2 = 2d$, which has no integral solutions. □

Case 3: $m, n, k \equiv 1 \pmod{4}$

In this case, the Gram matrices are

$$G(H_1, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_2 & \gamma_1 - \gamma_3 & \gamma_2 - \gamma_4 \\ 2\gamma_1 & 2\gamma_1 - 2\gamma_2 & \gamma_1 & \gamma_1 - \gamma_2 \\ 0 & 0 & x & y \end{pmatrix},$$

$$G(H_2, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & \gamma_3 & \left(\frac{1}{2} - \frac{m}{2d}\right)\gamma_1 + \frac{m}{d}\gamma_3 - \gamma_4 \\ 2\gamma_1 & \gamma_1 & 2\gamma_1 - 2\gamma_3 & \frac{(m+d)\gamma_1 - 2m\gamma_3}{2d} \\ 0 & z & 0 & t \end{pmatrix},$$

$$G(H_3, L) = \begin{pmatrix} \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \gamma_1 & \gamma_1 - \gamma_2 & \gamma_1 - \gamma_3 & \frac{d+m}{2d}\gamma_1 - \gamma_2 - \frac{m}{d}\gamma_3 + \gamma_4 \\ 2\gamma_1 & \gamma_1 & \gamma_1 & \frac{d-m}{2d}\gamma_1 + \gamma_2 + \frac{m}{d}\gamma_3 - 2\gamma_4 \\ 0 & \frac{m}{d}\gamma_1 - 2\frac{m}{d}\gamma_3 & -\frac{n}{d}\gamma_1 + \frac{2n}{d}\gamma_2 & \left(-\frac{m}{2d^2} + \frac{m}{2d}\right)\gamma_1 + \frac{m}{d^2}\gamma_2 - \frac{m}{d}\gamma_3 \end{pmatrix},$$

where

$$x = m\gamma_1 - 2d\gamma_2 - 2m\gamma_3 + 4d\gamma_4,$$
$$y = \frac{m(m+1)}{2d}\gamma_1 - m\gamma_2 - \frac{m(m+1)}{d}\gamma_3 + 2m\gamma_4,$$
$$z = m\gamma_1 - 2d\gamma_2 - 2m\gamma_3 + 4d\gamma_4,$$

$$t = \left(\frac{n}{2d} + \frac{m}{2}\right)\gamma_1 - \left(d + \frac{n}{d}\right)\gamma_2 - m\gamma_3 + 2d\gamma_4.$$

Let us find the Hermite normal form of each matrix of the action. Using the matrix (B.13), we can reduce the matrix of the action $M(H_1, L)$ to

$$\begin{pmatrix} 1 & 0 & 0 & m\left(\frac{m+1}{2d} - 1\right) \\ 0 & 1 & 0 & -m\left(\frac{m+1}{2d} - 1\right) \\ 0 & 0 & 1 & -\frac{m(m+1)}{2d} \\ 0 & 0 & 0 & \frac{m}{d}(m+1) \\ 0 & 0 & 0 & 2d \end{pmatrix}.$$

Now, we are interested in the greatest common divisor of $2d$ and $\frac{m}{d}(m+1)$. Since $\frac{m}{d}$ and $m+1$ are coprime, this is the product of $\gcd(\frac{m}{d}, 2d)$ and $\gcd(m+1, 2d)$. The first of these is 1 because $\frac{m}{d}$, 2 and d are pairwise coprime. As for the other one, $m+1$ and $2d$ are both 2 mod 4, and $m+1$ is coprime with d, hence the greatest common divisor is 2. Then, the matrix above is equivalent to

$$\begin{pmatrix} 1 & 0 & 0 & m\left(\frac{m+1}{2d} - 1\right) \\ 0 & 1 & 0 & -m\left(\frac{m+1}{2d} - 1\right) \\ 0 & 0 & 1 & -\frac{m(m+1)}{2d} \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

The entries above 2 in the fourth column reduce to 0 or 1 depending on their parity. Therefore, the Hermite normal form of $M(H_1, L)$ is:

$$D(H_1, L) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Then, $I(H_1, L) = 2$ and $\mathfrak{A}_{H_1}$ has $\mathbb{Z}$-basis

$$\left\{u_1, u_2, u_3, \frac{-u_3 + u_4}{2}\right\}.$$

For the second one, we first use (B.14) to reduce the matrix of the action to

$$\begin{pmatrix} 1 & 0 & 0 & \frac{3m^2+n}{2d} \\ 0 & 1 & 0 & \frac{-9m^2+n}{2d} \\ 0 & 0 & 1 & \frac{-2md-3m^2-n}{2d} \\ 0 & 0 & 0 & d + \frac{n}{d} \\ 0 & 0 & 0 & m + d \\ 0 & 0 & 0 & \frac{2n}{d} \\ 0 & 0 & 0 & 2d \end{pmatrix}.$$

Since the greatest common divisor of $2d$ and $\frac{2n}{d}$ is 2, arguing as in previous cases, we obtain that the Hermite normal form is

$$D(H_2, L) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

We then see that $I(H_2, L) = 2$ and $\mathfrak{A}_{H_2}$ has $\mathbb{Z}$-basis

$$\left\{v_1, v_2, v_3, \frac{-v_1 + v_2}{2}\right\}.$$

Finally, for H_3, we reduce $M(H_3, L)$ to

$$\begin{pmatrix} 1 & 0 & 0 & \frac{nd^2+m(m-n)d-m^2n}{2d^3} \\ 0 & 1 & 0 & \frac{nd^2+m(m-n)d-m^2n}{2d^3} \\ 0 & 0 & 1 & \frac{nd^2-m(m-n)d+m^2n}{2d^3} \\ 0 & 0 & 0 & \frac{m^2}{d^2}(d-n) \\ 0 & 0 & 0 & \frac{m+d}{d}\frac{m}{d} \\ 0 & 0 & 0 & \frac{m+n}{d} \\ 0 & 0 & 0 & \frac{2n}{d} \end{pmatrix}$$

by means of (B.15). Let us focus in the last two entries. Since m and n are 1 mod 4, $m + n$ is 2 mod 4, just as $2n$. Then, $\gcd(m + n, 2n) = 2\gcd(m + n, n) = 2d$. Thus, $\gcd(\frac{m+n}{d}, \frac{2n}{d}) = 2$. Therefore, the Hermite normal form of the matrix of the action is

$$D(H_3, L) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

We deduce that $I(H_3, L) = 2$ and $\mathfrak{A}_H$ has $\mathbb{Z}$-basis

$$\left\{w_1, w_2, w_3, \frac{-w_3 + w_4}{2}\right\}.$$

Regarding the freeness, for $\beta \in \mathcal{O}_L$, we have

$$D_\beta(H_1, L) = -2(2\beta_2 + \beta_4)(4\beta_1 + 2\beta_2 + 2\beta_3 + \beta_4)\left(2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2\right),$$

$$D_\beta(H_2, L) = 2\left(2\beta_3 + \frac{m}{d}\beta_4\right)(4\beta_1 + 2\beta_2 + 2\beta_3 + \beta_4)\left(2d\beta_2^2 + 2d\beta_2\beta_4 + \frac{1}{2}\left(d + \frac{n}{d}\right)\beta_4^2\right),$$

$$D_\beta(H_3, L) = 2\beta_4(4\beta_1 + 2\beta_2 + 2\beta_3 + \beta_4)q_3(\beta_1, \beta_2, \beta_3, \beta_4),$$

where

$$q_3(\beta_1, \beta_2, \beta_3, \beta_4) = 2\frac{m}{d}\beta_2^2 + 2\frac{m}{d}\beta_2\beta_4 + 2\frac{n}{d}\beta_3^2 + 2k\beta_3\beta_4 + \frac{m}{d}\frac{k+1}{2}\beta_4^2.$$

Proposition 3.23. *For $i \in \{1, 2, 3\}$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free if and only if there exist integers $a, b \in \mathbb{Z}$ such that:*

1. *$a^2 + mb^2 = \pm 2d$, if $i = 1$.*
2. *$a^2 + nb^2 = \pm 2d$, if $i = 2$.*
3. *$a^2 + kb^2 = \pm 2\frac{n}{d}$, if $i = 3$.*

In that case, a generator of $\mathcal{O}_L$ as $\mathfrak{A}_{H_i}$-module is

$$\beta = \begin{cases} \frac{mb-a}{4d}\gamma_1 + \frac{1-b}{2}\gamma_2 + \frac{-mb+a}{2}\gamma_3 + b\gamma_4 & \textit{if } i = 1 \textit{ and } a \equiv b \pmod 4 \\ \frac{mb-a-2d}{4d}\gamma_1 + \frac{1-b}{2}\gamma_2 + \frac{-mb+a}{2}\gamma_3 + b\gamma_4 & \textit{if } i = 1 \textit{ and } a \not\equiv b \pmod 4 \\ \frac{mb-a}{4d}\gamma_1 + \frac{-bd+a}{2d}\gamma_2 + \frac{1}{2}\left(1 - \frac{m}{d}b\right)\gamma_3 + b\gamma_4 & \textit{if } i = 2 \textit{ and } a \equiv b \pmod 4 \\ \frac{mb-a-2d}{4d}\gamma_1 + \frac{-bd+a}{2d}\gamma_2 + \frac{1}{2}\left(1 - \frac{m}{d}b\right)\gamma_3 + b\gamma_4 & \textit{if } i = 2 \textit{ and } a \not\equiv b \pmod 4 \\ \frac{1}{2}\left(\frac{1-b}{2} - \frac{-k+a}{2\frac{n}{d}}\right)\gamma_1 + \frac{b-1}{2}\gamma_2 + \frac{-k+a}{2\frac{n}{d}}\gamma_3 + \gamma_4 & \textit{if } i = 3 \textit{ and } \frac{1-b}{2} \equiv \frac{-k+a}{2\frac{n}{d}} \pmod 2 \\ \frac{1}{2}\left(\frac{-1-b}{2} - \frac{-k+a}{2\frac{n}{d}}\right)\gamma_1 + \frac{b-1}{2}\gamma_2 + \frac{-k+a}{2\frac{n}{d}}\gamma_3 + \gamma_4 & \textit{if } i = 3 \textit{ and } \frac{1-b}{2} \not\equiv \frac{-k+a}{2\frac{n}{d}} \pmod 2 \end{cases}$$

Proof. First, note that if a and b are integers that satisfy any of the equalities above, then a and b are necessarily odd. Indeed, Since $m, n, k \equiv 1 \pmod 4$, then taking classes mod 4 gives $a^2 + b^2 \equiv 2 \pmod 4$, whence it must be $a^2 \equiv b^2 \equiv 1 \pmod 4$. This is only possible when a and b are odd.

1. We proceed as in the previous cases. In this case, the equation to consider is

$$2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 = s_1,\ s_1 \in \{-1, 1\},$$

with unknown β_3 and parameter β_4. It has discriminant $\Delta = 4(-m\beta_4^2 + 2ds)$ and the solutions are $\frac{-2m\beta_4 \pm \sqrt{\Delta}}{4d}$. Let us choose the plus sign. Now, there are integers a and b as in the statement if and only if Δ is a square with $\beta_4 = b$, and the solution becomes $\beta_3 = \frac{-mb+a}{2d}$. This is an integer number because d divides both a and m, and $-mb + a$ is even. On the other hand, $\beta_4 = b$ must fulfill the equality $2\beta_2 + \beta_4 = s_2$, $s_2 \in \{-1, 1\}$, which is the case since b is odd. Replacing this into the equality $4\beta_1 + 2\beta_2 + 2\beta_3 + \beta_4 = s_3$, $s_3 \in \{-1, 1\}$, gives $4\beta_1 + 2\beta_3 = s_3 - s_2$. Since $s_3 - s_2 \in \{-2, 0, 2\}$, we need $2\beta_1 + \beta_3 \in \{-1, 0, 1\}$. Since there are both even and odd possibilities for this quantity, we can always find $\beta_1 \in \mathbb{Z}$ satisfying the equality, regardless of the parity of $\beta_3 = \frac{-mb+a}{2d}$.

2. In this case, the quadratic equation is

$$2d\beta_2^2 + 2d\beta_2\beta_4 + \frac{1}{2}\left(d + \frac{n}{d}\right)\beta_4^2 = s,$$

with unknown β_2 and parameter β_4. The discriminant is $\Delta = 4(-n\beta_4^2 + 2ds)$, and the solutions are $\frac{-2d\beta_4 \pm \sqrt{\Delta}}{4d}$. We see that there are integers a and b such that $a^2 + nb^2 = 2ds$ if and only if Δ is a square with $\beta_4 = b$. In that case, the solution becomes $\beta_2 = \frac{-bd+a}{2d}$. On the other hand, since b and $\frac{m}{d}$ are odd, any of the equality $2\beta_3 + \frac{m}{d}\beta_4 = \pm 1$ do not impose any restriction on $\beta_3 \in \mathbb{Z}$. Finally, neither do any of the equalities $4\beta_1 + 2\beta_2 + 2\beta_3 + \beta_4 = \pm 1$ on $\beta_1 \in \mathbb{Z}$. Indeed, this is equivalent to $2\beta_1 = \frac{\pm 1 - b}{2} - \beta_3 - \beta_4$, and we can choose conveniently the sign of the independent term in order to obtain an even number.

3. We must consider the equation

$$2\frac{m}{d}\beta_2^2 + 2\frac{m}{d}\beta_2\beta_4 + 2\frac{n}{d}\beta_3^2 + 2k\beta_3\beta_4 + \frac{m}{d}\frac{k+1}{2}\beta_4^2 = s,$$

and we choose unknown β_3 and parameters β_2 and β_4. The discriminant for this equation is $\Delta = 4((2\beta_2 + \beta_4)^2 k + 2\frac{n}{d}s)$, and the solutions are $\frac{-2k\beta_4 \pm \sqrt{\Delta}}{4\frac{n}{d}}$. There are integers a and b such that $a^2 + kb^2 = 2\frac{n}{d}s$ if and only if Δ is a square with $2\beta_2+\beta_4=b$. Since β_4 is one of the factors of $D_\beta(H_3,L)$, it must be $\beta_4=\pm1$, and since b is odd, there is $\beta_2\in\mathbb{Z}$ satisfying that equality. The solution then becomes $\beta_3=\frac{-k+a}{2\frac{n}{d}}$, which is an integer number because $-k+a$ is even and divisible by $\frac{n}{d}$. Finally, we need the equality $4\beta_1+2\beta_2+2\beta_3+\beta_4=\pm1$ to hold. This is equivalent to $4\beta_1+2\beta_2+2\beta_3+\beta_4=4\beta_1+2\beta_3=\pm1-b$, that is, $2\beta_1=\frac{\pm1-b}{2}-\beta_3$, and it does not impose any restriction on $\beta_1\in\mathbb{Z}$ because we can choose suitably the sign in the independent term so that it becomes an even number.

□

Remark 3.24. The criteria obtained in Proposition 3.23 were proved by Truman in [Tru12, Proposition 6.1] using the theory of idèles. In his case, he works indistinctly with a non-classical Hopf Galois structure of a tame biquadratic extension $\mathbb{Q}(\sqrt{m},\sqrt{n})/\mathbb{Q}$ and obtains the same condition for m. This fits with our result because m,n,k being 1 mod 4 allows to exchange them indistinctly. Our Propositions 3.16 and 3.21 show that $\mathcal{O}_L$ presents a similar behaviour as $\mathfrak{A}_{H_i}$-module for a wildly ramified biquadratic extension.

3.3.3 Summary of results

Let $L=\mathbb{Q}(\sqrt{m},\sqrt{n})$ be a biquadratic extension of $\mathbb{Q}$ with m and n square-free and let $k=\frac{mn}{d^2}$, where $d=\gcd(m,n)$.

Theorem 3.25 (Associated orders). *1. If $m\equiv3\pmod 4$ and $n,k\equiv2\pmod 4$, then:*

(i) The associated order $\mathfrak{A}_{L/\mathbb{Q}}$ in the classical Galois structure has $\mathbb{Z}$-basis

$$\Big\{1_G,\sigma,\frac{-1_G+\sigma}{2},\frac{-1_G+\sigma-\tau+\sigma\tau}{4}\Big\}.$$

(ii) The associated orders $\mathfrak{A}_{H_1}$, $\mathfrak{A}_{H_2}$ and $\mathfrak{A}_{H_3}$ in the non classical Hopf Galois structures have $\mathbb{Z}$-basis

$$\Big\{u_1,\frac{-u_1+u_2}{2},\frac{-u_1-u_2+u_3}{4},\frac{u_1-u_2+u_4}{4}\Big\},$$

$$\Big\{v_1,\frac{-v_1+v_2}{2},\frac{-v_1-v_2+v_3}{4},\frac{v_4}{2}\Big\},$$

$$\Big\{w_1,\frac{-w_1+w_2}{2},\frac{-w_1-w_2+w_3}{4},\frac{w_4}{2}\Big\},$$

respectively.

2. If $m\equiv1\pmod 4$ and $n,k\not\equiv1\pmod 4$, then:

(i) The classical associated order $\mathfrak{A}_{L/\mathbb{Q}}$ has $\mathbb{Z}$-basis

$$\Big\{1_G,\sigma,\frac{-1_G+\tau}{2},\frac{-\sigma+\sigma\tau}{2}\Big\}.$$

(ii) The non-classical associated orders $\mathfrak{A}_{H_i}$, $i\in\{1,2,3\}$, have $\mathbb{Z}$-bases

$$\Big\{u_1,\frac{-u_1+u_2}{2},\frac{u_3}{2},\frac{u_4}{2}\Big\},$$

$$\Big\{v_1,v_2,\frac{-v_1-v_2+v_3}{2},v_4\Big\},$$

$$\Big\{w_1,w_2,\frac{-w_1-w_2+w_3}{2},w_4\Big\}.$$

3. *If $m, n, k \equiv 1 \pmod 4$, then:*

   (i) *The elements of G form a $\mathbb{Z}$-basis of $\mathfrak{A}_{L/\mathbb{Q}}$.*

   (ii) *The associated orders $\mathfrak{A}_{H_1}$, $\mathfrak{A}_{H_2}$ and $\mathfrak{A}_{H_3}$ have $\mathbb{Z}$-bases*
$$\left\{u_1, u_2, u_3, \frac{-u_3+u_4}{2}\right\},$$
$$\left\{v_1, v_2, v_3, \frac{-v_3+v_4}{2}\right\},$$
$$\left\{w_1, w_2, w_3, \frac{-w_3+w_4}{2}\right\}.$$

Theorem 3.26 (Freeness). 1. *If $m \equiv 3 \pmod 4$ and $n, k \equiv 2 \pmod 4$, then:*

   (i) *The element $\beta = 1 + \sqrt{m} + \frac{\sqrt{n}+\sqrt{k}}{2}$ is a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_{L/\mathbb{Q}}$-module.*

   (ii) *$\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free (resp. $\mathfrak{A}_{H_2}$-free, resp. $\mathfrak{A}_{H_3}$-free) if and only if there are integers a, b such that $a^2 + mb^2 = \pm 4d$ (resp. $a^2 + nb^2 = \pm 2d$, resp. $a^2 + kb^2 = \pm 2\frac{n}{d}$).*

2. *If $m \equiv 1 \pmod 4$ and $n, k \not\equiv 1 \pmod 4$, then:*

   (i) *A generator of $\mathcal{O}_L$ as $\mathfrak{A}_{L/\mathbb{Q}}$-module is $\beta = \gamma_2 + \gamma_4$*

   (ii) *$\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free if and only if there are integers a, b such that $a^2 + mb^2 = \pm 2d$. Moreover, $\mathcal{O}_L$ is never $\mathfrak{A}_{H_2}$-free nor $\mathfrak{A}_{H_3}$-free.*

3. *If $m, n, k \equiv 1 \pmod 4$, then:*

   (i) *$\mathcal{O}_L$ has $\mathfrak{A}_{L/\mathbb{Q}}$-generator*
$$\beta = \begin{cases} \frac{1}{4}\left(-1+\frac{m}{d}\right)\gamma_1 - \frac{1}{2}\left(1+\frac{m}{d}\right)\gamma_3 + \gamma_4 & \text{if } \frac{m}{d} \equiv 1 \pmod 4, \\ \frac{1}{4}\left(1+\frac{m}{d}\right)\gamma_1 - \frac{1}{2}\left(1+\frac{m}{d}\right)\gamma_3 + \gamma_4 & \text{if } \frac{m}{d} \equiv 3 \pmod 4). \end{cases}.$$

   (ii) *$\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free (resp. $\mathfrak{A}_{H_2}$-free, resp. $\mathfrak{A}_{H_3}$-free) if and only if there are integers a, b such that $a^2 + mb^2 = \pm 2d$ (resp. $a^2 + nb^2 = \pm 2d$, resp. $a^2 + kb^2 = \pm 2\frac{n}{d}$).*

3.4 Totally ramified cyclic quartic extensions of $\mathbb{Q}_2$

If $L/\mathbb{Q}_2$ is a totally ramified cyclic quartic extension of 2-adic fields, L is the splitting field over $\mathbb{Q}_2$ of one of the polynomials
$$x^4 \pm 4x^2 + 2, \quad x^4 \pm 20x^2 + 50, \quad x^4 \pm 52x^2 + 26, \quad x^4 \pm 20x^2 + 10.$$

The first four polynomials correspond to the liftings of $\mathbb{Q}(\sqrt{2})$ to cyclic quartic extensions and appear in [Rio95, Section 2.7]. The other ones generate the liftings of $\mathbb{Q}_2(\sqrt{10})$ and are taken from the online database [LMFDB]. Looking at the roots of these polynomials (that can be computed easily as solutions of a biquadratic equation), we see that there are $a, b, c, d \in \mathbb{Z}_2$ for which $L/\mathbb{Q}_2$ is as in [Har+87, Theorem 1] and $f(x) = x^4 - 2adx^2 + a^2c^2d$. The relations determined in Section 3.2 remain valid in this case. Then
$$w = \frac{1}{abc}z^3 - \frac{b^2+d}{bc}z.$$

When f is 2-Eisenstein, $B = \{1, z, z^2, z^3\}$ is an integral basis of L. For this reason, we will need also the coordinates of the powers of w:
$$w^2 = -z^2 + 2ad,$$
$$w^3 = \frac{b^2+d}{bc}z^3 - \frac{ad}{bc}(d+3b^2)z.$$

3.4.1 Classical Galois structure

We begin with the classical Galois structure. The Gram matrix where in L we fix the basis of the powers of z is

$$G(H_c, L_B) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & w & w^2 & w^3 \\ 1 & -z & z^2 & -z^3 \\ 1 & -w & w^2 & -w^3 \end{pmatrix}.$$

Case 1: $f(x) = x^4 + 4sx^2 + 2$, $s \in \{-1, 1\}$

The roots of f are

$$z = \sqrt{-s(2+\sqrt{2})}, \quad w = \sqrt{-s(2-\sqrt{2})}$$

and the negatives. Then $a = -s$, $b = c = 1$ and $d = 2$. Since f is 2-Eisenstein, B is an integral basis of L. Now, we have $w = -3z - sz^3$, $w^2 = -4s - z^2$ and $w^3 = 10sz + 3z^3$. Then, the Gram matrix is

$$G(H_c, L) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -3z - sz^3 & -4s - z^2 & 10sz + 3z^3 \\ 1 & -z & z^2 & -z^3 \\ 1 & 3z + sz^3 & -4s - z^2 & -10sz - 3z^3 \end{pmatrix}.$$

The Hermite normal form of the matrix of the action is

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix},$$

which gives the basis of $\mathfrak{A}_{L/\mathbb{Q}_2}$

$$\left\{ 1_G, \sigma, \frac{-1_G + \sigma^2}{2}, \frac{-1_G + \sigma - \sigma^2 + \sigma^3}{4} \right\}.$$

We also deduce that $I(H_c, L) = v_2(\det(D)) = 3$. If $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L) = -8\,\beta_3 \left({\beta_2}^2 s + 10\,{\beta_4}^2 s - 6\,\beta_2\,\beta_4 \right) \left(-2\,\beta_3\,s + \beta_1 \right).$$

If $\beta_1 = \beta_2 = \beta_3 = 1$ and $\beta_4 = 0$, then this is $16 - 8s$, which has 2-adic valuation 3, so $\beta = 1 + z + z^2$ is a normal integral basis generator.

Case 2: $f(x) = x^4 + 20sx^2 + 50$, $s \in \{1, -1\}$

In this case, the roots of f are

$$z = \sqrt{-5s(2+\sqrt{2})}, \quad w = \sqrt{-5s(2-\sqrt{2})},$$

and the negatives, and we have $a = -5s$, $b = c = 1$ and $d = 2$. The Gram matrix is in this case

$$G(H_c, L) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -3z - \frac{s}{5}z^3 & -20s - z^2 & 50sz + 3z^3 \\ 1 & -z & z^2 & -z^3 \\ 1 & 3z + \frac{s}{5}z^3 & -20s - z^2 & -(50sz + 3z^3) \end{pmatrix}.$$

The Hermite normal form of $M(H_c, L)$ turns out to be

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Then, as before, $I(H_c, L) = 3$ and $\mathfrak{A}_{L/\mathbb{Q}_2}$ has $\mathbb{Z}_2$-basis

$$\left\{ 1_G, \sigma, \frac{-1_G + \sigma^2}{2}, \frac{-1_G + \sigma - \sigma^2 + \sigma^3}{4} \right\}.$$

For $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L) = \frac{8\beta_3 \left({\beta_2}^2 s + 250\, {\beta_4}^2 s - 30\, \beta_2\, \beta_4 \right) (-10\, \beta_3\, s + \beta_1)}{5}.$$

In particular, if $\beta = 1 + z + z^2$, then $v_3(D_\beta(H_c, L)) = 3$, so β is a normal integral basis generator.

Case 3: $f(x) = x^4 + 52sx^2 + 26$, $s \in \{-1, 1\}$

The roots are $z = \sqrt{-s(26 + 5\sqrt{26})}$, $w = \sqrt{-s(26 - 5\sqrt{26})}$, $-z$ and $-w$. Then $a = -s$, $b = 5$, $c = 1$ and $d = 26$. The Gram matrix in this case is

$$G(H_c, L) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -\frac{51z+sz^3}{5} & -52s - z^2 & \frac{2626sz+51z^3}{5} \\ 1 & -z & z^2 & -z^3 \\ 1 & \frac{51z+sz^3}{5} & -52s - z^2 & -\frac{2626sz+51z^3}{5} \end{pmatrix}.$$

We obtain once again as Hermite normal form of $M(H_c, L)$

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix},$$

whence $I(H_c, L) = 3$ and a $\mathbb{Z}_2$-basis of $\mathfrak{A}_{L/\mathbb{Q}_2}$

$$\left\{ 1_G, \sigma, \frac{-1_G + \sigma^2}{2}, \frac{-1_G + \sigma - \sigma^2 + \sigma^3}{4} \right\}.$$

For $\beta \in \mathcal{O}_L$, one computes

$$D_\beta(H_c, L) = -\frac{8\beta_3 \left({\beta_2}^2 s + 2626\, {\beta_4}^2 s - 102\, \beta_2\, \beta_4 \right) (-26\, \beta_3\, s + \beta_1)}{5}.$$

For $\beta = 1 + z + z^2$, we have $D_\beta(H_c, L) = \frac{208}{5} - \frac{8s}{5}$, with 2-adic valuation 3, so this β is a normal integral basis generator of L.

Case 4: $f(x) = x^4 + 20sx^2 + 10$, $s \in \{-1, 1\}$

Now, we have

$$z = \sqrt{-s(10 + 3\sqrt{10})}, \quad w = \sqrt{-s(10 - 3\sqrt{10})}.$$

Then, $a = -s$, $b = 3$, $c = 1$ and $d = 10$. The Gram matrix in this case is

$$G(H_c, L) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -\frac{19z+sz^3}{3} & -20s - z^2 & \frac{370sz+19z^3}{3} \\ 1 & -z & z^2 & -z^3 \\ 1 & \frac{19z+sz^3}{3} & -20s - z^2 & -\frac{370sz+19z^3}{3} \end{pmatrix}.$$

This leads to exactly the same Hermite normal form

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

as in the previous cases, so the basis of $\mathfrak{A}_{L/\mathbb{Q}_2}$ is the same as above. On the other hand, for $\beta \in \mathcal{O}_L$, we have

$$D_\beta(H_c, L) = -\frac{8\beta_3 \left(\beta_2{}^2 s + 370\,\beta_4{}^2 s - 38\,\beta_2\,\beta_4\right)(-10\,\beta_3\,s + \beta_1)}{3}.$$

In particular, for $\beta = 1 + z + z^2$, one obtains $D_\beta(H_c, L) = \frac{80}{3} - \frac{8s}{3}$, so this is a normal integral basis generator of $\mathcal{O}_L$.

3.4.2 Non-classical Hopf Galois structure

Now, we consider the non-classical Hopf Galois structure $H := H_{T,1}$ of $L/\mathbb{Q}_2$. The Gram matrix where in L we fix the basis $B = \{1, z, z^2, z^3\}$ is

$$G(H, L_B) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -z & -z^2 & z^3 \\ 2 & 0 & 2w^2 & 0 \\ 0 & 2w\sqrt{d} & 0 & 2w^3\sqrt{d} \end{pmatrix}.$$

Let us determine the entries in the last row in terms of the basis of the powers of z. We know by Section 3.2.2 that

$$w\sqrt{d} = -\frac{1}{ac}z^3 + \frac{2d}{c}z.$$

Using the expression of w^2 computed in the Galois case,

$$w^3\sqrt{d} = -\frac{2d}{c}z^3 + \frac{4ad^2}{c}z - acdz.$$

Then, the Gram matrix results as follows:

$$G(H, L_B) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -z & z^2 & -z^3 \\ 2 & 0 & -2z^2 + 4ad & 0 \\ 0 & -\frac{2}{ac}z^3 + \frac{4d}{c}z & 0 & -\frac{4d}{c}z^3 + \left(\frac{8ad^2}{c} - 2acd\right)z \end{pmatrix}.$$

Case 1: $f(x) = x^4 + 4sx^2 + 2$, $s \in \{-1, 1\}$

The Gram matrix above becomes

$$G(H,L) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -z & z^2 & -z^3 \\ 2 & 0 & -8s - 2z^2 & 0 \\ 0 & 8z + 2sz^3 & 0 & -28sz - 8z^3 \end{pmatrix}.$$

Now, the Hermite normal form of $M(H,L)$ is

$$D(H,L) = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

which yields the basis of $\mathfrak{A}_H$

$$\left\{ w_1, \frac{-w_1 + w_2}{2}, \frac{-w_1 - w_2 + w_3}{4}, \frac{w_4}{2} \right\}.$$

Moreover, $I(H,L) = 4$. On the other hand, given $\beta \in \mathcal{O}_L$, we have

$$D_\beta(H,L) = 16\beta_3(\beta_1 - 2s\beta_3)(s\beta_2^2 + 14s\beta_4^2 - 8\beta_2\beta_4).$$

For $\beta = 1 + z + z^2$, we obtain $D_\beta(H,L) = 16s - 32$, which has 2-adic valuation 4, so $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

Case 2: $f(x) = x^4 + 20sx^2 + 50$, $s \in \{1, -1\}$

The Gram matrix of H is in this case

$$G(H,L) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -z & z^2 & -z^3 \\ 2 & 0 & -40s - 2z^2 & 0 \\ 0 & 8z + \frac{2s}{5}z^3 & 0 & -140sz - 8z^3 \end{pmatrix}.$$

We obtain the same Hermite normal form as in the previous case, and hence the same basis for the associated order. Regarding the freeness, for $\beta \in \mathcal{O}_L$,

$$D_\beta(H,L) = \frac{16\,\beta_3\,\left({\beta_2}^2 s + 350\,{\beta_4}^2 s - 40\,\beta_2\,\beta_4\right)(-10\,\beta_3\,s + \beta_1)}{5}.$$

In particular, this equals $-32 + \frac{16s}{5}$ for $\beta = 1 + z + z^2$, so $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

Case 3: $f(x) = x^4 + 52sx^2 + 26$, $s \in \{-1, 1\}$

In this case,

$$G(H,L) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -z & z^2 & -z^3 \\ 2 & 0 & -104s - 2z^2 & 0 \\ 0 & 104z + 2sz^3 & 0 & -5356sz - 104z^3 \end{pmatrix}.$$

In this case, we obtain as Hermite normal form

$$D(H,L) = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

once again. Now, given $\beta \in \mathcal{O}_L$,

$$D_\beta(H,L) = 16\beta_3(s\beta_2^2 + 2678s\beta_4^2 - 104\beta_2\beta_4)(\beta_1 - 26s\beta_3).$$

In particular, for $\beta = 1 + z + z^2$, $D_\beta(H,L) = 16s - 416$, which has 2-adic valuation 4. Then, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

Case 4: $f(x) = x^4 + 20sx^2 + 10$, $s \in \{-1, 1\}$

The Gram matrix for this case is

$$G(H,L) = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 1 & -z & z^2 & -z^3 \\ 2 & 0 & -40s - 2z^2 & 0 \\ 0 & 40z + 2sz^3 & 0 & -780z - 40z^3 \end{pmatrix}.$$

The Hermite normal form of $M(H,L)$ is as in the previous cases. On the other hand, for $\beta \in \mathcal{O}_L$, one has

$$D_\beta(H,L) = 16\beta_3(\beta_1 - 10s\beta_3)(s\beta_2^2 + 390s\beta_4^2 - 40\beta_2\beta_4).$$

Choosing $\beta = 1 + z + z^2$, we have

$$D_\beta(H,L) = 16s - 160,$$

which has 2-adic valuation 4 and once again $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

3.4.3 Summary of results

We gather the results obtained in this section. Although we have considered four different cases, we have obtained uniform behaviour for all of them. Concretely:

Theorem 3.27. *Let $L/\mathbb{Q}_2$ be a cyclic quartic extension of 2-adic fields.*

1. *The Hermite normal form of $M(H_c, L)$ is*

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix},$$

and consequently, $\mathfrak{A}_{L/\mathbb{Q}}$ has $\mathbb{Z}_2$-basis

$$\left\{ 1_G, \sigma, \frac{-1_G + \sigma^2}{2}, \frac{-1_G + \sigma - \sigma^2 + \sigma^3}{4} \right\}.$$

2. *The Hermite normal form of $M(H, L)$ is*

$$\begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

so $\mathfrak{A}_H$ has $\mathbb{Z}_2$-basis

$$\left\{ w_1, \frac{-w_1 + w_2}{2}, \frac{-w_1 - w_2 + w_3}{4}, \frac{w_4}{2} \right\}.$$

3. *The element $\beta = 1 + z + z^2$ is a generator of $\mathcal{O}_L$ both as $\mathfrak{A}_{L/\mathbb{Q}}$-module and as $\mathfrak{A}_H$-module.*

3.5 Totally ramified biquadratic extensions of $\mathbb{Q}_2$

Let $L/\mathbb{Q}_2$ be a totally ramified quartic extension of 2-adic fields with elementary abelian Galois group $G \cong C_2 \times C_2$. By [Rio95, Section 2.6], L is the splitting field over $\mathbb{Q}_2$ of one of the polynomials

$$x^4 + 1, \quad x^4 + 25, \quad x^4 + 4x^2 + 9, \quad x^4 - 4x^2 + 9.$$

Even though none of these polynomials is 2-Eisenstein, the powers of a root of each of them generate an integral basis. Indeed, all of them have discriminant with 2-adic valuation 8, and this coincides with the discriminant exponent of L. This is deduced from applying Proposition 1.24 to the chain of ramification groups of $L/\mathbb{Q}_2$, which is

$$C_2 \times C_2 \supset C_2 \times C_2 \supset C_2 \supset C_2 \supset \{1\}.$$

3.5.1 Classical Galois structure

As in the previous sections, we work first with the classical Galois structure H_c. We will determine the Gram matrix with respect to a convenient basis to then carry out a change of basis for each polynomial. We know that $L/\mathbb{Q}_2$ has three intermediate quadratic subfields E_i, $i \in \{1, 2, 3\}$. Let us write $E_i = \mathbb{Q}_2(z_i)$ with $z_i \in E_i$, $z_i \notin \mathbb{Q}_2$ and $z_i^2 \in \mathbb{Q}_2$ for every $i \in \{1, 2, 3\}$. Then L has a $\mathbb{Q}_2$-basis $B_c = \{e_i\}_{i=1}^4$ given by $e_1 = 1$ and $e_i = z_{i-1}$ for $i \in \{2, 3, 4\}$, which of course need not be an integral basis. We may assume that $E_1 = L^{\langle\tau\rangle}$, $E_2 = L^{\langle\sigma\rangle}$ and $E_3 = L^{\langle\sigma\tau\rangle}$. Since $z_1 z_2 \notin E_1, E_2$ and $(z_1 z_2)^2 = z_1^2 z_2^2$, necessarily there exists $r \in \mathbb{Q}_2$ such that $z_3 = r z_1 z_2$, and G acts on z_3 as on the product $z_1 z_2$. Then the Gram matrix with respect to this basis is

$$G(H_c, L_{B_c}) = \begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ e_1 & -e_2 & e_3 & -e_4 \\ e_1 & e_2 & -e_3 & -e_4 \\ e_1 & -e_2 & -e_3 & e_4 \end{pmatrix}.$$

What we do for each case is to change the Gram matrix from B_c to the power integral basis $B = \{1, \alpha, \alpha^2, \alpha^3\}$, where α is a root of the polynomial f that defines the extension.

Case 1: $f(x) = x^4 + 1$

The intermediate fields in this case are given by $E_1 = \mathbb{Q}_2(\sqrt{-1})$, $E_2 = \mathbb{Q}_2(\sqrt{2})$ and $E_3 = \mathbb{Q}_2(\sqrt{-2})$. A root of the polynomial f is $\alpha = \frac{\sqrt{2}+\sqrt{-2}}{2}$, and we have

$$\alpha^2 = \sqrt{-1}, \quad \alpha^3 = \frac{-\sqrt{2}+\sqrt{-2}}{2}.$$

Then, we have

$$P^B_{B_c} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \end{pmatrix}.$$

Now,

$$G(H_c, L_B) = G(H_c, L_{B_c})P^B_{B_c} = \begin{pmatrix} e_1 & \frac{e_3}{2}+\frac{e_4}{2} & e_2 & -\frac{e_3}{2}+\frac{e_4}{2} \\ e_1 & \frac{e_3}{2}-\frac{e_4}{2} & -e_2 & -\frac{e_3}{2}-\frac{e_4}{2} \\ e_1 & -\frac{e_3}{2}-\frac{e_4}{2} & e_2 & \frac{e_3}{2}-\frac{e_4}{2} \\ e_1 & -\frac{e_3}{2}+\frac{e_4}{2} & -e_2 & \frac{e_3}{2}+\frac{e_4}{2} \end{pmatrix}.$$

We pass the coordinates of each entry from B_c to B by applying $P^{B_c}_B$, and we obtain

$$G(H_c, L_B) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & -\alpha^3 & -\alpha^2 & -\alpha \\ 1 & -\alpha & \alpha^2 & -\alpha^3 \\ 1 & \alpha^3 & -\alpha^2 & \alpha \end{pmatrix}.$$

From this we can determine the matrix of the action $M(H_c, L_B)$. Its Hermite normal form is

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

This gives the $\mathbb{Z}_2$-basis of $\mathfrak{A}_{L/\mathbb{Q}_2}$

$$\left\{1_G, \sigma, \frac{-1_G+\sigma^2}{2}, \frac{-1_G+\sigma-\sigma^2+\sigma^3}{4}\right\}.$$

On the other hand, given $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L) = -8\beta_1\beta_3(\beta_2+\beta_4)(\beta_2-\beta_4).$$

In particular, for $\beta = 1+\alpha+\alpha^2$ this is -8, so this β is a normal integral basis generator.

Case 2: $f(x) = x^4 + 25$

In this case, the intermediate fields are $E_1 = \mathbb{Q}_2(\sqrt{-1})$, $E_2 = \mathbb{Q}_2(\sqrt{10})$ and $E_3 = \mathbb{Q}_2(\sqrt{-10})$, and the integral basis is $B = \{1, \alpha, \alpha^2, \alpha^3\}$, where

$$\alpha = \frac{\sqrt{10}+\sqrt{-10}}{2}, \quad \alpha^2 = 5\sqrt{-1}, \quad \alpha^3 = 5\frac{-\sqrt{10}+\sqrt{-10}}{2}.$$

Then, in this case

$$P_{B_c}^{B} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & \frac{1}{2} & 0 & -\frac{5}{2} \\ 0 & \frac{1}{2} & 0 & \frac{5}{2} \end{pmatrix}.$$

Now, the Gram matrix is

$$G(H_c, L_B) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & -\frac{\alpha^3}{5} & -\alpha^2 & -5\alpha \\ 1 & -\alpha & \alpha^2 & -\alpha^3 \\ 1 & \frac{\alpha^3}{5} & -\alpha^2 & 5\alpha \end{pmatrix}.$$

The Hermite normal form of the matrix of the action turns out to be

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix},$$

exactly the same as in the previous case, so we obtain the same basis of $\mathfrak{A}_{L/\mathbb{Q}_2}$. Now, for $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L) = \frac{-8\beta_1\,\beta_3\,(\beta_2 - 5\,\beta_4)\,(\beta_2 + 5\,\beta_4)}{5}.$$

For $\beta = 1 + \alpha + \alpha^2$, this is $-\frac{8}{5}$, proving that β is a normal integral basis generator.

Case 3**:** $f(x) = x^4 + 4x^2 + 9$

The intermediate fields for this case are $E_1 = \mathbb{Q}_2(\sqrt{-5})$, $E_2 = \mathbb{Q}_2(\sqrt{2})$ and $E_3 = \mathbb{Q}_2(\sqrt{-10})$, and we have

$$\alpha = \frac{\sqrt{2} + \sqrt{-10}}{2}, \quad \alpha^2 = -2 + \sqrt{-5}, \quad \alpha^3 = \frac{-7\sqrt{2} - \sqrt{-10}}{2}.$$

The Gram matrix is

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & -\frac{4\alpha+\alpha^3}{3} & -4-\alpha^2 & \frac{7\alpha+4\alpha^3}{3} \\ 1 & -\alpha & \alpha^2 & -\alpha^3 \\ 1 & \frac{4\alpha+\alpha^3}{3} & -4-\alpha^2 & -\frac{7\alpha+4\alpha^3}{3} \end{pmatrix},$$

which leads to the Hermite normal form

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Then, $\mathfrak{A}_{L/\mathbb{Q}_2}$ has basis

$$\left\{1_G, \sigma, \frac{-1_G + \sigma^2}{2}, \frac{-1_G + \sigma - \sigma^2 + \sigma^3}{4}\right\}.$$

Let $\beta \in \mathcal{O}_L$. One computes

$$D_\beta(H_c, L) = -\frac{8}{3}\,\beta_3\,(\beta_2 - \beta_4)\,(\beta_2 - 7\,\beta_4)\,(\beta_1 - 2\,\beta_3)\,.$$

For $\beta = 1 + \alpha + \alpha^2$, we have $D_\beta(H_c, L) = \frac{8}{3}$, and its 2-adic valuation is 3, which coincides with $I(H_c, L) = v_2(\det(D)) = 3$, so this is a normal integral basis generator.

Case 4: $f(x) = x^4 - 4x^2 + 9$

We have the intermediate fields $E_1 = \mathbb{Q}_2(\sqrt{-5})$, $E_2 = \mathbb{Q}_2(\sqrt{-2})$ and $E_3 = \mathbb{Q}_2(\sqrt{10})$. The root of f and its powers are

$$\alpha = \frac{\sqrt{-2}+\sqrt{10}}{2}, \quad \alpha^2 = 2+\sqrt{-5}, \quad \alpha^3 = \frac{7\sqrt{-2}+\sqrt{10}}{2}.$$

We obtain the Gram matrix

$$G(H_c, L) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & -\frac{4\alpha-\alpha^3}{3} & 4-\alpha^2 & -\frac{7\alpha-4\alpha^3}{3} \\ 1 & -\alpha & \alpha^2 & -\alpha^3 \\ 1 & \frac{4\alpha-\alpha^3}{3} & 4-\alpha^2 & \frac{7\alpha-4\alpha^3}{3} \end{pmatrix},$$

whence we compute the Hermite normal form of $M(H_c, L)$:

$$D = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 4 \end{pmatrix},$$

just exactly the same as in the previous case, and then the basis of $\mathfrak{A}_{L/\mathbb{Q}_2}$ is also the same. For $\beta \in \mathcal{O}_L$,

$$D_\beta(H_c, L) = -\frac{8}{3}\beta_3\,(\beta_2 + 7\,\beta_4)\,(\beta_2 + \beta_4)\,(\beta_1 + 2\,\beta_3)\,.$$

Setting $\beta = 1 + \alpha + \alpha^2$, then $D_\beta(H_c, L) = 8$, so this β is a normal integral basis generator.

3.5.2 Non-classical Hopf Galois structures

Let us consider the non-classical Hopf Galois structures $H_i := H_{T_i,1}$ of $L/\mathbb{Q}_2$, $i \in \{1, 2, 3\}$. By Section 3.1.2, a basis of H_i is

$$\{\mathrm{Id}, \mu_i, \eta_{T_i,1} + \mu_i\eta_{T_i,1}, (\eta_{T_i,1} - \mu_i\eta_{T_i,1})z_i\},$$

where $z_i \in E_i$. As in Section 3.3.2, we call these bases $\{u_i\}_{i=1}^4$, $\{v_i\}_{i=1}^4$ and $\{w_i\}_{i=1}^4$, respectively. Since the intermediate fields are fixed, the bases are uniquely determined by the convention that $E_1 = L^{\langle\tau\rangle}$, $E_2 = L^{\langle\sigma\rangle}$ and $E_3 = L^{\langle\sigma\tau\rangle}$.

Case 1: $f(x) = x^4 + 1$

If $f(x) = x^4 + 1$, then $E_1 = \mathbb{Q}_2(\sqrt{-1})$, $E_2 = \mathbb{Q}_2(\sqrt{2})$ and $E_3 = \mathbb{Q}_2(\sqrt{-2})$, so

$$G(H_1, L) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & -\alpha & \alpha^2 & -\alpha^3 \\ 2 & 0 & -2\alpha^2 & 0 \\ 0 & 2\alpha & 0 & -2\alpha^3 \end{pmatrix},$$

$$G(H_2, L) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & -\alpha^3 & -\alpha^2 & -\alpha \\ 2 & -\alpha+\alpha^3 & 0 & \alpha-\alpha^3 \\ 0 & -2\alpha^2 & 2\alpha+2\alpha^3 & -2\alpha^2 \end{pmatrix},$$

$$G(H_3,L)=\begin{pmatrix}1 & \alpha & \alpha^2 & \alpha^3\\ -1 & \alpha^3 & -\alpha^2 & \alpha\\ 2 & -\alpha-\alpha^3 & 0 & -\alpha-\alpha^3\\ 0 & 2\alpha^2 & 2\alpha-2\alpha^3 & -2\alpha^2\end{pmatrix}.$$

The corresponding matrices of the action $M(H_i,L)$ have Hermite normal forms

$$D(H_1,L)=\begin{pmatrix}1 & 1 & 2 & 0\\ 0 & 2 & 2 & 2\\ 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 4\end{pmatrix},\qquad D(H_2,L)=\begin{pmatrix}1 & 0 & -1 & 0\\ 0 & 1 & -1 & 0\\ 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 2\end{pmatrix},$$

$$D(H_3,L)=\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 2\end{pmatrix}.$$

Then, for $i\in\{1,2,3\}$, $\mathfrak{A}_{H_i}$ has $\mathbb{Z}_2$-basis

$$\left\{u_1,\frac{-u_1+u_2}{2},\frac{u_1+u_2+u_3}{4},\frac{-2u_2+u_4}{4}\right\},$$

$$\left\{v_1,v_2,\frac{v_1+v_2+v_3}{4},\frac{v_4}{2}\right\},$$

$$\left\{w_1,w_2,\frac{-w_1-w_2+w_3}{2},\frac{w_4}{2}\right\},$$

respectively. Concerning the freeness, for $\beta\in\mathcal{O}_L$, we have

$$D_\beta(H_1,L)=-32\beta_1\beta_2\beta_3\beta_4,$$

$$D_\beta(H_2,L)=8\beta_1(\beta_2-\beta_4)(\beta_2^2+2\beta_2\beta_4+2\beta_3^2+\beta_4^2),$$

$$D_\beta(H_3,L)=-4\beta_1(\beta_2+\beta_4)(\beta_2^2-2\beta_2\beta_4-2\beta_3^2+\beta_4^2).$$

The powers of α form an integral basis of eigenvectors for H_1. Then, $\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free with generator $\beta=1+\alpha+\alpha^2+\alpha^3$. For $i\in\{2,3\}$, $\mathcal{O}_L$ is also $\mathfrak{A}_{H_i}$-free with generator $\beta=1+\alpha+\alpha^2$.

Case 2: $f(x)=x^4+25$

In this case, the Gram matrices are

$$G(H_1,L)=\begin{pmatrix}1 & \alpha & \alpha^2 & \alpha^3\\ 1 & -\alpha & \alpha^2 & -\alpha^3\\ 2 & 0 & -2\alpha^2 & 0\\ 0 & 2\alpha & 0 & -2\alpha^3\end{pmatrix},$$

$$G(H_2,L)=\begin{pmatrix}1 & \alpha & \alpha^2 & \alpha^3\\ 1 & -\frac{\alpha^3}{5} & -\alpha^2 & -5\alpha\\ 2 & -\alpha+\frac{\alpha^3}{5} & 0 & 5\alpha-\alpha^3\\ 0 & -2\alpha^2 & 10\alpha+2\alpha^3 & -10\alpha^2\end{pmatrix},$$

$$G(H_3,L)=\begin{pmatrix}1 & \alpha & \alpha^2 & \alpha^3\\ 1 & \frac{\alpha^3}{5} & -\alpha^2 & 5\alpha\\ 2 & -\alpha-\frac{\alpha^3}{5} & 0 & -5\alpha-\alpha^3\\ 0 & 2\alpha^2 & 10\alpha^2 & -10\alpha^2\end{pmatrix}.$$

The Hermite normal form of the matrix of the action at each Hopf Galois structure is

$$D(H_1,L)=\begin{pmatrix}1&1&2&0\\0&2&2&2\\0&0&4&0\\0&0&0&4\end{pmatrix},\qquad D(H_2,L)=\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&2\end{pmatrix},$$

$$D(H_3,L)=\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&2\end{pmatrix}.$$

Then the associated orders have $\mathbb{Z}_2$-bases

$$\Big\{u_1,\frac{-u_1+u_2}{2},\frac{u_1+u_2+u_3}{4},\frac{-2u_2+u_4}{4}\Big\},$$

$$\Big\{v_1,v_2,\frac{v_1+v_2+v_3}{4},\frac{v_4}{2}\Big\},$$

$$\Big\{w_1,w_2,\frac{w_1+w_2+w_3}{4},\frac{w_4}{2}\Big\}.$$

Concerning the freeness, given $\beta\in\mathcal{O}_L$,

$$D_\beta(H_1,L)=-32\beta_1\beta_2\beta_3\beta_4,$$

$$D_\beta(H_2,L)=-\frac{8}{5}\beta_1\,(\beta_2-5\,\beta_4)\left({\beta_2}^2+10\,\beta_2\,\beta_4+10\,{\beta_3}^2+25\,{\beta_4}^2\right),$$

$$D_\beta(H_3,L)=-\frac{8}{5}\beta_1\,(\beta_2-5\,\beta_4)\,(\beta_2+5\,\beta_4)\,(\beta_2+5\,\beta_3-5\,\beta_4)\,.$$

Again, the powers of α are eigenvectors of the action of H_1, so $\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free with generator $\beta=1+\alpha+\alpha^2+\alpha^3$. As for the other two, one checks easily that $\mathcal{O}_L$ is $\mathfrak{A}_{H_2}$-free with generator $\beta=1+\alpha+\alpha^2$ and $\mathfrak{A}_{H_3}$-free with generator $\beta=1+\alpha$.

Case 3: $f(x)=x^4+4x^2+9$

The Gram matrices for the non-classical Hopf Galois structures are

$$G(H_1,L)=\begin{pmatrix}1&\alpha&\alpha^2&\alpha^3\\1&-\alpha&\alpha^2&-\alpha^3\\2&0&-8-2\alpha^2&0\\0&\frac{2\alpha-4\alpha^3}{3}&0&\frac{-44\alpha-2\alpha^3}{3}\end{pmatrix},$$

$$G(H_2,L)=\begin{pmatrix}1&\alpha&\alpha^2&\alpha^3\\1&-\frac{4\alpha+\alpha^3}{7}&-4-\alpha^2&\frac{7\alpha+4\alpha^3}{3}\\2&\frac{\alpha+\alpha^3}{3}&-4&\frac{-7\alpha-7\alpha^3}{3}\\0&-4-2\alpha^2&\frac{14\alpha+2\alpha^3}{3}&4+2\alpha^2\end{pmatrix},$$

$$G(H_3,L)=\begin{pmatrix}1&\alpha&\alpha^2&\alpha^3\\1&\frac{4\alpha+\alpha^3}{3}&-4-\alpha^2&\frac{-7\alpha-4\alpha^3}{3}\\2&\frac{-7\alpha-\alpha^3}{3}&-4&\frac{7\alpha+\alpha^3}{3}\\0&4+2\alpha^2&\frac{-10\alpha-10\alpha^3}{3}&-56-28\alpha^2\end{pmatrix}.$$

The Hermite normal forms for this case are once again

$$D(H_1,L)=\begin{pmatrix}1&1&2&0\\0&2&2&2\\0&0&4&0\\0&0&0&4\end{pmatrix},\qquad D(H_2,L)=\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&2\end{pmatrix},$$

$$D(H_3,L)=\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&2\end{pmatrix},$$

just as in the previous case, so the bases are the same. Now, for $\beta\in\mathcal{O}_L$, one computes

$$\begin{aligned}D_\beta(H_1,L)&=-\frac{32\,\beta_3\left({\beta_2}^2+\beta_2\,\beta_4-11\,{\beta_4}^2\right)(\beta_1-2\,\beta_3)}{3},\\ D_\beta(H_2,L)&=-\frac{8}{3}\,(\beta_2-7\,\beta_4)\left({\beta_2}^2-2\,\beta_2\,\beta_4+2\,{\beta_3}^2+{\beta_4}^2\right)(\beta_1-2\,\beta_3)\,,\\ D_\beta(H_3,L)&=-\frac{8}{3}\,(\beta_2-\beta_4)\left({\beta_2}^2-21\,\beta_2\,\beta_4-10\,{\beta_3}^2+98\,{\beta_4}^2\right)(\beta_1-2\,\beta_3)\,.\end{aligned}$$

In this case, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free for $i\in\{1,2,3\}$, and the element $\beta=1+\alpha+\alpha^2$ is always a generator.

Case 4: $f(x)=x^4-4x^2+9$

The Gram matrices are

$$G(H_1,L)=\begin{pmatrix}1&\alpha&\alpha^2&\alpha^3\\1&-\alpha&\alpha^2&-\alpha^3\\2&0&8-2\alpha^2&0\\0&\frac{-2\alpha-4\alpha^3}{3}&0&\frac{-44\alpha+2\alpha^3}{3}\end{pmatrix},$$

$$G(H_2,L)=\begin{pmatrix}1&\alpha&\alpha^2&\alpha^3\\1&\frac{-4\alpha+\alpha^3}{3}&4-\alpha^2&\frac{-7\alpha+4\alpha^3}{3}\\2&\frac{\alpha-\alpha^3}{3}&4&\frac{7\alpha-7\alpha^3}{3}\\0&\frac{5-5\alpha^2}{3}&\frac{-14\alpha+2\alpha^3}{3}&\frac{5-5\alpha^2}{3}\end{pmatrix},$$

$$G(H_3,L)=\begin{pmatrix}1&\alpha&\alpha^2&\alpha^3\\1&\frac{4\alpha-\alpha^3}{3}&4-\alpha^2&\frac{7\alpha-4\alpha^3}{3}\\2&\frac{-7\alpha+\alpha^3}{3}&4&\frac{-7\alpha+\alpha^3}{3}\\0&-4+2\alpha^2&\frac{10\alpha-10\alpha^3}{3}&-28+14\alpha^2\end{pmatrix}.$$

The corresponding matrices of the actions have Hermite normal forms

$$D(H_1,L)=\begin{pmatrix}1&1&2&0\\0&2&2&2\\0&0&4&0\\0&0&0&4\end{pmatrix},\qquad D(H_2,L)=\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&2\end{pmatrix},$$

$$D(H_3,L)=\begin{pmatrix}1&0&-1&0\\0&1&-1&0\\0&0&4&0\\0&0&0&2\end{pmatrix},$$

as in the previous two cases, so we obtain the same bases.

Let us study the freeness. Given $\beta \in \mathcal{O}_L$, we have

$$D_\beta(H_1, L) = -\frac{32\,\beta_3\left(\beta_2{}^2 - \beta_2\,\beta_4 - 11\,\beta_4{}^2\right)(\beta_1 + 2\,\beta_3)}{3},$$

$$D_\beta(H_2, L) = \frac{8\,(\beta_2 + 7\,\beta_4)\,(\beta_2 + \beta_4)\,(3\,\beta_2 - \beta_3 + 3\,\beta_4)\,(\beta_1 + 2\,\beta_3)}{9},$$

$$D_\beta(H_3, L) = \frac{8}{3}\,(\beta_2 + \beta_4)\left(\beta_2{}^2 + 14\,\beta_2\,\beta_4 + 10\,\beta_3{}^2 + 49\,\beta_4{}^2\right)(\beta_1 + 2\,\beta_3)\,.$$

For the last two cases, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free with generator $\beta = 1 + \alpha$. As for the first one, $\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free with generator $\beta = 1 + \alpha + \alpha^3$.

3.5.3 Summary of results

Looking back at the results obtained, we see that we have obtained the same behaviour in the classical Galois structure, regardless of the defining polynomial. It is in the non-classical Hopf Galois structures where the behaviour may differ.

Theorem 3.28. *Let $L/\mathbb{Q}_2$ be a biquadratic extension of 2-adic fields.*

1. *In the classical Galois structure, the associated order $\mathfrak{A}_{L/\mathbb{Q}_2}$ has $\mathbb{Z}_2$-basis*

$$\left\{1_G, \sigma, \frac{-1_G + \sigma^2}{2}, \frac{-1_G + \sigma - \sigma^2 + \sigma^3}{4}\right\}.$$

Moreover, $\beta = 1 + \alpha + \alpha^2$ is always a generator of $\mathcal{O}_L$ as $\mathfrak{A}_{L/\mathbb{Q}_2}$-module.

2. *At case 1, the associated orders $\mathfrak{A}_{H_1}$, $\mathfrak{A}_{H_2}$ and $\mathfrak{A}_{H_3}$ have $\mathbb{Z}_2$-bases*

$$\left\{u_1, \frac{-u_1 + u_2}{2}, \frac{u_1 + u_2 + u_3}{4}, \frac{-2u_2 + u_4}{4}\right\},$$
$$\left\{v_1, v_2, \frac{v_1 + v_2 + v_3}{4}, \frac{v_4}{2}\right\},$$
$$\left\{w_1, w_2, \frac{-w_1 - w_2 + w_3}{2}, \frac{w_4}{2}\right\},$$

respectively. In the other three cases, those bases are

$$\left\{u_1, \frac{-u_1 + u_2}{2}, \frac{u_1 + u_2 + u_3}{4}, \frac{-2u_2 + u_4}{4}\right\},$$
$$\left\{v_1, v_2, \frac{v_1 + v_2 + v_3}{4}, \frac{v_4}{2}\right\},$$
$$\left\{w_1, w_2, \frac{w_1 + w_2 + w_3}{4}, \frac{w_4}{2}\right\}.$$

3. *At each case, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free for all $i \in \{1, 2, 3\}$ and a generator is indicated in the table below.*

Case	H_1	H_2	H_3
1	$1 + \alpha + \alpha^2 + \alpha^3$	$1 + \alpha + \alpha^2$	$1 + \alpha + \alpha^2$
2	$1 + \alpha + \alpha^2 + \alpha^3$	$1 + \alpha + \alpha^2$	$1 + \alpha$
3,4	$1 + \alpha + \alpha^2$	$1 + \alpha + \alpha^2$	$1 + \alpha + \alpha^2$

Chapter 4

Separable degree p extensions with dihedral Galois closure

We have seen that we can apply the reduction method to low degree Galois extensions with success in most of the cases. Moreover, in Chapter 2 we worked with the main example of [GP87], which is an extension that is not Galois. This is an example of the simplest case of Hopf Galois extensions that are not Galois; namely, for an odd prime number p, a separable non-normal degree p extension E/K whose Galois closure L has Galois group over K isomorphic to the dihedral group D_p.

By Proposition 1.12, such an extension E/K is indeed Hopf Galois, and by the generalized Byott Uniqueness Theorem 1.17, it has a unique Hopf Galois structure H_1, which is almost classically Galois. In this chapter we study these extensions, and when they are Hermite, we consider the problem of determining the Hopf Galois module structure of $\mathcal{O}_E$. Concerning the example in [GP87], we could even determine a normal integral basis because the action of the Hopf Galois structure is given explicitly, and the Hopf algebra was described using descent theory. In general a description like that one is not available. In the first section we give a basis of the Hopf Galois structure using a different approach, the one given by Greither-Pareigis theory.

It is in the second section when we assume that the extension is Hermite, and we discuss all requirements we need so as to apply the reduction method. In the third section we determine the entries of the Gram matrix $G(H_1, E)$, and since it is a $p \times p$ matrix, we carry out the reduction with concrete cases: $K = \mathbb{Q}_3$ and $K = \mathbb{Q}_5$. We will find a basis of the associated order $\mathfrak{A}_{H_1}$ at each case and prove that $\mathcal{O}_E$ is always $\mathfrak{A}_{H_1}$-free.

4.1 The unique Hopf Galois structure

Let E/K be an extension of arbitrary fields of degree p which is non-normal and whose Galois closure L has Galois group over K isomorphic to D_p. We use Greither-Pareigis theory so as to describe the unique Hopf Galois structure of E/K.

Let us analyze the unique Hopf Galois structure of E/K. Let $G = \mathrm{Gal}(L/K)$ and $G' = \mathrm{Gal}(L/E)$. Since G is the dihedral group of $2p$ elements, it has p order 2 subgroups and a unique order p one. By the fundamental theorem of Galois theory, this gives the lattice of subextensions of L/K: it has p different degree p subextensions, among which it is E/K, and a unique quadratic subextension that we call F/K.

We establish a presentation of G

$$G = \langle \sigma, \tau \,|\, \sigma^p = \tau^2 = 1,\ \tau\sigma = \sigma^{p-1}\tau \rangle.$$

The unique order p subgroup of G is $J = \langle \sigma \rangle$, while the p order 2 subgroups are

$$\langle \sigma^d \tau \rangle,\ 0 \leq d \leq p-1.$$

Let us choose such a d so that $G' = \langle \sigma^d \tau \rangle$. Then,

$$G/G' = \{\overline{1_G}, \overline{\sigma}, \dots, \overline{\sigma^{p-1}}\},$$

where $\overline{\sigma^i} = \{\sigma^i, \sigma^{d-i}\tau\}$ for every $0 \leq i \leq p-1$.

As already mentioned, E/K has a unique Hopf Galois structure. Let $\overline{\lambda}\colon G \longrightarrow \mathrm{Perm}(G/G')$ be the left translation map. By Greither-Pareigis theorem, there is a unique regular subgroup N_1 of $\mathrm{Perm}(G/G')$ which is normalized by $\overline{\lambda}(G)$. One can easily check that $N_1 = \overline{\lambda}(J)$ satisfies the required properties. Let us call $\overline{\mu} = \overline{\lambda}(\sigma)$, which can be expressed as the permutation $(\overline{1_G}, \overline{\sigma}, \dots, \overline{\sigma^{p-1}})$ of the quotient set G/G'. This element is the generator of N_1, that is,

$$N_1 = \langle \overline{\mu} \rangle = \{\overline{\mathrm{Id}}, \overline{\mu}, \dots \overline{\mu}^{p-1}\}.$$

Next, we determine the Hopf algebra $H_1 = L[N_1]^G$ of this Hopf Galois structure.

Theorem 4.1. *The Hopf algebra of the unique Hopf Galois structure of E/K has a K-basis formed by the p elements*

$$w_1 = \mathrm{Id}, \quad w_{1+i} = z(\overline{\mu}^i - \overline{\mu}^{-i}), \quad w_{\frac{p-1}{2}+i} = \overline{\mu}^i + \overline{\mu}^{-i},$$

where $1 \leq i \leq \frac{p-1}{2}$ and:

- *$\overline{\mu} = \overline{\lambda}(\sigma) \in \mathrm{Perm}(G/G')$ is the image of σ by the left translation map $\overline{\lambda} := G \longrightarrow \mathrm{Perm}(G/G')$ of G into $\mathrm{Perm}(G/G')$*
- *$z = \sqrt{d}$ is any element such that $d \in K$ and $d \notin K^2$, so that $F = K(z)$.*

Proof. Let $x \in H_1$. Since $H_1 \subset L[N_1]$, there are elements $a_i \in L$ with $0 \leq i \leq p-1$ such that

$$x = \sum_{i=0}^{p-1} a_i \overline{\mu}^i.$$

The action of G on N_1 is given by

$$\sigma(\overline{\mu}) = \overline{\mu}, \quad \tau(\overline{\mu}) = \overline{\mu}^{-1}.$$

Now, since $x \in H$, it is fixed by the action of G on H_1. Then,

$$\begin{aligned} x = \sigma(x) &= \sum_{i=0}^{p-1} \sigma(a_i)\overline{\mu}^i, \\ x = \tau(x) &= \sum_{i=0}^{p-1} \tau(a_i)\overline{\mu}^{-i} \\ &= \sum_{i=0}^{p-1} \tau(a_{p-i})\overline{\mu}^i, \end{aligned}$$

where in the last line we consider the subscripts mod p. The first equality gives that $\sigma(a_i) = a_i$ for all $0 \leq i \leq p-1$, so $a_i \in L^{\langle\sigma\rangle} = F$. On the other hand, the second one yields $\tau(a_i) = a_{p-i}$ for every i. Since subscripts are mod p, $\tau(a_0) = a_0$, giving that $a_0 \in K$.

Now, $a_i \in F$ for $1 \leq i \leq p$, so there are $a_i^{(1)}, a_i^{(2)} \in K$ such that $a_i = a_i^{(1)} + a_i^{(2)}z$. For those values of i, $\tau(a_i) = a_i^{(1)} - a_i^{(2)}z$, but also $\tau(a_i) = a_{p-i}$, so $a_{p-i} = a_i^{(1)} - a_i^{(2)}z$. Then,

$$\begin{aligned} x &= a_0\mathrm{Id} + \sum_{i=0}^{\frac{p-1}{2}} (a_i^{(1)} + a_i^{(2)}z)\overline{\mu}^i + \sum_{i=0}^{\frac{p-1}{2}} (a_i^{(1)} - a_i^{(2)}z)\overline{\mu}^i\eta \\ &= a_0\mathrm{Id} + \sum_{i=0}^{\frac{p-1}{2}} a_i^{(1)}(\overline{\mu}^i + \overline{\mu}^{-i}) + \sum_{i=0}^{\frac{p-1}{2}} a_i^{(2)}z(\overline{\mu}^i - \overline{\mu}^{-i}). \end{aligned} \tag{4.1}$$

This proves that x belongs to the space generated by a K-basis as in the statement, so such a space contains H_1. But both of them have dimension p, so they coincide. □

It is not difficult prove a more general result for separable degree p^n extensions (see Appendix A).

Remark 4.2. *Let $\lambda\colon G \longrightarrow \mathrm{Perm}(G)$ be the left regular representation of G. Since the powers of $\mu = \lambda(\sigma)$ factorize through G' as permutations of G, the groups $\overline{\lambda}(J)$ and $\lambda(J)$ can be identified by establishing $\overline{\lambda}(\sigma^i) = \lambda(\sigma^i)$, and in particular, $\overline{\mu} = \mu$. Hence, from now on, we will take the elements of the basis of H_1 in the statement above with the powers of μ instead of $\overline{\mu}$.*

Remark 4.3. *The elements w_k for k even (resp. odd) can be described as linear combination of even (resp. odd) powers of $w_2 = z(\mu - \mu^{-1})$, so they generate H_1 as K-algebra. That is,*

$$H_1 = K[z(\mu - \mu^{-1})].$$

4.2 The integral setting

Now, let us assume that E/K is Hermite and $\mathrm{char}(K) \neq 2$. Hence, the extension has an integral setting and we want to determine a basis of $\mathfrak{A}_{H_1}$ and the structure of $\mathcal{O}_E$ as $\mathfrak{A}_{H_1}$-module, where H_1 is the unique Hopf Galois structure of E/K.

We know a basis of H_1 from Theorem 4.1. We first show that this is also an $\mathcal{O}_K$-basis of $\mathcal{O}_L[N]^G$, the naive $\mathcal{O}_K$-order in H.

Corollary 4.4. *If $v_K(z^2) \leq 1$ and $\mathcal{O}_F = \mathcal{O}_K[z]$, then the elements $\{w_i\}_{i=1}^p$ of Theorem 4.1 form an $\mathcal{O}_K$-basis of the $\mathcal{O}_K$-order $\mathcal{O}_L[N]^G$ in H.*

Proof. We follow the same steps as in the proof of Theorem 4.1 with an element $x \in \mathcal{O}_L[N]^G$, so in this case

$$x = \sum_{i=0}^{p-1} a_i\mu^i$$

with $a_i \in \mathcal{O}_L$. We have that $a_0 \in K \cap \mathcal{O}_L = \mathcal{O}_K$ and $a_i \in \mathcal{O}_L \cap F = \mathcal{O}_F$. But $\mathcal{O}_F = \mathcal{O}_K[z]$, so we may obtain a description as in (4.1) with the coefficients in $\mathcal{O}_K$. □

Using the basis in Theorem 4.1, we will apply the reduction method so as to determine a basis of $\mathfrak{A}_{H_1}$. To this end, we need to know an integral basis on $\mathcal{O}_E$ and how H_1 acts on this basis.

We discuss the problem of determining an integral basis. It depends strongly on the nature of the fields, and so nothing can be said in general. Throughout this chapter, we will work with the hypothesis that E/K has a power integral basis. There are some sufficient conditions for this to happen. We are interested in extensions of p-adic or number fields. If E/K is an extension of p-adic fields, it is enough that the irreducible polynomial of a primitive element α over K is π_K-Eisenstein. If we choose the base field to be $\mathbb{Q}_p$, then it is always possible to ensure that condition (see [AE12, Theorem 5.2]):

Theorem 4.5 (Amano polynomials)**.** *Let $E/\mathbb{Q}_p$ be a degree p extension of local fields whose Galois closure $L/\mathbb{Q}_p$ is dihedral of degree $2p$. Then, E is generated by some root of one of the polynomials:*

1. *If $p = 3$,*
$$x^3+3, \quad x^3+12, \quad x^3+21,$$
$$x^3+3x+3, \quad x^3+6x+3, \quad x^3+3x^2+3.$$
2. *If $p > 3$,*
$$x^p+2px^{\frac{p-1}{2}}+p, \quad x^p+p(p-2)x^{\frac{p-1}{2}}+p, \quad x^p+px^{p-1}+p.$$

For $p \geq 3$, the inertia subgroup of the Galois group of $L/\mathbb{Q}_p$ is D_p for all polynomials except $x^p+px^{p-1}+p$, in which case the inertia subgroup is C_p.

The polynomials of the previous result will be referred to as the Amano polynomials henceforth. All of them are p-Eisenstein, so in those cases by Theorem 1.20 we have that the powers of a root α is an integral basis of E. In practice, we will sometimes need to replace f by other polynomial generating the same extension, just as in Section 2.7.2.

As for extensions of number fields, it is known that extensions of quadratic or cyclotomic fields have a power integral basis, but beyond that, the available criteria are much more specific. In Section 4.6, we examine the case in which $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{m})$ for $m \in \mathbb{Z}$ cubic-free.

4.3 The Gram matrix of E/K

To apply the reduction method, the unique ingredient left is the Gram matrix $G(H_1, E)$ where in H_1 we fix the basis of Theorem 4.1 and in E we choose an integral basis. Actually, we will fix a power basis generated by an element $\alpha \in \mathcal{O}_E$. This is enough when the basis is integral. The action of H_1 on E when taking these bases can be expressed in general by means of Lucas sequences.

Let f be the irreducible polynomial of α. We use the same idea of Section 2.7.2: we write
$$f(x) = (x-\alpha)f_1(x),$$

where in this case $f_1 \in E[x]$ is a polynomial of degree $p-1$. Now we use the hypothesis that the Galois closure of E/K has Galois group D_p over K to group the roots of f_1 in a convenient way. Indeed, the hypothesis implies that the Galois closure of E/K is quadratic over E, so

$$f_1(x) = \prod_{i=1}^{\frac{p-1}{2}} P_i(x),$$

with $P_i \in E[x]$ quadratic polynomials. Let us write

$$P_i(x) = x^2 - A_i x + B_i,\ A_i, B_i \in E,$$

for every $1 \leq i \leq \frac{p-1}{2}$. Let us call $d_i = A_i^2 - 4B_i \in E$ the discriminant of P_i. Then, the roots of P_i are

$$\alpha_{2,i} = \frac{A_i + \sqrt{d_i}}{2}, \qquad \alpha_{3,i} = \frac{A_i - \sqrt{d_i}}{2}.$$

We can assume without loss of generality that $\sigma^{-i}(\alpha) = \alpha_{2,i}$ for every $1 \leq i \leq \frac{p-1}{2}$ (otherwise we would reorder the polynomials P_i). Then,

$$\alpha_{3,i} = \tau(\alpha_{2,i}) = \tau\sigma^{-i}(\alpha) = \sigma^i\tau(\alpha) = \sigma^i(\alpha).$$

In other words, the roots of P_i are $\sigma^{-i}(\alpha)$ and $\sigma^i(\alpha)$. Looking at the form of the elements of the basis of H_1, we have to deal with sums and differences of each pair of roots of P_i. The suitable tool to deal with such objects are Lucas sequences.

Definition 4.6. *Let K be a field and let $A, B \in K$. The* ***Lucas sequences of first kind*** *$U_j(A,B)$ and* ***of second kind*** *$V_j(A,B)$ for the parameters A, B are defined by the expressions*

$$\begin{aligned}
&U_0(A,B) = 0,\\
&U_1(A,B) = 1,\\
&U_j(A,B) = AU_{j-1}(A,B) - BU_{j-2}(A,B),\ j \geq 2,
\end{aligned}$$

$$\begin{aligned}
&V_0(A,B) = 2,\\
&V_1(A,B) = A,\\
&V_j(A,B) = AV_{j-1}(A,B) - BV_{j-2}(A,B),\ j \geq 2.
\end{aligned}$$

The characteristic polynomial of $U_j(A,B)$ and $V_j(A,B)$ is defined as $P(x) = x^2 - Ax + B$. The relation of the sequences with the roots of the polynomial is given by the following result, whose proof is straightforward by induction on j.

Proposition 4.7. *Assume that the discriminant $d = A^2 - 4B$ of P is non-zero and let $\alpha_2 = \frac{A+\sqrt{d}}{2}$ and $\alpha_3 = \frac{A-\sqrt{d}}{2}$ be its roots. Then,*

$$U_j(A,B) = \frac{\alpha_2^j - \alpha_3^j}{\sqrt{d}},$$

$$V_j(A,B) = \alpha_2^j + \alpha_3^j.$$

We compute the action of H_1 over E as follows:

Theorem 4.8. *Let us consider the basis $W = \{w_i\}_{i=1}^{p}$ of H_1 as before and the integral basis $B = \{\alpha^i\}_{i=0}^{p-1}$ of E. Call d_i the discriminant of P_i. Then, for every $1 \leq i \leq \frac{p-1}{2}$ and every $0 \leq j \leq p-1$,*

$$w_1 \cdot \alpha^j = \alpha^j, \qquad w_{1+i} \cdot \alpha^j = U_j(A_i, B_i)\sqrt{d_i}z, \qquad w_{\frac{p+1}{2}+i} \cdot \alpha^j = V_j(A_i, B_i).$$

Proof. The first equality is trivial since $w_1 = \text{Id}$. Let $1 \leq i \leq \frac{p-1}{2}$ and $0 \leq j \leq p-1$. Then,

$$\begin{aligned} w_{1+i} \cdot \alpha^j &= (z(\mu^i - \mu^{-i})) \cdot \alpha^j = (\sigma^{-i}(\alpha^j) - \sigma^i(\alpha^j))z \\ &= (\alpha_{2,i}^j - \alpha_{3,i}^j)z = U_j(A_i, B_i)\sqrt{d_i}z \\ w_{\frac{p+1}{2}+i} \cdot \alpha^j &= (\mu^i + \mu^{-i}) \cdot \alpha^j = \sigma^{-i}(\alpha^j) + \sigma^i(\alpha^j) \\ &= \alpha_{2,i}^j + \alpha_{3,i}^j = V_j(A_i, B_i) \end{aligned}$$

□

Remark 4.9. This result shows the reason why we have chosen $\alpha_{2,i} = \sigma^{-i}(\alpha)$. Otherwise, since μ acts on elements of L as σ^{-1}, we would have $w_{1+i} \cdot \alpha^j = -U_j(A_i, B_i)\sqrt{d_i}z$. Another option is to identify G and $\lambda(G)$ by identifying σ with $\mu = \lambda(\sigma)$, which in terms of actions means to replace μ by $-\mu$.

Corollary 4.10. *Let us call $U_i(P_i) = U_i(A_i, B_i)$ and $V_i(P_i) = V_i(A_i, B_i)$ for every $1 \leq i \leq \frac{p-1}{2}$. The Gram matrix of H_1 is*

$$G(H_1, E) = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{p-1} \\ U_0(P_1)\sqrt{d_1}z & U_1(P_1)\sqrt{d_1}z & \cdots & U_{p-1}(P_1)\sqrt{d_1}z \\ U_0(P_2)\sqrt{d_2}z & U_1(P_2)\sqrt{d_2}z & \cdots & U_{p-1}(P_2)\sqrt{d_2}z \\ \vdots & \vdots & \ddots & \vdots \\ U_0(P_{\frac{p-1}{2}})\sqrt{d_{\frac{p-1}{2}}}z & U_1(P_{\frac{p-1}{2}})\sqrt{d_{\frac{p-1}{2}}}z & \cdots & U_{p-1}(P_{\frac{p-1}{2}})\sqrt{d_{\frac{p-1}{2}}}z \\ V_0(P_1) & V_1(P_1) & \cdots & V_{p-1}(P_1) \\ V_0(P_2) & V_1(P_2) & \cdots & V_{p-1}(P_2) \\ \vdots & \vdots & \ddots & \vdots \\ V_0(P_{\frac{p-1}{2}}) & V_1(P_{\frac{p-1}{2}}) & \cdots & V_{p-1}(P_{\frac{p-1}{2}}) \end{pmatrix}$$

Note that Corollary 4.10 implies that $\sqrt{d_i}z \in E$ for every $1 \leq i \leq \frac{p-1}{2}$. That is, $\sqrt{d_i}$ is the product of an element of E and z. But recall that z can be any element such that $z^2 \in \mathcal{O}_K$ and $z \in \mathcal{O}_L - \mathcal{O}_K$. In practice, what we will usually do is to choose z after computing $\sqrt{d_1}$, so that the expression of $\sqrt{d_1}z$ is convenient enough.

All the previous considerations lead to the following method to compute $G(H_1, E)$:

1. We factorize the polynomials f in terms of a root α to compute the polynomials $P_i \in E[x]$, $1 \leq i \leq \frac{p-1}{2}$.

2. For every $1 \leq i \leq \frac{p-1}{2}$, we compute the square root of $d_i = \sqrt{A_i^2 - 4B_i}$.

3. We determine the entries of $G(H_1, E)$ following Corollary 4.10.

Once we have computed $G(H_1, E)$, if the power basis is integral, we can determine $M(H_1, E)$ from its entries and use the reduction method to obtain a basis of $\mathfrak{A}_H$ and determine the freeness of $\mathcal{O}_E$ as $\mathfrak{A}_H$-module.

Thus, if we know explicitly an Eisenstein polynomial f of a generating root of E, this would lead to a description of the Hopf Galois module structure of $\mathcal{O}_E$. This is possible when $K = \mathbb{Q}_p$ thanks to Theorem 4.5. Unfortunately, the general expression of the terms of the Lucas sequences $U_k(A, B)$ and $V_k(A, B)$ with respect to A and B is very complicated as k increases. We also need to compute the square root of the discriminants d_i of the quadratic polynomials P_i, something difficult to find explicitly unless the degree is very low. For those reasons, when $K = \mathbb{Q}_p$, we have been able to carry out all the explicit computations only for $p = 3$ and $p = 5$.

4.4 The case $K = \mathbb{Q}_3$

Let $E/\mathbb{Q}_3$ be a separable degree 3 extension with Galois closure D_3. Then, $E = \mathbb{Q}_3(\alpha)$ with α a root of one of the polynomials

$$x^3 + 3, \quad x^3 + 12, \quad x^3 + 21, \quad x^3 + 3x + 3, \quad x^3 + 6x + 3, \quad x^3 + 3x^2 + 3.$$

These polynomials correspond to [LMFDB, p-adic field 3.3.5.1, p-adic field 3.3.5.3, p-adic field 3.3.5.2, p-adic field 3.3.3.2, p-adic field 3.3.3.1, p-adic field 3.3.3.4], respectively. We divide them in three groups. The first three are of the form $x^3 + 3a$ with $a \in \{1, 4, 7\}$, and these are the radical cases. The next two polynomials may be expressed by $x^3 + 3ax + 3$ with $a \in \{1, 2\}$, while the sixth polynomial is the unique one for which $L/\mathbb{Q}_p$ is not totally ramified. From now on, these will be called the first and second group and the singular case, respectively.

4.4.1 The action on the 3-part

The extension $E/\mathbb{Q}_3$ has a unique Hopf Galois structure H_1 with $\mathbb{Q}_3$-basis

$$w_1 = \mathrm{Id}, \quad w_2 = z(\mu - \mu^{-1}), \quad w_3 = \mu + \mu^{-1}$$

where $\mu = \lambda(\sigma)$ and z is any quadratic element in L. Let f denote one of the previous polynomials. We know that

$$f(x) = (x - \alpha)P(x),$$

where $P(x) = x^2 - Ax + B$ and $A, B \in E$. Let d be the discriminant of f. According to Corollary 4.10,

$$G(H_1, E) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 0 & \sqrt{d}z & A\sqrt{d}z \\ 2 & A & A^2 - 2B \end{pmatrix}.$$

Since the first terms of Lucas sequences are well known, the matter is to determine $\sqrt{d}z$.

Let f be a polynomial of the first group. Using Ruffini algorithm one checks easily that

$$f(x) = (x - \alpha)(x^2 + \alpha x + \alpha^2),$$

that is, $A = -\alpha$ and $B = \alpha^2$. Then, the discriminant of the quadratic polynomial is

$$d = A^2 - 4B = \alpha^2 - 4\alpha^2 = -3\alpha^2.$$

Let us take $z = \sqrt{-3}$. Then, $\sqrt{d} = \alpha z$. Thus, one obtains

$$G(H_1, E) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 0 & -3\alpha & 3\alpha^2 \\ 2 & -\alpha & -\alpha^2 \end{pmatrix}.$$

We move to the second group. Fix a root α of f. Now

$$f(x) = (x-\alpha)(x^2 + \alpha x + \alpha^2 + 3a),$$

that is, $A = -\alpha$ and $B = \alpha^2 + 3a$. Then,

$$d = \alpha^2 - 4(\alpha^2 + 3a) = -3\alpha^2 - 12a = -3(\alpha^2 + 4a).$$

To compute its square root, we distinguish cases again.

If $a = 1$, we need to compute the square root of $-3\alpha^2 - 12$ in L. To do this, we solve a system of equations. Let $\alpha^2 + l\alpha + m \in E$ and $r \in \mathbb{Q}_p$ such that

$$-3\alpha^2 - 12 - r(\alpha^2 + l\alpha + m)^2 = 0.$$

Expanding the expression and associating by powers of α,

$$\left(-3 + \left(-l^2 - 2\,m\right) r\right) \alpha^2 + \left(-2\,lm + 3\,\right) r\alpha - 12 + \left(6\,l - m^2\right) r = 0.$$

The system of equations

$$\begin{cases} -3 + \left(-l^2 - 2\,m + 3\right) r = 0 \\ -2\,r\left(-\frac{3}{2} + (m-3)\,l\right) = 0 \\ -12 + \left(-m^2 + 6\,l\right) r = 0 \end{cases}$$

has as unique solution over $\mathbb{Q}_3$

$$\left\{ l = -\frac{3}{2}, m = 2, r = -\frac{12}{13} \right\},$$

meaning that

$$-3\alpha^2 - 12 = -\frac{12}{13}(\alpha^2 - \frac{3}{2}\alpha + 2)^2.$$

This can be rewritten as

$$-3\alpha^2 - 12 = -\frac{3}{13}(2\alpha^2 - 3\alpha + 4)^2.$$

Then,

$$\sqrt{d} = \sqrt{\frac{-3}{13}}(2\alpha^2 - 3\alpha + 4),$$

where we have chosen the sign by convention (choosing the negative of this quantity would mean exchanging α_2 and α_3).

Let $z = \sqrt{-39}$. Since $13 \equiv 1 \pmod 3$, $\sqrt{13}$ is a square in $\mathbb{Q}_3$ and actually $F = \mathbb{Q}_3(z)$. Then,

$$\sqrt{d}z = -6\alpha^2 + 9\alpha - 12.$$

If $a = 2$, we need to compute the square root of $-3\alpha^2 - 24$ in L. Proceeding as in the previous case, we find that

$$-3\alpha^2 - 24 = -\frac{3}{41}(4\alpha^2 - 3\alpha + 16)^2.$$

Hence, choosing again the sign by convention,

$$\sqrt{d} = \sqrt{\frac{3}{-41}}(-4\alpha^2 + 3\alpha - 16).$$

Let us choose $z = \sqrt{-123}$. Since $-41 \equiv 1(\bmod 3)$, $\sqrt{-41}$ is a square in $\mathbb{Q}_3$, so $F = \mathbb{Q}_3(z) = \mathbb{Q}_3(\sqrt{3})$. Then,

$$\sqrt{d}z = -12\alpha^2 + 9\alpha - 48.$$

Now, it is easy to fill the whole matrix $G(H_1, E)$. We have

$$G(H_1, E) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 0 & -6a\alpha^2 + 9\alpha - 12a^2 & -9\alpha^2 - 6a^2\alpha - 18a \\ 2 & -\alpha & -\alpha^2 - 6a \end{pmatrix}.$$

Finally, let us assume that $f(x) = x^3 + 3x^2 + 3$. Let us fix a root α of f. Then,

$$f(x) = (x - \alpha)(x^2 + (\alpha + 3)x + \alpha^2 + 3\alpha),$$

that is, $A = \alpha + 3$ and $B = \alpha^2 + 3\alpha$. We compute

$$d = (\alpha + 3)^2 - 4(\alpha^2 + 3\alpha) = -3\alpha^2 - 6\alpha + 9.$$

In this case,

$$-3\alpha^2 - 6\alpha + 9 = -\frac{1}{7}(2\alpha^2 + 9\alpha + 3)^2$$

Thus,

$$\sqrt{d} = \sqrt{-\frac{1}{7}}(-2\alpha^2 - 9\alpha - 3).$$

Let $z = \sqrt{-7}$. Then $F = \mathbb{Q}_3(z) = \mathbb{Q}_3(\sqrt{-1})$ and

$$\sqrt{d}z = 2\alpha^2 + 9\alpha + 3.$$

From here, we deduce

$$G(H_1, E) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 0 & 2\alpha^2 + 9\alpha + 3 & -9\alpha^2 - 30\alpha - 3 \\ 2 & -\alpha - 3 & -\alpha^2 + 9 \end{pmatrix}$$

4.4.2 Basis of $\mathfrak{A}_{H_1}$

For the radical cases,

$$M(H_1, E) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & -3 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 3 & -1 \end{pmatrix},$$

while for polynomials of the second group, we have

$$M(H_1, E) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -12a^2 & 0 \\ 1 & 9 & -1 \\ 0 & -6a & 0 \\ 0 & -18a & -6a \\ 0 & -6a^2 & 0 \\ 1 & -9 & -1 \end{pmatrix}.$$

In both cases, the Hermite normal form turns out to be

$$D(H_1, E) = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

The columns of its inverse

$$D(H_1, E)^{-1} = \begin{pmatrix} 1 & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} \end{pmatrix}$$

provide a $\mathbb{Z}_3$-basis of $\mathfrak{A}_H$

$$\left\{ w_1, \frac{w_2}{3}, \frac{w_1 + w_3}{3} \right\}$$

for the five polynomials.

Note also that for the radical cases, $E/\mathbb{Q}_3$ has the eigenvectors property with respect to its unique Hopf Galois structure. The matrix of eigenvalues is

$$\Lambda = \begin{pmatrix} 1 & 0 & 2 \\ 1 & -3 & -1 \\ 1 & 3 & -1 \end{pmatrix},$$

with inverse

$$\Omega = \frac{1}{6} \begin{pmatrix} 2 & 2 & 2 \\ 0 & -1 & 1 \\ 2 & -1 & -1 \end{pmatrix}.$$

Then, in the radical cases, $\mathfrak{A}_{H_1}$ has also the $\mathbb{Z}_3$-basis of pairwise orthogonal idempotents

$$\left\{\frac{w_1 - w_3}{3}, \frac{2w_1 - w_2 - w_3}{6}, \frac{2w_1 + w_2 - w_3}{6}\right\}.$$

Finally, for the singular case,

$$M(H_1, E) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 3 & -3 \\ 1 & 9 & -1 \\ 0 & 2 & 0 \\ 0 & -3 & 9 \\ 0 & 30 & 0 \\ 1 & -9 & -1 \end{pmatrix},$$

and the Hermite normal form is

$$D(H_1, E) = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

This provides the basis of $\mathfrak{A}_H$

$$\left\{w_1, w_2, \frac{w_1 + w_3}{3}\right\}.$$

4.4.3 Freeness over $\mathfrak{A}_H$

Let f be of the first group. Since 3 appears twice in the diagonal of D, $I(H_1, E) = 2$ in this case. On the other hand, given $\epsilon = \epsilon_1 + \epsilon_2\alpha + \epsilon_3\alpha^2$, the matrix associated to this element is

$$M_\epsilon(H_1, E) = \begin{pmatrix} \epsilon_1 & 0 & 2\epsilon_1 \\ \epsilon_2 & -3\epsilon_2 & -\epsilon_2 \\ \epsilon_3 & 3\epsilon_3 & -\epsilon_3 \end{pmatrix},$$

with determinant $18\epsilon_1\epsilon_2\epsilon_3$. If $\epsilon = 1 + \alpha + \alpha^2$, then

$$v_3(D_\epsilon(H_1, E)) = 2 = I(H_1, E),$$

so $\mathcal{O}_E$ is $\mathfrak{A}_H$-free and ϵ is a generator.

For the second group, the matrix associated to an element $\epsilon = \epsilon_1 + \epsilon_2\alpha + \epsilon_3\alpha^2$ is

$$M_\epsilon(H_1, E) = \begin{pmatrix} \epsilon_1 & -12a^2\epsilon_2 - 18a\epsilon_3 & 2\epsilon_1 - 6a\epsilon_3 \\ \epsilon_2 & 9\epsilon_2 - 6a^2\epsilon_3 & -\epsilon_2 \\ \epsilon_3 & -6a\epsilon_2 - 9\epsilon_3 & -\epsilon_3 \end{pmatrix},$$

with determinant

$$D_\epsilon(H_1, E) = -18\left(a\epsilon_2{}^2 + 3\,\epsilon_3\epsilon_2 - a^2\epsilon_3{}^2\right)(\epsilon_1 - 2a\,\epsilon_3).$$

If $\epsilon = 1 + \alpha$, then the determinant is $-18a$, and so

$$v_3(D_\epsilon(H_1, E)) = 2 = I(H_1, E).$$

Thus, $\mathcal{O}_E$ is $\mathfrak{A}_H$-free with generator ϵ.

Finally, if f is the sixth polynomial,

$$M_\epsilon(H_1, E) = \begin{pmatrix} \epsilon_1 & -9\,\epsilon_3 + 9\,\epsilon_2 & 2\,\epsilon_1 + 9\,\epsilon_3 - 3\,\epsilon_2 \\ \epsilon_2 & -90\,\epsilon_3 + 27\,\epsilon_2 & -\epsilon_2 \\ \epsilon_3 & -27\,\epsilon_3 + 6\,\epsilon_2 & -\epsilon_3 \end{pmatrix},$$

with determinant

$$D_\epsilon(H_1, E) = 6\,\left({\epsilon_2}^2 - 9\,\epsilon_3\epsilon_2 + 15\,{\epsilon_3}^2\right)(\epsilon_1 - \epsilon_2 + 3\,\epsilon_3)\,.$$

In this case, $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free with generator $\epsilon = 2 + \alpha$.

4.4.4 Summary of results

For the case $p = 3$, we have proved the following:

Theorem 4.11. *Let $E/\mathbb{Q}_3$ be a separable degree 3 extension with dihedral degree 6 Galois closure and let H_1 be its unique Hopf Galois structure.*

1. *The associated order $\mathfrak{A}_{H_1}$ has $\mathbb{Z}_3$-basis*

$$\left\{ w_1, \frac{w_2}{3}, \frac{w_1 + w_3}{3} \right\}$$

for all polynomials but the last one, in which case a basis is

$$\left\{ w_1, w_2, \frac{w_1 + w_3}{3} \right\}.$$

For the first three polynomials, $\mathfrak{A}_{H_1}$ has also a $\mathbb{Z}_3$ basis of pairwise orthogonal idempotents

$$\left\{ \frac{w_1 - w_3}{3}, \frac{2w_1 - w_2 - w_3}{6}, \frac{2w_1 + w_2 - w_3}{6} \right\}.$$

2. *$\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free and a normal basis generator can be determined explicitly at each case.*

4.5 The case $K = \mathbb{Q}_5$

If $p = 5$, then L is the splitting field over $\mathbb{Q}_5$ of one of the polynomials

$$x^5 + 15x^2 + 5, \quad x^5 + 10x^2 + 5, \quad x^5 + 5x^4 + 5,$$

which we call f as usual. Those polynomials appear in [LMFDB, p-adic field 5.5.6.2, p-adic field 5.5.6.1, p-adic field 5.5.8.6], respectively. The majority of the field-theoretical considerations for this case are completely analogous to the case $p = 3$, so we will usually skip them.

However, there are some important differences. For instance, $p = 5 \equiv 1 \pmod 4$, which implies that the Galois group of $L/\mathbb{Q}_5$, which is D_5, is contained in the alternating group A_5. By Galois theory, this is the same as saying that $\operatorname{disc}(f)$ is a square in $\mathbb{Q}_5$. Then, we cannot use the square root of the discriminant to identify the quadratic subextension of $L/\mathbb{Q}_5$. We will get that information from the discriminant of the quadratic polynomials in the decomposition of f in $E[x]$. The other difference is that for a root α of f, the factorisation of f in L does not have coefficients in $\mathbb{Q}(\alpha)$, so we will need to replace f by another polynomial with that property generating the same extension.

4.5.1 The action on E

Let H_1 be the unique Hopf Galois structure of $E/\mathbb{Q}_5$. A basis of H_1 is given by

$$w_1 = \mathrm{Id}, \quad w_2 = z(\mu - \mu^{-1}), \quad w_3 = z(\mu^2 - \mu^{-2}),$$
$$w_4 = \mu + \mu^{-1}, \quad w_5 = \mu^2 + \mu^{-2},$$

where $z \in L$ is a square root of some element in $\mathbb{Q}_5$. Let f be the Amano polynomial defining $L/\mathbb{Q}_5$. For a polynomial g defining the same extension, we have that $g(x) = (x-\alpha)P_1(x)P_2(x)$, where $P_i(x) = x^2 - A_ix + B_i$ is a quadratic polynomial with discriminant $d_i = A_i^2 - 4B_i$, $i \in \{1,2\}$. In this case,

$$G(H_1, E) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 \\ 0 & \sqrt{d_1}z & A_1\sqrt{d_1}z & (A_1^2 - B_1)\sqrt{d_1}z & (A_1^2 - 2B_1)\sqrt{d_1}z \\ 0 & \sqrt{d_2}z & A_2\sqrt{d_2}z & (A_2^2 - B_2)\sqrt{d_2}z & (A_2^2 - 2B_2)\sqrt{d_2}z \\ 2 & A_1 & A_1^2 - 2B_1 & A_1(A_1^2 - 3B_1) & A_1^4 - 4A_1^2B_1 + 2B_1^2 \\ 2 & A_2 & A_2^2 - 2B_2 & A_2(A_2^2 - 3B_2) & A_2^4 - 4A_2^2B_2 + 2B_2^2 \end{pmatrix}.$$

In practice, as in previous cases, we will take g to be some polynomial that decomposes over $\mathbb{Q}(\alpha)$ for α a root of g.

Assume that f is the first polynomial of the three above. By [LMFDB, Number Field 5.1.23765625.1], L is the completion at 5 of the number field generated by a root α of the polynomial

$$g(x) = x^5 - 15x^3 - 10x^2 + 75x + 30,$$

so $L = \mathbb{Q}_5(\alpha)$. Moreover, g splits over E with

$$P_1(x) = x^2 + \left(\frac{-\alpha^4 - \alpha^3 + 11\alpha^2}{6} + 3\alpha - 5\right)x + \frac{\alpha^4}{6} - \frac{\alpha^3}{3} - \frac{7\alpha^2}{3} + \frac{5\alpha}{2} + 10,$$

$$P_2(x) = x^2 + \left(\frac{\alpha^4 + \alpha^3 - 11\alpha^2}{6} - 2\alpha + 5\right)x - \frac{\alpha^3}{2} - \frac{3\alpha^2}{2} + \frac{5\alpha}{2} + 10.$$

Then, we have

$$A_1 = -\left(\frac{-\alpha^4 - \alpha^3 + 11\alpha^2}{6} + 3\alpha - 5\right), \quad B_1 = \frac{\alpha^4}{6} - \frac{\alpha^3}{3} - \frac{7\alpha^2}{3} + \frac{5\alpha}{2} + 10,$$

$$A_2 = -\left(\frac{\alpha^4 + \alpha^3 - 11\alpha^2}{6} - 2\alpha + 5\right), \quad B_2 = -\frac{\alpha^3}{2} - \frac{3\alpha^2}{2} + \frac{5\alpha}{2} + 10,$$

$$d_1 = \frac{\alpha^8 + 2\alpha^7 - 21\alpha^6 - 58\alpha^5 + 121\alpha^4 + 504\alpha^3 - 1440\alpha - 540}{36},$$

$$d_2 = \frac{\alpha^8 + 2\alpha^7 - 21\alpha^6 - 46\alpha^5 + 157\alpha^4 + 396\alpha^3 - 200\alpha^2 - 1080\alpha - 540}{36}.$$

We compute the square root of d_1:

$$\begin{aligned} \alpha^8 &+ 2\alpha^7 - 21\alpha^6 - 58\alpha^5 + 121\alpha^4 + 504\alpha^3 - 1440\alpha - 540 = \\ &= -\frac{3}{65}(3\alpha^4 + 15\alpha^3 - 25\alpha^2 - 110\alpha - 30)^2. \end{aligned}$$

Therefore,

$$\sqrt{d_1} = \frac{1}{6}\sqrt{-\frac{3}{65}}(3\alpha^4 + 15\alpha^3 - 25\alpha^2 - 110\alpha - 30).$$

Now, we have

$$\sqrt{-\frac{65}{3}} = \frac{\sqrt{-39}}{3}\sqrt{5}$$

and $-39 \in \mathbb{Z}_5^2$, so the element

$$z = -\sqrt{-\frac{65}{3}}$$

satisfies $F = \mathbb{Q}_5(z) = \mathbb{Q}_5(\sqrt{5})$ and

$$\sqrt{d_1}z = \frac{1}{6}(3\alpha^4 + 15\alpha^3 - 25\alpha^2 - 110\alpha - 30).$$

Now we compute the square root of d_2:

$$\begin{aligned} \alpha^8 &+ 2\alpha^7 - 21\alpha^6 - 46\alpha^5 + 157\alpha^4 + 396\alpha^3 - 200\alpha^2 - 1080\alpha - 540 = \\ &= -\frac{3}{65}(11\alpha^4 + 25\alpha^3 - 75\alpha^2 - 270\alpha - 30)^2. \end{aligned}$$

Therefore,

$$\sqrt{d_2} = \frac{1}{6}\sqrt{\frac{-3}{65}}(11\alpha^4 + 25\alpha^3 - 75\alpha^2 - 270\alpha - 30),$$

and

$$\sqrt{d_2}z = \frac{1}{6}(11\alpha^4 + 25\alpha^3 - 75\alpha^2 - 270\alpha - 30).$$

Now, we choose f to be the second polynomial. By [LMFDB, Number field 5.1.34515625],

$$g(x) = x^5 - 35x^2 + 50x + 20,$$

generates the same extension as f. Now, g decomposes over E with

$$\begin{aligned} P_1(x) = x^2 &+ \left(-\frac{\alpha^4}{42} - \frac{5\,\alpha^3}{21} - \frac{8\,\alpha^2}{21} + \frac{\alpha}{42} + \frac{85}{21}\right)x \\ &+ \frac{19\,\alpha^4}{42} + \frac{11\,\alpha^3}{21} + \frac{26\,\alpha^2}{21} - \frac{565\,\alpha}{42} + \frac{170}{21}, \end{aligned}$$

$$\begin{aligned} P_2(x) = x^2 &+ \left(\frac{\alpha^4}{42} + \frac{5\,\alpha^3}{21} + \frac{8\,\alpha^2}{21} + \frac{41\,\alpha}{42} - \frac{85}{21}\right)x \\ &+ \frac{2\alpha^4}{21} - \frac{\alpha^3}{21} + \frac{11\,\alpha^2}{21} - \frac{65\,\alpha}{21} + \frac{80}{21}. \end{aligned}$$

$$A_1 = -\left(-\frac{\alpha^4}{42} - \frac{5\,\alpha^3}{21} - \frac{8\,\alpha^2}{21} + \frac{\alpha}{42} + \frac{85}{21}\right), B_1 = \frac{19\,\alpha^4}{42} + \frac{11\,\alpha^3}{21} + \frac{26\,\alpha^2}{21} - \frac{565\,\alpha}{42} + \frac{170}{21},$$

$$A_2 = -\left(\frac{\alpha^4}{42} + \frac{5\,\alpha^3}{21} + \frac{8\,\alpha^2}{21} + \frac{41\,\alpha}{42} - \frac{85}{21}\right), B_2 = \frac{2\alpha^4}{21} - \frac{\alpha^3}{21} + \frac{11\,\alpha^2}{21} - \frac{65\,\alpha}{21} + \frac{80}{21},$$

$$d_1 = \frac{\alpha^8 + 20\,\alpha^7 + 132\,\alpha^6 + 318\,\alpha^5 - 3296\,\alpha^4 - 7128\,\alpha^3 - 14175\,\alpha^2 + 95260\,\alpha - 28220}{1764},$$

$$d_2 = \frac{\alpha^8 + 20\,\alpha^7 + 132\,\alpha^6 + 402\,\alpha^5 + 64\,\alpha^4 - 1752\,\alpha^3 - 7455\,\alpha^2 + 7900\,\alpha + 2020}{1764}.$$

We compute the square root of d_1. We have

$$\alpha^8 + 20\,\alpha^7 + 132\,\alpha^6 + 318\,\alpha^5 - 3296\,\alpha^4 - 7128\,\alpha^3 - 14175\,\alpha^2 + 95260\,\alpha - 28220 = \frac{441}{235}(\alpha^4 + 10\alpha^3 + 20\alpha^2 + 35\alpha - 170)^2.$$

Hence,

$$\begin{aligned}\sqrt{d_1} &= \frac{1}{42}\sqrt{\frac{441}{235}}(\alpha^4 + 10\alpha^3 + 20\alpha^2 + 35\alpha - 170)\\ &= \frac{1}{42}\frac{21}{\sqrt{235}}(\alpha^4 + 10\alpha^3 + 20\alpha^2 + 35\alpha - 170)\end{aligned}$$

Since $\sqrt{235} = \frac{\sqrt{94}}{2}\sqrt{10}$ and $94 \equiv 4 \pmod 5$ is a square in $\mathbb{Z}/5\mathbb{Z}$, the element $z = \sqrt{235}$ satisfies $F = \mathbb{Q}_5(z) = \mathbb{Q}_5(\sqrt{10})$ and

$$\sqrt{d_1}z = \frac{\alpha^4 + 10\alpha^3 + 20\alpha^2 + 35\alpha - 170}{2}.$$

Now, we compute the square root of d_2. In this case,

$$\alpha^8 + 20\,\alpha^7 + 132\,\alpha^6 + 402\,\alpha^5 + 64\,\alpha^4 - 1752\,\alpha^3 - 7455\,\alpha^2 + 7900\,\alpha + 2020 = \frac{(53\alpha^4 + 110\alpha^3 + 260\alpha^2 - 2195\alpha - 190)^2}{235}$$

This implies that

$$\sqrt{d_2} = \frac{1}{42}\sqrt{\frac{1}{235}}(53\alpha^4 + 110\alpha^3 + 260\alpha^2 - 2195\alpha - 190),$$

whence

$$\sqrt{d_2}z = \frac{1}{42}(53\alpha^4 + 110\alpha^3 + 260\alpha^2 - 2195\alpha - 190).$$

Finally, we take f to be the third polynomial. In this case, the same extension is generated by

$$g(x) = x^5 + 10x^4 + 50x^3 + 125x^2 + 150x + 60,$$

which is obtained by applying the change $x \mapsto x + 2$ to the polynomial [LMFDB, Number Field 5.1.3515625.1]. Now, one has $g(x) = (x - \alpha)P_1(x)P_2(x)$ with

$$P_1(x) = x^2 - \frac{5\alpha^4 + 38\alpha^3 - 150\alpha^2 + 199\alpha - 40}{22}x - \frac{\alpha^4}{22} + \frac{5\alpha^3}{11} + \frac{51\alpha^2}{11} + \frac{475\alpha}{22} + \frac{345}{11},$$

$$P_2(x) = x^2 + \frac{5\alpha^4 + 38\alpha^3 + 150\alpha^2 + 221\alpha + 180}{22}x + \frac{3\alpha^4}{11} + \frac{25\alpha^3}{11} + \frac{101\alpha^2}{11} + \frac{170\alpha}{11} + \frac{130}{11}.$$

$$A_1 = \frac{5\alpha^4 + 38\alpha^3 - 150\alpha^2 + 199\alpha - 40}{22}, \quad B_1 = -\frac{\alpha^4}{22} + \frac{5\alpha^3}{11} + \frac{51\alpha^2}{11} + \frac{475\alpha}{22} + \frac{345}{11},$$

$$A_2 = -\frac{5\alpha^4 + 38\alpha^3 + 150\alpha^2 + 221\alpha + 180}{22}, \quad B_2 = \frac{3\alpha^4}{11} + \frac{25\alpha^3}{11} + \frac{101\alpha^2}{11} + \frac{170\alpha}{11} + \frac{130}{11},$$

$$\begin{aligned}d_1 = \frac{1}{484}(&25\,\alpha^8 + 380\,\alpha^7 + 2944\,\alpha^6 + 13390\,\alpha^5 + 37312\,\alpha^4\\ &+55780\,\alpha^3 + 18625\,\alpha^2 - 57720\,\alpha - 59120),\end{aligned}$$

$$d_2 = \frac{1}{484}(25\,\alpha^8 + 380\,\alpha^7 + 2944\,\alpha^6 + 13610\,\alpha^5 + 40568\,\alpha^4$$
$$+75580\,\alpha^3 + 85065\,\alpha^2 + 49640\,\alpha + 9520).$$

We compute the square root of d_1:

$$\sqrt{d_1} = \frac{1}{22}\sqrt{-\frac{1}{3}}(9\alpha^4 + 86\alpha^3 + 402\alpha^2 + 895\alpha + 720).$$

Let $z = \sqrt{-3}$. Then $F = \mathbb{Q}_5(z)$ and

$$\sqrt{d_1}z = \frac{1}{22}(9\alpha^4 + 86\alpha^3 + 402\alpha^2 + 895\alpha + 720).$$

As for d_2, we have

$$\sqrt{d_2} = \frac{1}{22}\sqrt{-\frac{1}{3}}(7\alpha^4 + 62\alpha^3 + 254\alpha^2 + 415\alpha + 120).$$

Then,

$$\sqrt{d_2}z = \frac{1}{22}(7\alpha^4 + 62\alpha^3 + 254\alpha^2 + 415\alpha + 120).$$

Once $\sqrt{d_1}z$ and $\sqrt{d_2}z$ are computed in all cases, we can obtain all the entries of $G(H_1, E)$ following Corollary 4.10.

4.5.2 Basis of $\mathfrak{A}_{H_1}$

We compute a basis for the associated order $\mathfrak{A}_{H_1}$. The matrices of the action for the first, second and third polynomial can be found in (B.16), (B.17) and (B.18) respectively.

For the first polynomial, the Hermite normal form of $M(H_1, E)$ is

$$D(H_1, E) = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

and the columns of its inverse provide a basis for the associated order

$$\left\{ w_1, w_2, \frac{-2w_2 + w_3}{5}, w_4, \frac{w_1 + w_4 + w_5}{5} \right\}$$

Analogously, for the second polynomial, we obtain the Hermite normal form

$$D(H_1, E) = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 5 \end{pmatrix},$$

which provides the basis for $\mathfrak{A}_H$

$$\left\{w_1, w_2, \frac{2w_2+w_3}{5}, w_4, \frac{w_1+w_4+w_5}{5}\right\}.$$

Finally, for the third polynomial,

$$D_E = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

and we obtain the basis of the associated order

$$\left\{w_1, w_2, w_3, w_4, \frac{w_1+w_4+w_5}{5}\right\}.$$

4.5.3 Freeness over $\mathfrak{A}_{H_1}$

From the above we can compute the associated matrix $M_\epsilon(H_1, E)$ of an element $\epsilon = \epsilon_1 + \epsilon_2\alpha + \epsilon_3\alpha^2 + \epsilon_4\alpha^3 + \epsilon_5\alpha^4 \in \mathcal{O}_E$.

For the first polynomial, 5 appears twice in the diagonal of D, so $I(H_1, E) = 2$. On the other hand,

$$D_\epsilon(H_1, E) = 25q_1(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5)$$

for a product q_1 of homogeneous polynomials of degree at most 4 (see (B.19)). We have that $v_5(25) = 2$ and this coincides with $I(H_1, E)$. Taking $\epsilon = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$, $q_2(1, 1, 1, 1, 1)$ is coprime with 5, and then $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free with generator ϵ.

Moving on to the second polynomial, we have that $I(H_1, E) = 2$ and

$$D_\epsilon(H_1, E) = 50q_2(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5)$$

for a product q_2 of homogeneous polynomials of degree at most 4 (see (B.20)). As in the previous case, $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free with generator ϵ.

Finally, for the third polynomial, $I(H_1, E) = 1$ and

$$D_\epsilon(H_1, E) = 10q_3(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5)$$

for a product q_3 of homogeneous polynomials of degree at most 4 (see (B.21)). For $\epsilon = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$ the determinant has 5-adic valuation 1, and again, $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free with generator ϵ.

4.5.4 Summary of results

For the case $p = 5$, we have proved the following results.

Theorem 4.12. *Let $E/\mathbb{Q}_5$ be a separable degree 5 extension with dihedral degree 10 Galois closure and let H_1 be its unique Hopf Galois structure.*

1. *A basis of* $\mathfrak{A}_{H_1}$ *is*

$$\left\{ w_1, w_2, \frac{-2w_2 + w_3}{5}, w_4, \frac{w_1 + w_4 + w_5}{5} \right\},$$

$$\left\{ w_1, w_2, \frac{2w_2 + w_3}{5}, w_4, \frac{w_1 + w_4 + w_5}{5} \right\},$$

$$\left\{ w_1, w_2, w_3, w_4, \frac{w_1 + w_4 + w_5}{5} \right\},$$

for the first, second and third polynomial respectively.

2. $\mathcal{O}_E$ *is* $\mathfrak{A}_{H_1}$*-free and a normal basis generator can be determined explicitly for each case.*

Remark 4.13. The element $\frac{w_1+w_4+w_5}{5}$ obtained in the three bases in Theorem 4.12 is actually $\frac{\mathrm{Id}+\mu+\mu^2+\mu^3+\mu^4}{5}$. Likewise, for $p = 3$, the element $\frac{w_1+w_3}{3}$ was obtained in all the bases in Theorem 4.11, and it is $\frac{\mathrm{Id}+\mu+\mu^2}{3}$. For an arbitrary p, the element $\frac{\sum_{i=0}^{p-1}\mu^i}{p}$ (which acts on E as $\frac{1}{p}$ times the trace map of $J = \langle\sigma\rangle$) always belongs to the associated order $\mathfrak{A}_{H_1}$. Indeed, its action on α gives $\frac{\sum_{i=1}^{p}\alpha_i}{p}$, where $\{\alpha_i\}_{i=1}^{p}$ are the conjugates of α. Working with the symmetric functions of the roots, we see that this is -1 for the field defined by the polynomial $x^p + px^{p-1} + p$ and 0 otherwise.

4.6 Radical cubic extensions of $\mathbb{Q}$

When one chooses $\mathbb{Q}$ instead of $\mathbb{Q}_p$ as ground field, there is not a finite collection of polynomials that covers all possibilities for a non-Galois extension of $L/\mathbb{Q}$. Instead, we will focus on a specific class of these extensions, the radical ones. Concretely, we will take $E = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[3]{m}$, for $m \in \mathbb{Z}$ cube-free and not divisible by 9. Let us write $m = hk^2$, for h and k coprime and square-free integers. An integral basis of E is given as follows (see [Mar77, Exercise 2.41]):

1. If $m \not\equiv 1, -1 (\mathrm{mod}\, 9)$, $B = \{1, \alpha, \frac{\alpha^2}{k}\}$.

2. If $m \equiv s (\mathrm{mod}\, 9)$ with $s \in \{-1, 1\}$, $B = \{1, \alpha, \frac{k^2+sk^2\alpha+\alpha^2}{3k}\}$.

We will first determine the Gram matrix $G(H_1, E_{B'})$ with respect to the power basis $B' = \{1, \alpha, \alpha^2\}$, and then carry out a change of basis so as to obtain the matrix $G(H_1, E_B)$. Actually, this first computation is exactly the same as the one in Section 4.4.1: since $f(x) = (x - \alpha)(x^2 + \alpha + \alpha^2 x)$, A, B and d are the same as in that case, so one has

$$G(H_1, E_{B'}) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 0 & -3\alpha & 3\alpha^2 \\ 2 & -\alpha & -\alpha^2 \end{pmatrix}.$$

In particular, B' is a basis of eigenvectors.

Let us assume that $m \not\equiv \pm 1 \,(\mathrm{mod}\, 9)$. Then,

$$G(H_1, E_B) = G(H_1, E_{B'})P_{B'}^{B} = \begin{pmatrix} 1 & \alpha & \frac{1}{k}\alpha^2 \\ 0 & -3\alpha & \frac{3}{k}\alpha^2 \\ 2 & -\alpha & \frac{-1}{k}\alpha^2 \end{pmatrix}.$$

This means that B is an integral basis of eigenvectors with eigenvalues matrix

$$\Lambda = \begin{pmatrix} 1 & 0 & 2 \\ 1 & -3 & -1 \\ \frac{1}{k} & \frac{3}{k} & \frac{-1}{k} \end{pmatrix}.$$

The inverse is

$$\Omega = \frac{1}{6}\begin{pmatrix} 2 & 2 & 2k \\ 0 & -1 & k \\ 2 & -1 & -k \end{pmatrix}.$$

Then, $\mathfrak{A}_{H_1}$ has a $\mathbb{Z}$-basis of pairwise orthogonal idempotents

$$\left\{ \frac{w_1 - w_3}{3}, \frac{2w_1 - w_2 - w_3}{6}, \frac{2kw_1 + kw_2 - kw_3}{6} \right\}.$$

Moreover, $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free and $\epsilon = 1 + \alpha + \alpha^2$ is a normal integral basis generator.

Now, we assume that $m \equiv \pm 1 \pmod 9$. In this case,

$$G(H_1, E_B) = G(H_1, E_{B'})P_{B'}^{B} = \begin{pmatrix} 1 & \alpha & \frac{k^2+sk^2\alpha+\alpha^2}{3k} \\ 0 & -3\alpha & -k - 2sk\alpha + 3\frac{k^2+sk^2\alpha+\alpha^2}{3k} \\ 2 & -\alpha & k - \frac{k^2+sk^2\alpha+\alpha^2}{3k} \end{pmatrix}.$$

Now, we apply the matrix

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -s & 0 \\ 2 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -s & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

to reduce $M(H_1, E_B)$ to the matrix

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 3 \\ 0 & k & k \\ 0 & 0 & 6 \\ 0 & 0 & 2k \end{pmatrix}.$$

If 3 divided k, since $m = hk^2$, we would have $m \equiv 0 (\mathrm{mod}\, 9)$, but we are assuming $m \equiv \pm 1 \pmod 9$. Then 3 is coprime with k, so we can use Euclid's algorithm for the second and third rows and the fourth and fifth ones to place 1 and 0 instead of k and 3. We obtain then as Hermite normal form

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix},$$

giving the basis of $\mathfrak{A}_{E/\mathbb{Q}}$

$$\Big\{w_1, w_2, \frac{-w_1+w_2}{2}\Big\}.$$

Let us study the freeness over $\mathfrak{A}_{E/\mathbb{Q}}$. For $\epsilon \in \mathcal{O}_E$, one has

$$D_\epsilon(H_1, E) = 2\epsilon_3(sk\epsilon_3 + 3\epsilon_2)(3\epsilon_1 + k\epsilon_3).$$

Let $k = 3a + b$ be the Euclidean division of k by 3. Since 3 does not divide k, $b \in \{1, 2\}$.

- If $b = 1$, then we choose $\epsilon_1 = -a$, $\epsilon_2 = -as$ and $\epsilon_3 = 1$, and we have $D_\epsilon(H_1, E) = 2s$, so $\mathcal{O}_E$ is $\mathfrak{A}_{E/\mathbb{Q}}$-free and $\epsilon = -a - as\alpha + \frac{k^2+sk^2\alpha+\alpha^2}{3k}$ is a generator.

- If $b = 2$, choosing $\epsilon_1 = -(1+a)$, $\epsilon_2 = -s(1+a)$, $\epsilon_3 = 1$, we have again $D_\epsilon(H_1, E) = 2s$, so $\mathcal{O}_E$ is $\mathfrak{A}_{E/\mathbb{Q}}$-free and $\epsilon = -(1+a) - (1+a)s\alpha + \frac{k^2+sk^2\alpha+\alpha^2}{3k}$ is a generator.

To sum up, we have obtained the following result:

Corollary 4.14. *Let $E = \mathbb{Q}(\sqrt[3]{m})$ with $m \in \mathbb{Z}$ not divisible by 9 and write $m = hk^2$, $h, k \in \mathbb{Z}$ coprime and square-free.*

1. *If $m \not\equiv 1, -1 \pmod 9$, $\mathfrak{A}_{H_1}$ has a $\mathbb{Z}$-basis of pairwise orthogonal idempotents*

$$\left\{\frac{w_1 - w_3}{3}, \frac{2w_1 - w_2 - w_3}{6}, \frac{2kw_1 + kw_2 - kw_3}{6}\right\}.$$

Moreover, $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free and $\epsilon = 1 + \alpha + \alpha^2$ is a normal integral basis generator.

2. *If $m \equiv \pm 1 \pmod 9$, $\mathfrak{A}_{H_1}$ has a $\mathbb{Z}$-basis*

$$\Big\{w_1, w_2, \frac{-w_1+w_2}{2}\Big\}.$$

Moreover, $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free and a generator is

$$\epsilon = \begin{cases} -a \mp a\alpha + \frac{k^2 \pm k^2\alpha + \alpha^2}{3k} & \text{if } k \bmod 3 = 1, \\ -(1+a) \mp (1+a)\alpha + \frac{k^2 \pm k^2\alpha + \alpha^2}{3k} & \text{if } k \bmod 3 = 2. \end{cases}$$

Chapter 5

Induced Hopf Galois structures

Let p be an odd prime number. For a separable degree p Hermite extension of fields E/K with dihedral degree $2p$ Galois closure L, we have given account of the associated order in its unique Hopf Galois structure and the Hopf Galois module structure of $\mathcal{O}_E$. Now, we are interested in the Galois closure L/K itself. Namely, we would like to determine all its Hopf Galois structures and the module structure of $\mathcal{O}_L$ over all the corresponding associated orders. Since the Galois group is not abelian, the classical Galois structure and the canonical non-classical Hopf Galois structure are two different Hopf Galois structures of L/K. But other than these, there are a number of other Hopf Galois structures that can be built from the Hopf Galois structures of more simple extensions. These are what we will call induced Hopf Galois structures. Before studying dihedral degree $2p$ extensions, in this chapter we establish the basic theory of induced Hopf Galois structures and their properties.

Let L/K be a Hopf Galois extension of fields. The induction of Hopf Galois structures of L/K consists in the process of construction of Hopf Galois structures in L/K from Hopf Galois structures of other extensions of smaller degree. Under suitable hypotheses on the extension, we can induce Hopf Galois structures of L/K either from L/E and E/K for some intermediate field E of L/K, or from E/K and F/K for some intermediate fields E and F of L/K such that $L = EF$. The notion of induced Hopf Galois structure was introduced in the first approach of the above by Crespo, Rio and Vela in their paper [CRV16]. We will prefer the second approach as it is more suitable for our purposes.

First we will motivate the induction of Hopf Galois structures by presenting the particular case in Galois theory as usual; namely, the product of Galois extensions E/K and F/K, whose Galois group is the direct product of the Galois groups of E/K and F/K. Then we will prove the equivalence of both approaches in the previous paragraph and we shall define induced Hopf Galois structures by means of the corresponding permutation subgroups under the Greither-Pareigis correspondence.

The replacement of the classical Galois structure by an arbitrary Hopf Galois structure translates into the replacement of the direct product of the Galois group by the semidirect product. Consequently, our basic hypothesis will be that the Galois group of L/K is a semidirect product $G = J \rtimes G'$. We will give an explicit description of induced Hopf Galois structures: if $E = L^{G'}$ and $F = L^J$, then all induced Hopf Galois structures arising from the previous decomposition of G as semidirect product are of the form $H = H_1 \otimes_K H_2$ both as Hopf algebras and actions, where H_1 (resp. H_2) is a Hopf Galois structure on E/K (resp. F/K).

In the last section, we will assume that the extension is Hermite and we will study the Hopf Galois module structure of $\mathcal{O}_L$. We shall seek criteria to ensure that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$, and whether the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$ can be deduced from the $\mathfrak{A}_{H_1}$-freeness of $\mathcal{O}_E$ and the $\mathfrak{A}_{H_2}$-freeness of $\mathcal{O}_F$. For both problems, a sufficient condition can be found in the arithmetic disjointness of E/K and F/K. Moreover, for the first one, there is a slightly stronger sufficient condition: the existence of an integral induced basis.

5.1 Inducing a Galois extension

Let E/K and F/K be finite Galois extensions such that $E, F \subset \overline{K}$ such that $E \cap F = K$. We want to construct a Galois extension of K from these two and describe its Galois group in terms of the Galois groups of E/K and F/K. Let us consider the compositum $L = EF$ of E and F. We begin by checking that it is Galois and studying its Galois group.

Proposition 5.1. *Let L_1/K and L_2/K be Galois extensions with $L_1, L_2 \subset \overline{K}$ and let $L = L_1L_2$. Call $G_1 = \mathrm{Gal}(L_1/K)$ and $G_2 = \mathrm{Gal}(L_2/K)$. Then:*

1. *L/K is Galois.*
2. *Let $G = \mathrm{Gal}(L/K)$. The map*

$$\begin{array}{rccc} f\colon & G & \longrightarrow & G_1 \times G_2 \\ & \sigma & \longmapsto & (\sigma|_{L_1}, \sigma|_{L_2}) \end{array}$$

is injective.

Proof. 1. It is straightforward to check that normality and separability are preserved by compositum.

2. Trivially, f is an homomorphism of groups. Let $\sigma \in G$ such that $\sigma|_{L_1} = \mathrm{Id}_{L_1}$ and $\sigma|_{L_2} = \mathrm{Id}_{L_2}$. Since elements of L are sums of products of an element of L_1 and an element of L_2 and σ preserves sums and products, $\sigma = \mathrm{Id}_L$.

□

Thus, we have that this result holds for our extensions E/K and F/K, without needing that $E \cap F = K$. But under this hypothesis, we will show that we can see the extension L/K in *pieces*. We know that elements of L are sums of products of an element of E and an element of F. What we mean by pieces is that for (x, y), $(x', y') \in E \times F$, we have $xy = x'y'$ if and only if $x' = rx$ and $y = ry'$ for some $r \in K$.

Definition 5.2. *We say that two extensions of fields L_1/K and L_2/K with $L_1, L_2 \subset \overline{K}$ are linearly disjoint if the map*

$$\begin{array}{ccc} L_1 \otimes_K L_2 & \longrightarrow & L_1L_2 \\ x \otimes y & \longmapsto & xy \end{array}$$

is an isomorphism of K-algebras.

We are interested in the following equivalent definition of linear disjointness (see [Coh91, Proposition 5.1]).

Proposition 5.3. *Two extensions L_1/K and L_2/K are linearly disjoint if and only if every finite set $S \subset L_1$ which is K-linearly independent is also L_2-linearly independent.*

Another equivalent condition can be consulted in [Lan02, Chapter VIII, §3, Proposition 3.1]. An easy property of linearly disjoint extensions is that their intersection is the base field.

Proposition 5.4. *If L_1/K and L_2/K are linearly disjoint extensions, then $L_1 \cap L_2 = K$.*

Proof. Let $a \in L_1 \cap L_2$. Then, $\{1, a\}$ is a finite subset of L_1 which is L_2-linearly dependent, since $a \cdot 1 - 1 \cdot a = 0$ with $a, -1 \in L_2$. By linear disjointness, $\{1, a\}$ is K-linearly dependent, so there exist $\lambda, \mu \in K$ some not zero such that $\lambda \cdot 1 + \mu \cdot a = 0$. If $\mu = 0$, then $\lambda = 0$ which contradicts linear dependence, so $\mu \neq 0$, and then $a = -\dfrac{\lambda}{\mu} \in K$. □

The converse of this result in general does not hold. However, the converse holds when we assume that the extensions are Galois (see [Cla, Proposition 12.11]).

Proposition 5.5. *Two Galois extensions of fields L_1/K and L_2/K such that $L_1, L_2 \subset \overline{K}$ and $L_1 \cap L_2 = K$ are linearly disjoint.*

Proof. We must check that the map

$$\begin{array}{ccc} L_1 \otimes_K L_2 & \longrightarrow & L_1L_2 \\ x \otimes y & \longmapsto & xy \end{array}$$

is an isomorphism of K-algebras. It is in general an epimorphism, so it is enough to check that the dimensions of domain and codomain coincide, that is,

$$[L_1L_2 : K] = [L_1 : K][L_2 : K].$$

Let $L = L_1L_2$. By Proposition 5.1, L/K is Galois. Then, so are L/L_1 and L/L_2. Let us call $G_i = \mathrm{Gal}(L/L_i)$, $i \in \{1, 2\}$. Let us call $G = \mathrm{Gal}(L/K)$. Since L_1/K and L_2/K are normal extensions, G_1 and G_2 are normal subgroups of G. By the Galois correspondence,

$$L = L^{G_1}L^{G_2} = L^{G_1 \cap G_2},$$

so $G_1 \cap G_2 = \{1_G\}$. Then, $G_1G_2 \cong G_1 \times G_2$. On the other hand, by the hypothesis and the Galois correspondence,

$$K = L_1 \cap L_2 = L^{G_1} \cap L^{G_2} = L^{G_1G_2}.$$

Hence, $G = G_1G_2$. Since this is isomorphic to $G_1 \times G_2$, $|G| = |G_1||G_2|$, which translates into

$$[L : K] = [L : L_1][L : L_2] = \frac{[L : K]}{[L_2 : K]}\frac{[L : K]}{[L_1 : K]}.$$

We conclude that $[L : K] = [L_1 : K][L_2 : K]$. □

From the proof of this result we also deduce the following:

Corollary 5.6. *If L_1/K and L_2/K are Galois extensions such that $L_1, L_2 \subset \overline{K}$ and $L_1 \cap L_2 = K$, then*

$$\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K).$$

That is, the map f in Proposition 5.1 is an isomorphism.

We go back to the case of our extensions E/K and F/K such that $E, F \subset \overline{K}$ and $E \cap F = K$. We have seen that the compositum $L = EF$ gives a Galois extension of K with Galois group the direct product of the Galois groups of E/K and F/K. Using the fundamental theorem of Galois theory, it is straightforward to check that the converse also holds: if L/K is a Galois extension with Galois group $G = J \times G'$ and we define $E = L^{G'}$ and $F = L^J$, then E/K and F/K are Galois and $E \cap F = K$.

Example 5.7. Let L/K be a biquadratic extension. Then, there are different $a, b \in K$ such that $L = K(\sqrt{a}, \sqrt{b})$ and $G = \langle \sigma, \tau \rangle$ with $\sigma^2 = \tau^2 = 1_G$. Then $G = J \times G'$ with $J = \langle \sigma \rangle$ and $G' = \langle \tau \rangle$. Let $E = K(\sqrt{a})$ and $F = K(\sqrt{b})$. By the previous paragraph, E/K and F/K are Galois extensions with $E \cap F = K$. Then, L/K can be seen as the Galois extension induced by E/K and F/K.

Now, we study the behaviour of the group algebras of the corresponding Galois groups.

Corollary 5.8. *With the hypotheses of Proposition 5.1, $K[G] \cong K[J] \otimes_K K[G']$ as K-vector spaces.*

Proof. Since $J \cap G' = \{1_G\}$ and $G = JG'$, $K[J] \otimes_K K[G']$ can be embedded in $K[G]$. Now,

$$\dim_K(K[J] \otimes_K K[G']) = \dim_K(K[J])\dim_K(K[G']) = |J||G'| = |G| = \dim_K(K[G]).$$

We deduce that $K[G] \cong K[J] \otimes_K K[G']$. □

Next, we study the relation between the Galois actions. Recall that for an H-Galois extension L/K, the Hopf algebra H has a linear representation $\rho_H \colon H \longrightarrow \mathrm{End}_K(L)$ associated. In general, for A a $K-$algebra and V a $K-$vector space, a linear representation of A in V is a $K-$algebra homomorphism $\rho \colon A \longrightarrow \mathrm{End}_K(V)$. The tensor product or Kronecker product of two linear representations $\rho_1 \colon A_1 \longrightarrow \mathrm{End}_K(V_1)$ and $\rho_2 \colon A_2 \longrightarrow \mathrm{End}_K(V_2)$ is the representation

$$\rho_1 \otimes \rho_2 \colon A_1 \otimes_K A_2 \longrightarrow \mathrm{End}_K(V_1 \otimes V_2)$$

defined by

$$\rho_1 \otimes \rho_2(a_1 \otimes a_2)(v_1 \otimes v_2) = \rho_1(a_1)(v_1) \otimes \rho_2(a_2)(v_2).$$

This is the correct notion to describe the Galois action on the product of linearly disjoint Galois extensions.

Proposition 5.9. *If E/K and F/K are Galois extensions with groups J and G', such that $E, F \subset \overline{K}$ and $E \cap F = K$, then*

$$\rho_{K[G]} = \rho_{K[J]} \otimes_K \rho_{K[G']}.$$

Proof. We want to see that $\rho_{K[G]} \colon K[G] \longrightarrow \mathrm{End}_K(L)$ and $\rho_{K[J]} \otimes_K \rho_{K[G']} \colon K[J] \otimes_K K[G'] \longrightarrow \mathrm{End}_K(E \otimes_K F)$ coincide. By Corollary 5.8, the domains are isomorphic. Since E/K and F/K are linearly disjoint, the codomains are also isomorphic. Let us identify them. Regarding the definition, we also identify $L = EF$. Given $\sigma \in J$, $\tau \in G'$, $x \in E$ and $y \in F$,

$$\rho_{K[J]} \otimes_K \rho_{K[G']}(\sigma\tau)(xy) = \sigma(x)\tau(y) = (\sigma\tau)(xy) = \rho_{K[G]}(\sigma\tau)(xy),$$

which finishes the proof. □

Now, let us take the extension L/K to be Hermite. The Galois module structure of $\mathcal{O}_L$ has been studied and characterized in the case that the extensions E/K and F/K are arithmetically disjoint.

Definition 5.10. *Two Hermite extensions of fields L_1/K and L_2/K are said to be* ***arithmetically disjoint*** *if they are K-linearly disjoint and their discriminants are coprime.*

Our interest in arithmetically disjoint extensions relies in the fact that if L_1/K and L_2/K are arithmetically disjoint, then $\mathcal{O}_{L_1L_2} = \mathcal{O}_{L_1} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}$ (see [FT92, Chapter III, (2.13)] for a proof). The result that gives account of the associated order and the module structure of $\mathcal{O}_L$ is the following (see [BL96, Lemma 5]):

Proposition 5.11. *Let K be the quotient field of a Dedekind domain $\mathcal{O}_K$ and let E/K, F/K be finite Galois extensions. Put $L = EF$ and suppose that E/K and F/K are arithmetically disjoint. Then:*

1. $\mathfrak{A}_{L/F} = \mathfrak{A}_{E/K} \otimes_{\mathcal{O}_K} \mathcal{O}_F$ *and* $\mathfrak{A}_{L/K} = \mathfrak{A}_{E/K} \otimes_{\mathcal{O}_K} \mathfrak{A}_{F/K}$.
2. *If there exists some $\gamma \in \mathcal{O}_E$ with $\mathcal{O}_E = \mathfrak{A}_{E/K} \cdot \gamma$, then $\mathcal{O}_L = \mathfrak{A}_{L/F} \cdot (\gamma \otimes 1)$.* *If there also exists $\delta \in \mathcal{O}_F$ with $\mathcal{O}_F = \mathfrak{A}_{F/K} \cdot \delta$, then $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot (\gamma \otimes \delta)$.*

5.2 Inducing a Hopf Galois extension

We want to repeat the procedure of the previous section under slightly less restrictive hypotheses over E/K and F/K. Namely, we will assume that E/K is almost classically Galois and F/K is a Galois complement of E/K, that is, $\widetilde{E} \subset E \otimes_K F$. Let us call $L = E \otimes_K F$. By the definition of almost classically Galois extension, the Galois group of L/K is of the form

$$G = J \rtimes G',$$

where $J = \mathrm{Gal}(L/F)$ and $G' = \mathrm{Gal}(L/E)$. Actually, since this is an equivalent definition, we may take the following equivalent approach: instead of assuming that the Galois group of L/K is a direct product $G = J \times G'$, we assume that it is a semidirect product $G = J \rtimes G'$, which implies that E/K is almost classically Galois with Galois complement F/K and $E \cap F = K$.

The aim is to build a Hopf Galois structure on L/K from Hopf Galois structures on each E/K and F/K, which will be what we call an induced Hopf Galois structure. We will prove the following:

Theorem 5.12. *If E/K has a Hopf Galois structure of type N_1 and F/K has a Hopf Galois structure of type N_2, then L/K has a Hopf Galois structure of type $N_1 \times N_2$.*

In the next section, we will give the explicit form of the permutation subgroups involved in this statement. On the other hand, we have:

Proposition 5.13. *The Hopf Galois structures of L/E and F/K are in one-to-one correspondence.*

Proof. By the Galois correspondence, L/E is Galois with group G', and since J is normal in G, F/K is Galois with group G/J. Hence, by using Greither-Pareigis theorem, the Hopf Galois structures of L/E (resp. F/K) are in one-to-one correspondence with regular subgroups of $\mathrm{Perm}(G')$ (resp. $\mathrm{Perm}(G/J)$) normalized by $\lambda^{G'}(G')$ (resp. $\lambda^{G/J}(G/J)$). Since $G' \cong G/J$ and under this isomorphism the definitions of $\lambda^{G/J}$ and $\lambda^{G'}$ are the same, regular subgroups of $\mathrm{Perm}(G')$ normalized by $\lambda^{G'}(G')$ are in bijective correspondence with regular subgroups of $\mathrm{Perm}(G/J)$ normalized by $\lambda^{G/J}(G/J)$. Hence, Hopf Galois structures of L/E and F/K are in bijective correspondence. □

Hence, we can reformulate Theorem 5.12 as follows:

Theorem 5.14. *If E/K has a Hopf Galois structure of type N_1 and L/E has a Hopf Galois structure of type N_2, then L/K has a Hopf Galois structure of type $N_1 \times N_2$.*

This is the result of induction that appears in [CRV16].

Whenever $E \cap F = K$, the extensions E/K and F/K are still linearly disjoint, so actually $L = EF$. This is a consequence of the following result, which generalizes Proposition 5.5.

Theorem 5.15. *Let L_1/K and L_2/K be finite extensions of fields such that one of them is normal and one (possibly the same) separable. Then L_1/K and L_2/K are linearly disjoint if and only if $L_1 \cap L_2 = K$.*

Proof. See [Coh91, Theorem 5.5]. □

Example 5.16. Let E/K be a separable degree p extension of fields whose Galois closure L/K is dihedral of degree $2p$, for an odd prime number p. Let $F = K(z)$ with $z \in L$, $z \notin K$ and $z^2 \in K$, so F/K is quadratic and then Galois. Since $[E : K]$ and $[F : K]$ are coprime, then $E \cap F = K$. By the previous theorem, E/K and F/K are linearly disjoint. Then the extension EF/K is of degree $2p$, so it must be $L = EF$. By Theorem 5.12, we can induce Hopf Galois structures on a dihedral degree $2p$ extension from Hopf Galois structures of its subextensions.

We have seen that when E/K and F/K are Galois, the tensor product of the group algebras of the Galois groups gives a Hopf Galois structure on L/K, but this fact does not hold in general with the semidirect product. Instead, as shown in Theorem 5.12, we multiply the corresponding permutation subgroups which by the Greither Pareigis Theorem give Hopf Galois structures of E/K and F/K.

5.2.1 Induced permutation subgroups

We begin by considering the extension L/K. By the Greither-Pareigis theorem, its Hopf Galois structures are in bijective correspondence with regular subgroups of G normalized by $\lambda(G)$, where

$$\begin{array}{rccl} \lambda\colon & G & \longrightarrow & \mathrm{Perm}(G) \\ & g & \longmapsto & g' \mapsto gg' \end{array}$$

is the left regular representation of G. We explore this map in terms of the decomposition $G = J \rtimes G'$.

Proposition 5.17. *Let $\lambda^J\colon J \longrightarrow \mathrm{Perm}(J)$ (resp. $\lambda^{G'}\colon G' \longrightarrow \mathrm{Perm}(G')$) be the left regular representation of J (resp. G') and let $\phi\colon G \longrightarrow \mathrm{Aut}(G)$ be the map such that $\phi(\tau)$ is the conjugation-by-τ automorphism. Given $g = \sigma\tau, g' = \sigma'\tau' \in G$ with $\sigma, \sigma' \in J$ and $\tau, \tau' \in G'$, we have*

$$\lambda(g)(g') = (\lambda^J(\sigma)\phi(\tau))(\sigma')\lambda^{G'}(\tau)(\tau').$$

Proof.

$$\begin{aligned}\lambda(g)(g') &= gg' \\ &= \sigma\tau\sigma'\tau' = \sigma\tau\sigma'\tau^{-1}\tau\tau' \\ &= \sigma\phi(\tau)(\sigma')\lambda^{G'}(\tau)(\tau') \\ &= (\lambda^{J}(\sigma)\phi(\tau))(\sigma')\lambda^{G'}(\tau)(\tau')\end{aligned}$$

□

Thus, we can describe the left regular representation of G as

$$\lambda = \iota \circ \chi,$$

where ι and χ are the group homomorphisms given by

$$\begin{array}{rccc} \chi\colon & G & \longrightarrow & \mathrm{Perm}(J)\times\mathrm{Perm}(G') \\ & \sigma\tau & \longmapsto & (\lambda^{J}(\sigma)\phi(\tau), \lambda^{G'}(\tau)), \\ \iota\colon & \mathrm{Perm}(J)\times\mathrm{Perm}(G') & \longrightarrow & \mathrm{Perm}(G) \\ & (\varphi,\psi) & \longmapsto & \sigma\tau\mapsto\varphi(\sigma)\psi(\tau). \end{array}$$

Next, we consider the almost classically Galois extension E/K. Recall that we are assuming that F/K satisfies that $\widetilde{E}\subset EF$. By Theorem 1.13, there is also F'/K such that $\widetilde{E} = EF'$. By the Greither-Pareigis theorem, Hopf Galois structures of E/K are in one-to-one correspondence with regular subgroups of $\mathrm{Perm}(\widetilde{G}/\widetilde{G'})$ normalized by $\widetilde{\lambda}(\widetilde{G})$, where $\widetilde{G} = \mathrm{Gal}(\widetilde{E}/K)$, $\widetilde{G'} = \mathrm{Gal}(\widetilde{E}/E)$ and $\widetilde{\lambda}\colon \widetilde{G}\longrightarrow\mathrm{Perm}(\widetilde{G}/\widetilde{G'})$ is the left translation map of G into $\mathrm{Perm}(\widetilde{G}/\widetilde{G'})$. We see that in order to apply the Greither-Pareigis theorem we take the Galois group of the extension given by adjoining F'/K to E/K. Let us call $G = \mathrm{Gal}(L/K)$ and $G' = \mathrm{Gal}(L/E)$. The fundamental theorem of Galois theory gives us the isomorphisms

$$\mathrm{Gal}(\widetilde{E}/K)\cong\mathrm{Gal}(L/K)/\mathrm{Gal}(L/\widetilde{E}),$$

$$\mathrm{Gal}(\widetilde{E}/E)\cong\mathrm{Gal}(L/E)/\mathrm{Gal}(L/\widetilde{E}).$$

Hence, there is a canonical bijection $\widetilde{G}/\widetilde{G'}\cong G/G'$ which induces an isomorphism $\mathrm{Perm}(\widetilde{G}/\widetilde{G'})\cong\mathrm{Perm}(G/G')$, under which the definition of the map $\widetilde{\lambda}$ coincides with the one of

$$\begin{array}{rccc} \overline{\lambda}\colon & G & \longrightarrow & \mathrm{Perm}(G/G') \\ & g & \longmapsto & \overline{g'}\mapsto\overline{gg'} \end{array},$$

which is the left translation map of G into $\mathrm{Perm}(G/G')$. Hence, regular subgroups of $\mathrm{Perm}(\widetilde{G}/\widetilde{G'})$ normalized by $\widetilde{\lambda}(\widetilde{G})$ are in bijective correspondence with regular subgroups of $\mathrm{Perm}(G/G')$ normalized by $\overline{\lambda}(G)$. Thus, in order to compute the Hopf Galois structures of E/K, we can apply the Greither-Pareigis theorem with the Galois group of any extension of K that contains the Galois closure $\widetilde{E}$ of E/K, instead of the Galois group of $\widetilde{E}/K$ itself.

Under this consideration, Hopf Galois structures of E/K are in one-to-one correspondence with regular subgroups of $\mathrm{Perm}(G/G')$ normalized by $\overline{\lambda}(G)$. Now, J is a transversal of G' in G, that is, at every left coset of G/G' there is a unique element of J. Let us write $J = \{\sigma_1,...,\sigma_r\}$. Then, we can write $G/G' = \{\sigma_1G',...,\sigma_rG'\}$ and identify J with G/G'. Carrying this identification to $\overline{\lambda}$ we obtain a map $\lambda_c\colon G\longrightarrow\mathrm{Perm}(J)$ whose definition corresponds to the action of G on left cosets of G/G'. But this action turns out to be the first component of χ.

Proposition 5.18. *Let $\pi_1\colon \mathrm{Perm}(J)\times\mathrm{Perm}(G')\longrightarrow\mathrm{Perm}(J)$ be the projection onto the first component. Then, $\lambda_c=\pi_1\circ\chi$.*

Proof. It is enough to check that the action of G on the left cosets of G/G' is the definition of the first component of χ. Let $g=\sigma\tau\in G$ with $\sigma\in J$ and $\tau\in G'$. Given $i\in\{1,\dots,n\}$,

$$\begin{aligned} g\cdot(\sigma_iG') &= \sigma\tau\sigma_iG'=\sigma(\tau\sigma_i\tau^{-1})\tau G'=\sigma\phi(\tau)(\sigma_i)G'\\ &=\lambda^J(\sigma)\phi(\tau)(\sigma_i)G'=\pi_1\circ\chi(g)(\sigma_i)G'. \end{aligned}$$

This means that $\overline{\lambda}(g)(\sigma_iG')=\pi_1\circ\chi(g)(\sigma_i)G'$, and by means of the identification of G/G' with J we obtain that $\lambda_c(g)(\sigma_i)=\pi_1\circ\chi(g)(\sigma_i)$. Since g and i are arbitrary, $\lambda_c=\pi_1\circ\chi$. □

Corollary 5.19. *Given $g=\sigma\tau\in G$ with $\sigma\in J$ and $\tau\in G'$,*

$$\chi(g)=(\lambda_c(g),\lambda^{G'}(\tau)).$$

Example 5.20. Let L/K be a dihedral degree $2p$ extension of fields with Galois group G. We establish the presentation

$$G=\langle\sigma,\tau\rangle,\ \sigma^p=\tau^2=1,\ \tau\sigma=\sigma^{-1}\tau.$$

We review the lattice of subgroups of G: it has a unique order p subgroup $J=\langle\sigma\rangle$ and p order 2 subgroups $G'_d=\langle\sigma^d\tau\rangle$, where d ranges from 0 to $p-1$. Then G has p possible decompositions as semidirect product

$$G=J\rtimes G'_d,\ 0\leq d\leq p-1.$$

As in the discussion preceding Theorem 4.1, let us fix d and denote $G'=G'_d$. Let us check in this concrete example that the maps $\overline{\lambda}$ and λ_c are compatible. The map $\overline{\lambda}\colon G\longrightarrow\mathrm{Perm}(G/G')$ operates as follows:

$$\overline{\lambda}(\sigma^i)(\overline{\sigma^k})=\overline{\sigma^{i+k}},$$

$$\overline{\lambda}(\sigma^i\tau)(\overline{\sigma^k})=\overline{\sigma^i\tau\sigma^k}=\overline{\sigma^{i-k}\tau}=\overline{\sigma^{i-k-d}}$$

On the other hand, by Proposition 5.18, the definition of the map $\lambda_c\colon G\longrightarrow\mathrm{Perm}(J)$ is given by:

$$\lambda_c(\sigma^i)(\sigma^k)=\lambda^J(\sigma^i)(\sigma^k)=\sigma^{i+k},$$
$$\lambda_c(\sigma^i\tau)(\sigma^k)=\lambda_c(\sigma^{i-d}\sigma^d\tau)(\sigma^k)=\lambda^J(\sigma^{i-d})\phi(\sigma^d\tau)(\sigma^k)=\sigma^{i-d}\sigma^d\tau\sigma^{k+d}\tau=\sigma^{i-k-d}.$$

5.2.2 The Induction Theorem

We proceed to construct a Hopf Galois structure on L/K from Hopf Galois structures on E/K and F/K working with the corresponding permutation groups. We will prove a more general version of Theorem 5.12 by showing the explicit form of the subgroup of $\mathrm{Perm}(G)$ that gives the induced Hopf Galois structure. Concretely:

Theorem 5.21 (Induction Theorem). *Let $N_1\leq\mathrm{Perm}(J)$ be regular and normalized by $\lambda_c(G)$ and let $N_2\leq\mathrm{Perm}(G')$ be regular and normalized by $\lambda^{G'}(G')$. Then, $N=\iota(N_1\times N_2)$ is a regular subgroup of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$.*

The proof of this theorem will follow from the results that regularity and stability by action of the corresponding groups are preserved when multiplying N_1 and N_2.

Proposition 5.22. *If $N_1 \leq \mathrm{Perm}(J)$ and $N_2 \leq \mathrm{Perm}(G')$ are regular, so is N.*

Proof. Since $|N| = |\iota(N_1 \times N_2)| = |N_1 \times N_2| = |N_1||N_2| = |J||G'| = |G|$, it is enough to check that the action of N on G is transitive. Let $g = \sigma\tau$, $g' = \sigma'\tau' \in G$ with $\sigma, \sigma' \in J$ and $\tau, \tau' \in G'$. Since N_1 (resp. N_2) is regular, there exists $\varphi \in \mathrm{Perm}(J)$ (resp. $\psi \in \mathrm{Perm}(G')$) such that $\varphi(\sigma) = \sigma'$ (resp. $\psi(\tau) = \tau'$). Then,

$$\iota(\varphi, \psi)(g) = \iota(\varphi, \psi)(\sigma\tau) = \varphi(\sigma)\psi(\tau) = \sigma'\tau' = g'.$$

□

Proposition 5.23. *If $N_1 \leq \mathrm{Perm}(J)$ is normalized by $\lambda_c(G)$ and $N_2 \leq \mathrm{Perm}(G')$ is normalized by $\lambda^{G'}(G')$, then:*

1. *$N_1 \times N_2$ is normalized by $\chi(G)$.*
2. *$\iota(N_1 \times N_2)$ is normalized by $\lambda(G)$.*

Proof.

1. By Corollary 5.19, $\chi(g) = (\lambda_c(g), \lambda^{G'}(\tau))$ for every $g = \sigma\tau \in G$ with $\sigma \in J$ and $\tau \in G'$. Then, given $(\eta, \mu) \in N_1 \times N_2$,

$$\chi(g)(\eta, \mu)\chi(g^{-1}) = (\lambda_c(g)\eta\lambda_c(g)^{-1}, \lambda^{G'}(\tau)\mu\lambda^{G'}(\tau^{-1})) \in N_1 \times N_2.$$

2. It follows immediately from 1 and the fact that ι is an homomorphism of groups: if $(\eta, \mu) \in N_1 \times N_2$ and $g \in G$,

$$\lambda(g)\iota(\eta, \mu)\lambda(g^{-1}) = \iota \circ \chi(g)\iota(\eta, \mu)\iota \circ \chi(g^{-1}) = \iota(\chi(g)(\eta, \mu)\chi(g^{-1})) \in \iota(N_1 \times N_2).$$

□

The Induction Theorem assures that every pair of Hopf Galois structures of E/K and F/K (or L/E) gives rise to a Hopf Galois structure on L/K.

Definition 5.24. *Every Hopf Galois structure on L/K given by Theorem 5.21 is called **induced**.*

We see some examples of induced Hopf Galois structures.

Example 5.25. The induction procedure generalizes the product of Galois extensions presented at Section 5.1 of this chapter. Indeed, if L/K is Galois with group $G = J \times G'$, then G is in particular a semidirect product. Let $E = L^{G'}$ and $F = L^J$. Then both E/K and F/K are Galois with $\mathrm{Gal}(E/K) = G/G' \cong J$ and $\mathrm{Gal}(F/K) = G/J \cong G'$. By abuse of notation, let us call $J = \mathrm{Gal}(E/K)$. The classical Galois structure of E/K (resp. L/E) is given by $\rho^J(J)$ (resp. $\rho^{G'}(G')$) where $\rho^J \colon J \longrightarrow \mathrm{Perm}(J)$ (resp. $\rho^{G'} \colon G' \longrightarrow \mathrm{Perm}(G')$) is the right regular representation of J (resp. G'). By induction theorem, they induce the Hopf Galois structure given by $\iota(\rho^J(J) \times \rho^{G'}(G')) \leq \mathrm{Perm}(G)$. Given $g = \sigma\tau, g' = \sigma'\tau' \in G$ with $\sigma, \sigma' \in J$ and $\tau, \tau' \in G'$, one has

$$\iota(\rho^J(\sigma)\rho^{G'}(\tau))(g') = \rho^J(\sigma)(\sigma')\rho^{G'}(\tau)(\tau') = \sigma'\sigma^{-1}\tau'\tau^{-1} = \sigma'\tau'(\sigma\tau)^{-1} = \rho(g)(g'),$$

so $\iota(\rho^J(J) \times \rho^{G'}(G')) = \rho(G)$ gives the classical Galois structure of L/K.

Example 5.26. Let us consider again a dihedral degree $2p$ extension L/K and recover the notation of Example 5.20. For each decomposition $G = J \rtimes G'$ of $G := \mathrm{Gal}(L/K)$ as semidirect product, the subgroups of $\mathrm{Perm}(G)$ giving an induced Hopf Galois structure on L/K are of the form

$$N = \iota(N_1 \times N_2),$$

where N_1 is a regular subgroup of $\mathrm{Perm}(J)$ normalized by $\lambda_c(G)$ and N_2 is a regular subgroup of $\mathrm{Perm}(G')$ normalized by $\lambda^{G'}(G')$. In this case, $\mathrm{Perm}(J)$ has a unique regular subgroup $N_1 = \langle(\mathrm{Id}, \sigma, \dots, \sigma^p)\rangle$, and it is normalized by $\lambda_c(G)$, and $\mathrm{Perm}(G')$ has also a unique regular subgroup $N_2 = \langle(\mathrm{Id}, \tau)\rangle$, trivially normalized by $\lambda^{G'}(G')$. As there are p possibilities for G' and J is unique, L/K has in total p induced Hopf Galois structures.

If $p = 3$:

1. For $J = \langle\sigma\rangle$ and $G' = \langle\tau\rangle$, $N = \langle(1_G, \sigma\tau, \sigma^2, \tau, \sigma, \sigma^2\tau)\rangle$.
2. For $J = \langle\sigma\rangle$ and $G' = \langle\sigma\tau\rangle$, $N = \langle(1_G, \sigma^2\tau, \sigma^2, \sigma\tau, \sigma, \tau)\rangle$.
3. For $J = \langle\sigma\rangle$ and $G' = \langle\sigma^2\tau\rangle$, $N = \langle(1_G, \tau, \sigma^2, \sigma^2\tau, \sigma, \sigma\tau)\rangle$.

From a theoretical point of view, the existence of induced Hopf Galois structures is assured in case the Galois group is semidirect. However, it is interesting to analyze the relations involving Hopf algebras and Hopf actions of the extensions L/K, E/K and F/K.

5.2.3 Induced Hopf algebras

First, we describe the Hopf algebras involved in the Induction Theorem. By the Greither-Pareigis Theorem, these are

$$H = L[\iota(N_1 \times N_2)]^G,\ H_1 = L[N_1]^G,\ \overline{H} = L[N_2]^{G'},\ H_2 = F[N_2]^{G/J} = L[N_2]^G.$$

We know that the Hopf Galois structures of H_2 and $\overline{H}$ correspond to each other by means of the bijective correspondence showed in Proposition 5.13. Actually, this correspondence works as follows:

$$\begin{array}{ccc} \{\text{Hopf Galois structures of } L/E\} & \longleftrightarrow & \{\text{Hopf Galois structures of } F/K\} \\ \overline{H} & \longmapsto & \overline{H}^J \\ E \otimes_K H_2 & \longmapsfrom & H_2 \end{array}.$$

Remark 5.27. *The actions of the Hopf algebras involved work as follows:*

- *$E \otimes_K H_2$ acts on $L = E \otimes_K F$ through the product on E in the first factor and the Hopf action in the second one.*
- *The E-action of $\overline{H} = L[N_2]^{G'}$ on L is J-equivariant, namely $\sigma(h \cdot x) = \sigma(h) \cdot \sigma(x)$ for $\sigma \in J$, $h \in \overline{H}$ and $x \in L$. Indeed, J acts on L by the classical Galois action and by conjugation on N_2, but this last action turns out to be trivial. Consequently, the restricted action of $\overline{H}^J$ on $L = F^J$ makes sense, and this is the Hopf Galois action of H_2 on F.*

The result that gives the form of the Hopf algebra H in the Hopf Galois structure on L/K is the following.

Theorem 5.28. *Let H be the Hopf algebra of the induced Hopf Galois structure on L/K given by the permutation subgroup $N = \iota(N_1 \times N_2)$. Let H_1 (resp. H_2) be the Hopf algebra of the Hopf Galois structure on E/K (resp. F/K) given by N_1 (resp. N_2). Then,*

$$H = H_1 \otimes_K H_2.$$

Proof. We have

$$\begin{aligned} H &= L[\iota(N_1 \times N_2)]^G \\ &= L[\iota(N_1 \times \{1\})\iota(\{1\} \times N_2)]^G = (L[\iota(N_1 \times \{1\})] \otimes_K L[\iota(\{1\} \times N_2)])^G \\ &= (L[N_1] \otimes_K L[N_2])^G. \end{aligned}$$

Since λ factorizes through $\mathrm{Perm}(J) \times \mathrm{Perm}(G)$, the action of G on $L[N_1] \otimes_K L[N_2]$ by conjugation by $\lambda(G)$ coincides with the action by conjugation by $\lambda_c(G)$ on the first factor and conjugation by $\lambda^{G'}(G')$ on the second factor. Hence,

$$H = (L[N_1] \otimes_K L[N_2])^G = L[N_1]^G \otimes_K L[N_2]^G = H_1 \otimes_K H_2.$$

□

Note that this result is the naive generalization of Corollary 5.8.

5.2.4 Induced Hopf actions

Finally, we see the action of H on L in terms of the action of H_1 on E and of H_2 on F.

Proposition 5.29. *Given $w \in H_1$, $\eta \in H_2$, $x \in E$ and $y \in F$,*

$$(w \otimes \eta) \cdot (x \otimes y) = (w \cdot x)(\eta \cdot y),$$

that is,

$$\rho_H = \rho_{H_1} \otimes_K \rho_{H_2}.$$

Proof. Let us write $N_1 = \{\eta_i\}_{i=1}^r$, $N_2 = \{\mu_j\}_{j=1}^u$. Then,

$$w \in H_1 = L[N_1]^G \Longrightarrow w = \sum_{i=1}^r c_i\eta_i, c_i \in L,$$

$$\eta \in H_2 = L[N_2]^G \Longrightarrow \eta = \sum_{j=1}^u d_j\mu_j,\ d_j \in L.$$

Hence,

$$\begin{aligned} (w \otimes \eta) \cdot (x \otimes y) &= \left(\sum_{i=1}^r \sum_{j=1}^u c_i d_j \iota(\eta_i, \mu_j)\right) \cdot (x \otimes y) \\ &= \sum_{i=1}^r \sum_{j=1}^u c_i d_j \iota(\eta_i, \mu_j)^{-1}(\mathrm{Id}_G)(xy) = \sum_{i=1}^r \sum_{j=1}^u c_i d_j \iota(\eta_i^{-1}, \mu_j^{-1})(\mathrm{Id}_G)(xy) \\ &= \sum_{i=1}^r \sum_{j=1}^u \eta_i^{-1}(\mathrm{Id}_J)(x)\mu_j^{-1}(\mathrm{Id}_{G'})(y) \\ &= \left(\sum_{i=1}^r c_i\eta_i^{-1}(\mathrm{Id}_J)(x)\right)\left(\sum_{j=1}^u d_j\mu_j^{-1}(\mathrm{Id}_{G'})(y)\right) \\ &= (w \cdot x)(\eta \cdot y) \end{aligned}$$

□

Again, this result generalizes the behaviour of the Galois action in Proposition 5.9. We can use it to prove the naive generalization of Lemma 2.48.

Proposition 5.30. *The product of bases of eigenvectors of E and F with respect to the actions of H_1 and H_2 is a basis of eigenvectors of L with respect to the action of H.*

Proof. Let $\{\alpha_k\}_{k=1}^r$ be a basis of eigenvectors of E and $\{z_l\}_{l=1}^u$ a basis of eigenvectors of F. Let $\{w_i\}_{i=1}^r$, $\{\eta_j\}_{j=1}^u$ be K-bases of H_1 and H_2, so that $\{w_i\eta_j\}_{i,j}$ is J-basis of H. By hypothesis,

$$w_i \cdot \alpha_k = \lambda_{ik}\alpha_k,\ 1 \leq i,k \leq r,$$

$$\eta_j \cdot z_l = \mu_{jl}z_l,\ 1 \leq j,l \leq u.$$

Now, $\{\alpha_i z_j\}_{i,j=1}^n$ is a K-basis of L, and the action of H on this basis is

$$(w_i\eta_j) \cdot (\alpha_k z_l) = (w_i \cdot \alpha_k)(\eta_j \cdot \alpha_l) = \lambda_{ik}\mu_{jl}\alpha_k z_l.$$

□

Theorem 5.28 and Proposition 5.29 together mean that the Hopf Galois structures (H_1, ρ_{H_1}) of E/K and (H_2, ρ_{H_2}) of F/K produce (induce) the induced Hopf Galois structure $(H_1 \otimes_K H_2, \rho_{H_1} \otimes_K \rho_{H_2})$. We remark that the converse trivially holds: if (H, ρ_H) is an induced Hopf Galois structure on L/K, then H and ρ_H must decompose as above for some decomposition $G = J \rtimes G'$ of the Galois group as a semidirect product. Thus, we have:

Corollary 5.31. *Let L/K be a Galois extension. The induced Hopf Galois structures of L/K are of the form*

$$(H_1 \otimes_K H_2, \rho_{H_1} \otimes_K \rho_{H_2}),$$

where (H_1, ρ_{H_1}) is a Hopf Galois structure on $E = L^{G'}/K$, (H_2, ρ_{H_2}) is a Hopf Galois structure on $F = L^J/K$ and $G = J \rtimes G'$ runs through the decompositions of G as a semidirect product.

5.3 Induced Hopf Galois module structure

Let L/K be an H-Galois Hermite extension of fields, where H is an induced Hopf Galois structure. From now on we will keep the convention $H = H_1 \otimes_K H_2$, with H_1 a Hopf Galois structure on E/K and H_2 a Hopf Galois structure on F/K.

In this part we will address the problems of determining the associated order and the freeness of $\mathcal{O}_L$ not only for the induced Hopf Galois structure H, but also for the inducing structures H_1 and H_2. We will apply the reduction method simultaneously to the three Hopf Galois structures and try to relate them. We shall check that the behaviour is far from trivial. Regarding the associated order, one may expect that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$, but this does not happen in general. As for the freeness over $\mathfrak{A}_H$, the products of generators of $\mathcal{O}_E$ as $\mathfrak{A}_{H_1}$-module and of $\mathcal{O}_F$ as $\mathfrak{A}_{H_2}$-module is not in general a generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module. However, as in the Galois case, both of them hold when E/K and F/K are arithmetically disjoint. Moreover, for the associated order, we shall provide a stronger sufficient condition.

5.3.1 Relation between the matrices of actions

The starting point of the reduction method is the determination of the matrix of the action. For this reason, it seems reasonable to try to find some relation between the matrices of the actions involved in the induction procedure; namely $M(H, L)$, $M(H_1, E)$ and $M(H_2, F)$. Since no reduction is performed in this part, actually we can take L/K as an arbitrary H-Galois extension of fields.

The Kronecker product

As $H = H_1 \otimes_K H_2$ and $\rho_H = \rho_{H_1} \otimes_K \rho_{H_2}$, one may expect that the relation between the aforementioned matrices might have something to do with the tensor product. The analogous notion of tensor product for matrices is the following:

Definition 5.32. *Let F be a field and let $A = (a_{ij}) \in \mathcal{M}_{m_1 \times n_1}(F)$ and $B = (b_{kl}) \in \mathcal{M}_{m_2 \times n_2}(F)$. The* ***Kronecker product*** *of the matrices A and B is the matrix $A \otimes B = (c_{xy})_{x,y} \in \mathcal{M}_{m_1 m_2 \times n_1 n_2}(F)$ whose entries are given by the relations:*

$$a_{ij} b_{kl} = c_{(i-1)m_2+k,(j-1)n_2+l}$$

In other words, the Kronecker product of two matrices A and B is the matrix whose entries are products between all possible entries of A and B, arranged so that any entry of A is multiplied by all possible entries of B. For instance:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix} \implies A \otimes B = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{11}b_{31} & a_{11}b_{32} & a_{12}b_{31} & a_{12}b_{32} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \\ a_{21}b_{31} & a_{21}b_{32} & a_{22}b_{31} & a_{22}b_{32} \end{pmatrix}.$$

Induced Gram matrix

Going back to the induced Hopf Galois structure $H = H_1 \otimes_K H_2$ of L/K, we may deduce easily from Proposition 5.29 the relation between the Gram matrices involved:

$$G(H, L) = G(H_1, E) \otimes G(H_2, F),$$

whenever we consider in L the basis B which is the product of the previously fixed bases of E and F. If B' is another basis of L, we can combine the previous equality with the one in Proposition 2.10 to obtain:

$$G(H, L_{B'}) = (G(H_1, E) \otimes G(H_2, F))P_B^{B'}.$$

Then, to compute the Gram matrix of an induced Hopf Galois structure is quite straightforward once one knows the Gram matrices of the inducing Hopf Galois structures.

Remark 5.33. This is actually the strategy we have followed in Sections 3.3 and 3.5 to study the classical Galois structure of elementary abelian extensions of $\mathbb{Q}$ and $\mathbb{Q}_2$. Indeed, in those cases the basis $B_c = \{e_1, e_2, e_3, e_4\}$ is *almost* a product basis of the extensions $E = K(e_3)$ and $F = K(e_2)$, where $K = \mathbb{Q}$ or $\mathbb{Q}_2$. It is not exactly the product basis because e_4 is not the product of e_2 and e_3 but it is so up to multiplication by an element in the ground field, which does not affect the action. Let us call H_1 (resp. H_2) the unique Hopf Galois structure on E/K (resp. F/K). Then

$$G(H_1, E) = \begin{pmatrix} e_1 & e_3 \\ e_1 & -e_3 \end{pmatrix}, \qquad G(H_2, F) = \begin{pmatrix} e_1 & e_2 \\ e_1 & -e_2 \end{pmatrix},$$

$$G(H_c, L_{B_c}) = \begin{pmatrix} e_1 & e_3 \\ e_1 & -e_3 \end{pmatrix} \otimes \begin{pmatrix} e_1 & e_2 \\ e_1 & -e_2 \end{pmatrix} = \begin{pmatrix} e_1 & e_2 & e_3 & e_4 \\ e_1 & -e_2 & e_3 & -e_4 \\ e_1 & e_2 & -e_3 & -e_4 \\ e_1 & -e_2 & -e_3 & e_4 \end{pmatrix}$$

Induced matrix of the action

The relation between the matrices of the action is not as straightforward. Namely, it does not hold in general that $M(H, L) = M(H_1, E) \otimes M(H_2, F)$, even if in H and L we fix the corresponding product bases. The reason is that carrying out the tensor product and transforming from matrices to column vectors are not commutative operations. However, the equality holds up to a permutation of the rows. Concretely:

Theorem 5.34. *Let us fix the product bases of H and L. Then, there is a permutation matrix $P \in \mathcal{M}_{n^2}(K)$ such that*

$$PM(H, L) = M(H_1, E) \otimes M(H_2, F).$$

Proof. Let $n = [L : K]$, $r = [E : K]$ and $u = [F : K]$ (in particular $n = ru$). Let us fix a K-basis $\{w_i\}_{i=1}^r$ of H_1 and a K-basis $\{\eta_j\}_{j=1}^u$ of H_2. Since $H = H_1 \otimes_K H_2$, $\{w_i\eta_j\}_{i,j=1}^n$ is a K-basis of H, and similarly, since $L = E \otimes_K F$, for bases $\{\alpha_k\}_{k=1}^r$ of E and $\{z_l\}_{l=1}^u$ of F, $\{\alpha_k z_l\}_{k,l}$ is a K-basis of L. These are the bases we use to build the matrix $M(H, L)$.

We will use the description of the matrices of the action provided by Proposition 2.5. First we fix some notation. Given $m \geq 0$, let $\varphi_m \colon \mathcal{M}_m(K) \longrightarrow K^{m^2}$ be the map that takes matrices to column vectors. For $a, b \geq 0$ we call E^m_{ab} the matrix with zero in all entries but the (a, b)-th one, filled with 1. Then, $\{E^m_{ab}\}_{a,b=1}^m$ is a K-basis of $\mathcal{M}_m(K)$.

We compute the columns of $M(H, L)$ and $M(H_1, E) \otimes M(H_2, F)$ and compare them to find the suitable permutation. The columns of $M(H, L)$ are

$$\{\varphi_n(\rho_H(w_i \otimes \eta_j))\}_{i,j=1}^n.$$

Since $\rho_H = \rho_{H_1} \otimes \rho_{H_2}$ by Proposition 5.29,

$$\varphi_n(\rho_H(w_i \otimes \eta_j)) = \varphi_n(\rho_{H_1}(w_i) \otimes \rho_{H_2}(\eta_j)).$$

Now, $\rho_H(w_i \otimes \eta_j) \in \mathcal{M}_n(K)$, so it is linear combination of elements of the form $E^r_{ab} \otimes E^u_{cd}$. And we have:

$$\varphi_n(E^r_{ab} \otimes E^u_{cd}) = \varphi_n(E^n_{u(a-1)+c, u(b-1)+d}) = e_{nu(b-1)+n(d-1)+u(a-1)+c}.$$

On the other hand, the columns of $M(H_1, E) \otimes M(H_2, F)$ are

$$\{\varphi_r(\rho_{H_1}(w_i)) \otimes \varphi_u(\rho_{H_2}(\eta_j))\}_{i,j=1}^n.$$

Moreover, $\rho_{H_1}(w_i) \in \mathcal{M}_r(K)$ and $\rho_{H_2}(\eta_j) \in \mathcal{M}_u(K)$. Then:

$$\varphi_r(E^r_{ab}) \otimes \varphi_u(E^u_{cd}) = e^r_{r(b-1)+a} \otimes e^u_{u(d-1)+c} = e_{nu(b-1)+u^2(a-1)+u(d-1)+c}.$$

Let P be the $n^2 \times n^2$ matrix obtained by permuting the rows of the identity matrix following the permutation of $\{1, ..., n\}$

$$nu(b-1) + n(d-1) + u(a-1) + c \longmapsto nu(b-1) + u^2(a-1) + u(d-1) + c,$$

for $1 \leq a, b \leq r$ and $1 \leq c, d \leq u$. By construction,

$$P\varphi_n(E^r_{ab} \otimes E^u_{cd}) = \varphi_r(E^r_{ab}) \otimes \varphi_u(E^u_{cd}).$$

Then, by K-linearity,

$$P\varphi_n(\rho_H(w_i \otimes \eta_j)) = \varphi_r(\rho_{H_1}(w_i)) \otimes \varphi_u(\rho_{H_2}(\eta_j))$$

for every $1 \leq i, j \leq n$. Therefore,

$$\begin{aligned} PM(H,L) &= P\begin{pmatrix} | & | & | \\ \varphi_n(w_1 \otimes \eta_1) & \dots & \varphi_n(w_r \otimes \eta_u) \\ | & | & | \end{pmatrix} \\ &= \begin{pmatrix} | & | & | \\ \varphi_r(w_1) \otimes \varphi_u(\eta_1) & \dots & \varphi_r(w_r) \otimes \varphi_u(\eta_u) \\ | & | & | \end{pmatrix} \\ &= M(H_1, E) \otimes M(H_2, F). \end{aligned}$$

□

Remark 5.35. When L/K is a Hermite extension, $P \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ is a unimodular matrix, as its entries are 0 or 1 and its determinant is 1 or -1.

Remark 5.36. The permutation only depends on the factorisation of the degree of the extension: For different extensions $L/\mathbb{Q}_p$ of the same degree and with induced Hopf Galois structures $H = H_1 \otimes_K H_2$, the matrix determining the relation between $M(H,L)$ and $M(H_1,E) \otimes M(H_2,F)$ is always the same.

Example 5.37. Let us assume that $r = u = 2$. Then, $n = 4$ and $P \in GL_{16}(K)$. Let us compute the corresponding permutation.

$$\left.\begin{cases} \varphi(E^2_{11} \otimes E^2_{11}) = e_1 \\ \varphi(E^2_{11}) \otimes \varphi(E^2_{11}) = e_1 \end{cases}\right\} 1 \mapsto 1$$

$$\left.\begin{cases} \varphi(E^2_{11} \otimes E^2_{21}) = e_2 \\ \varphi(E^2_{11}) \otimes \varphi(E^2_{21}) = e_2 \end{cases}\right\} 2 \mapsto 2$$

$$\left.\begin{cases} \varphi(E^2_{11} \otimes E^2_{12}) = e_5 \\ \varphi(E^2_{11}) \otimes \varphi(E^2_{12}) = e_3 \end{cases}\right\} 5 \mapsto 3$$

$$\left.\begin{cases} \varphi(E^2_{11} \otimes E^2_{22}) = e_6 \\ \varphi(E^2_{11}) \otimes \varphi(E^2_{22}) = e_4 \end{cases}\right\} 6 \mapsto 4$$

$$\left.\begin{cases} \varphi(E^2_{21} \otimes E^2_{22}) = e_8 \\ \varphi(E^2_{21}) \otimes \varphi(E^2_{22}) = e_8 \end{cases}\right\} 8 \mapsto 8$$

$$\left.\begin{cases} \varphi(E^2_{12} \otimes E^2_{12}) = e_{13} \\ \varphi(E^2_{12}) \otimes \varphi(E^2_{12}) = e_{11} \end{cases}\right\} 13 \mapsto 11$$

$$\left.\begin{cases} \varphi(E^2_{22} \otimes E^2_{21}) = e_{12} \\ \varphi(E^2_{22}) \otimes \varphi(E^2_{21}) = e_{14} \end{cases}\right\} 12 \mapsto 14$$

$$\left.\begin{cases} \varphi(E^2_{22} \otimes E^2_{12}) = e_{15} \\ \varphi(E^2_{22}) \otimes \varphi(E^2_{12}) = e_{15} \end{cases}\right\} 15 \mapsto 15$$

$$\left.\begin{cases} \varphi(E^2_{21} \otimes E^2_{11}) = e_3 \\ \varphi(E^2_{21}) \otimes \varphi(E^2_{11}) = e_5 \end{cases}\right\} 3 \mapsto 5$$

$$\left.\begin{cases} \varphi(E^2_{12} \otimes E^2_{11}) = e_9 \\ \varphi(E^2_{11}) \otimes \varphi(E^2_{21}) = e_9 \end{cases}\right\} 9 \mapsto 9$$

$$\left.\begin{cases} \varphi(E^2_{22} \otimes E^2_{11}) = e_{11} \\ \varphi(E^2_{22}) \otimes \varphi(E^2_{11}) = e_{13} \end{cases}\right\} 11 \mapsto 13$$

$$\left.\begin{cases} \varphi(E^2_{21} \otimes E^2_{12}) = e_7 \\ \varphi(E^2_{21}) \otimes \varphi(E^2_{12}) = e_7 \end{cases}\right\} 7 \mapsto 7$$

$$\left.\begin{cases} \varphi(E^2_{21} \otimes E^2_{21}) = e_4 \\ \varphi(E^2_{21}) \otimes \varphi(E^2_{21}) = e_6 \end{cases}\right\} 4 \mapsto 6$$

$$\left.\begin{cases} \varphi(E^2_{12} \otimes E^2_{21}) = e_{10} \\ \varphi(E^2_{12}) \otimes \varphi(E^2_{21}) = e_{10} \end{cases}\right\} 10 \mapsto 10$$

$$\left.\begin{cases} \varphi(E^2_{12} \otimes E^2_{22}) = e_{14} \\ \varphi(E^2_{12}) \otimes \varphi(E^2_{22}) = e_{12} \end{cases}\right\} 14 \mapsto 12$$

$$\left.\begin{cases} \varphi(E^2_{22} \otimes E^2_{22}) = e_{16} \\ \varphi(E^2_{22}) \otimes \varphi(E^2_{22}) = e_{16} \end{cases}\right\} 16 \mapsto 16$$

Thus, P corresponds to the permutation

$$(3,5)(4,6)(11,13)(12,14).$$

Let us check it in a specific example. Let $L = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Then $L/\mathbb{Q}$ is Galois with group

$$G = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma,\tau\rangle \cong C_2 \times C_2,$$

where

$$\sigma(\sqrt{2}) = -\sqrt{2},\ \sigma(\sqrt{3}) = \sqrt{3},$$
$$\tau(\sqrt{2}) = \sqrt{2},\ \tau(\sqrt{3}) = -\sqrt{3}.$$

We consider the bases $\{1_G,\sigma,\tau,\sigma\tau\}$ of H_c and $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ of L. Let us call $E = \mathbb{Q}(\sqrt{3})$ and $F = \mathbb{Q}(\sqrt{2})$. We know by Remark 5.33 that

$$G(H_c,L) = \begin{pmatrix} 1 & \sqrt{2} & \sqrt{3} & \sqrt{6} \\ 1 & -\sqrt{2} & \sqrt{3} & -\sqrt{6} \\ 1 & \sqrt{2} & -\sqrt{3} & -\sqrt{6} \\ 1 & -\sqrt{2} & -\sqrt{3} & \sqrt{6} \end{pmatrix}.$$

On the other hand, the matrices of the action of $E/\mathbb{Q}$ and $F/\mathbb{Q}$ are:

$$M(H_1,E) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & -1 \end{pmatrix} \qquad M(H_2,F) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & -1 \end{pmatrix}$$

Now, we compare the matrix of the action $M(H_c,L)$ with the Kronecker product $M(H_1,E)\otimes M(H_2,F)$:

$$M(H_c,L) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 1 \end{pmatrix} \qquad M(H_1,E)\otimes M(H_2,F) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

It is immediate to check that the permutations of rows $(3,5)(4,6)(11,13)(12,14)$ carries the left side matrix to the right side one.

5.3.2 Induced bases

Once we have found a relation between $M(H,L)$ and $M(H_1,E)\otimes M(H_2,F)$, we may apply the reduction method simultaneously in order to find a relation between $\mathfrak{A}_H$, $\mathfrak{A}_{H_1}$ and $\mathfrak{A}_{H_2}$. Indeed, we will see how the reduction method applied to this equality yields that $\mathfrak{A}_H=\mathfrak{A}_{H_1}\otimes_{\mathcal{O}_K}\mathfrak{A}_{H_2}$. But before, we need to take into account that the reduction method requires the basis fixed at L to be integral, and Theorem 5.34 holds for the basis of L which is product of previously fixed bases of B_1 and B_2.

To sort out this problem, we can in fact work with the hypothesis that E/K and F/K are arithmetically disjoint, so that the product basis is actually an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. However, this does not mean a significant improvement. If, for instance, L/K is an extension of p-adic fields, then the discriminants of E/K and F/K being coprime is equivalent to E/K or F/K being unramified. This brings to light the fact that the arithmetic disjointness is a very restrictive condition: unramified extensions of p-adic fields are not common.

Example 5.38. Let us consider the biquadratic extension in Example 5.37. Since $2,3\not\equiv 1\,(\mathrm{mod}\,4)$, $\mathcal{O}_E=\mathbb{Z}[\sqrt{2}]$ and $\mathcal{O}_F=\mathbb{Z}[\sqrt{3}]$. Then, $\mathcal{O}_E\otimes_{\mathbb{Z}}\mathcal{O}_F=\mathbb{Z}[\sqrt{2},\sqrt{3}]$. On the other hand, by Proposition 3.14, L has an integral basis

$$\left\{1,\sqrt{2},\sqrt{3},\frac{\sqrt{2}+\sqrt{6}}{2}\right\}.$$

Thus, $\frac{\sqrt{2}+\sqrt{6}}{2}\in\mathcal{O}_L$ and $\frac{\sqrt{2}+\sqrt{6}}{2}\notin\mathcal{O}_E\otimes_{\mathbb{Z}}\mathcal{O}_F$, whence $\mathcal{O}_L\neq\mathcal{O}_E\otimes_{\mathbb{Z}}\mathcal{O}_F$.

Example 5.39. Let E be the separable degree 3 extension of $\mathbb{Q}_3$ generated by a root α of the polynomial $f(x)=x^3+3$. Its Galois closure is $L=EF$, where $F=\mathbb{Q}_3(z)$, for $z=\sqrt{-3}$, is the unique quadratic subextension of $L/\mathbb{Q}_3$. We know by the previous chapter that $B_1=\{1,\alpha,\alpha^2\}$ is $\mathcal{O}_K$-basis of $\mathcal{O}_E$ and $B_2=\{1,z\}$ is $\mathcal{O}_K$-basis of $\mathcal{O}_F$. Nevertheless, $B=\{1,z,\alpha,\alpha z,\alpha^2,\alpha^2 z\}$ is not $\mathcal{O}_K$-basis of $\mathcal{O}_L$. For example, $\gamma=\frac{z}{\alpha}\in L$ is a root of x^6+3, so it lies in $\mathcal{O}_L$ (in fact it is a uniformising parameter), and it clearly cannot be written as an $\mathcal{O}_K$-linear combination of elements of B.

Actually, we can work without difficulty in a slightly more general context. When we apply the reduction method to the Hopf Galois structures H, H_1 and H_2, all we need to prove a relation between their associated orders is that the matrices $M(H,L)$ and $M(H_1,E)\otimes M(H_2,F)$ are similar enough. This leads to the following definition.

Definition 5.40. *Let us fix bases of H_1 and H_2 and let W be their product basis, which is a basis of H. We will say that a K-basis B of L is* ***induced*** *with respect to W if there is a unimodular matrix $P\in\mathrm{GL}_{n^2}(\mathcal{O}_K)$ such that*

$$PM(H_W,L_B)=M(H_1,E)\otimes M(H_2,F).$$

By Theorem 5.34, the product of bases of E and F is always an induced basis. The integral basis of L in Example 5.37 is not still an induced basis. In Chapter 6, we will see that the basis of the powers of γ in Example 5.39 is an integral induced basis.

5.3.3 Determination of the induced associated order

This section is devoted to prove the following result.

Theorem 5.41. *Assume that L has some integral induced basis with respect to W. Then,*

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

In particular, we have:

Corollary 5.42. *If E/K and F/K are arithmetically disjoint, then*

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

We start the proof of Theorem 5.41.

Proposition 5.43. *Let B be an integral induced basis of L with respect to W. Then, the matrices $M(H,L)$ and $M(H_1,E) \otimes M(H_2,F)$ have the same reduced matrices.*

Proof. Let $D \in \mathcal{M}_n(K)$. Then D is a reduced matrix of $M(H,L)$ if and only if there is $U \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ unimodular such that

$$UM(H,L) = \begin{pmatrix} D \\ O \end{pmatrix}.$$

Likewise, D is a reduced matrix of $M(H_1,E) \otimes M(H_2,F)$ if and only if there is a unimodular matrix $U' \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ such that

$$U'M(H_1,E) \otimes M(H_2,F) = \begin{pmatrix} D \\ O \end{pmatrix}.$$

Since the basis B is induced, there is a unimodular matrix $P \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ such that $PM(H,L) = M(H_1,E) \otimes M(H_2,F)$. Now, given a matrix $U \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$, one has

$$UM(H,L) = UP^{-1}PM(H,L) = UP^{-1}M(H_1,E) \otimes M(H_2,F),$$

and U is unimodular if and only if UP^{-1} is. Hence, D is a reduced matrix of $M(H,L)$ if and only if it is a reduced matrix of $M(H_1,E) \otimes M(H_2,F)$. □

Corollary 5.44. *If D_1 (resp. D_2) is a reduced matrix of $M(H_1,E)$ (resp. $M(H_2,F)$), then $D_1 \otimes D_2$ is a reduced matrix of $M(H,L)$.*

Proof. Let $U_1 \in \mathrm{GL}_{r^2}(\mathcal{O}_K)$ and $U_2 \in \mathrm{GL}_{u^2}(\mathcal{O}_K)$ such that

$$U_1M(H_1,E) = \begin{pmatrix} D_1 \\ O \end{pmatrix}, \qquad U_2M(H_2,F) = \begin{pmatrix} D_2 \\ O \end{pmatrix}.$$

The Kronecker product of these two matrices is

$$U_1 \otimes U_2 M(H_1,E) \otimes M(H_2,F) = \begin{pmatrix} D_1 \otimes D_2 \\ O \end{pmatrix},$$

with $U_1 \otimes U_2 \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ unimodular. Then, $D_1 \otimes D_2$ is a reduced matrix of $M(H_1,E) \otimes M(H_2,F)$. By Proposition 5.43, it is also a reduced matrix of $M(H,L)$. □

Then, Theorem 5.41 is an immediate consequence of the following:

Corollary 5.45. *For $i \in \{1,2\}$, let V_i be an $\mathcal{O}_K$-basis of $\mathfrak{A}_{H_i}$ obtained by using the reduction method, and let*

$$V := V_1V_2 = \{vw \mid v \in V_1,\, w \in V_2\}.$$

Then, V is an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

Proof. Let D_1 (resp. D_2) be a reduced matrix of $M(H_1,E)$ (resp. $M(H_2,F)$). By Corollary 5.44, $D_1 \otimes D_2$ is a reduced matrix of $M(H,L)$. By Theorem 2.25, the columns of $(D_1 \otimes D_2)^{-1}$ as vector coordinates with respect to W form an $\mathcal{O}_K$-basis V' of $\mathfrak{A}_H$. Now, it is easy to check that $(D_1 \otimes D_2)^{-1} = D_1^{-1} \otimes D_2^{-1}$. Hence, by definition of Kronecker product, the columns of this matrix are the products of the columns of D_1^{-1} and D_2^{-1}. We conclude that $V' = V$, so V is an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$. □

In summary, reducing $M(H_1,E)$ by means of a unimodular matrix U_1 and reducing $M(H_2,F)$ by means of a unimodular matrix U_2 is the same as reducing $M(H,L)$ by using $U = U_1 \otimes U_2$. This solves the problem of finding a basis of the associated order in an induced Hopf Galois structure (whenever there is an induced basis) from a theoretical point of view.

In practice, it is more convenient to work with matrices with integer coefficients. This is always possible because in order to reduce the matrix of the action it is equivalent to reduce its primitive part, due to the following result.

Corollary 5.46. *Call $d_1 = \mathrm{cont}(M(H_1,E))$, $d_2 = \mathrm{cont}(M(H_2,F))$ and $d = \mathrm{cont}(M(H,L))$. Then, there is a unit $u \in \mathcal{O}_K^*$ such that $d = d_1d_2u$.*

Proof. Let D be a reduced matrix of $M(H,L)$, so there exists a unimodular matrix $U \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ such that $UM(H,L) = \begin{pmatrix} D \\ O \end{pmatrix}$. By the proof of Proposition 5.43,

$$UP^{-1}M(H_1,E) \otimes M(H_2,F) = \begin{pmatrix} D \\ O \end{pmatrix}.$$

Since UP^{-1} is unimodular,

$$\mathrm{cont}(M(H_1,E) \otimes M(H_2,F)) = \mathrm{cont}(UP^{-1}M(H_1,E) \otimes M(H_2,F)) = \mathrm{cont}(D).$$

Now, the content is unique up to multiplication by a unit, so there is some $u \in \mathcal{O}_K^*$ such that $d = d_1d_2u$. □

5.3.4 Induced freeness

In this part we study the freeness of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module when $H = H_1 \otimes_K H_2$ is an induced Hopf Galois structure. To obtain a direct relation, we need the arithmetic disjointness.

Theorem 5.47. *Let us assume that E/K and F/K are arithmetically disjoint. If $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free and $\mathcal{O}_F$ is $\mathfrak{A}_{H_2}$-free, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. Moreover, if γ is a $\mathfrak{A}_{H_1}$-free generator of $\mathcal{O}_E$ and δ is a $\mathfrak{A}_{H_2}$-free generator of $\mathcal{O}_F$, then $\gamma\delta$ is a $\mathfrak{A}_H$-free generator of $\mathcal{O}_L$.*

Proof. Let $\{v_i\}_{i=1}^r$ be an $\mathcal{O}_K$-basis of $\mathfrak{A}_{H_1}$ and let $\{\mu_j\}_{j=1}^u$ be an $\mathcal{O}_K$-basis of $\mathfrak{A}_{H_2}$. Then, $\{v_i \cdot \gamma\}_{i=1}^r$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_E$ and $\{\mu_j \cdot \delta\}_{j=1}^u$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_F$. Since $\mathcal{O}_L =$

$\mathcal{O}_E \otimes_{\mathcal{O}_K} \mathcal{O}_F$, the product of these bases is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. But that basis is formed by the elements

$$(v_i \cdot \gamma)(\mu_j \cdot \delta) = (v_i\mu_j) \cdot (\gamma\delta),\, 1 \leq i \leq r,\, 0 \leq j \leq u.$$

Since $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$, this amounts to say that $\gamma\delta$ is a $\mathfrak{A}_H$-free generator of $\mathcal{O}_L$. □

5.3.5 Freeness after tensoring by $\mathcal{O}_F$

We finally compute the associated order of $\mathcal{O}_L$ in $H^{(1)} := H_1 \otimes_K F$ and discuss the freeness of $\mathcal{O}_L$ as $\mathfrak{A}_{H^{(1)}}$-module. Note that this is actually a Hopf Galois structure on L/F because H_1 is a Hopf Galois structure on E/K and F is K-flat. Moreover, the action of $H^{(1)}$ on L is obtained by extending F-linearly the one of H_1 on E.

We study the relation between $\mathfrak{A}_{H_1}$ and $\mathfrak{A}_{H^{(1)}}$, as well as the $\mathfrak{A}_{H_1}$-freeness of $\mathcal{O}_E$ and the $\mathfrak{A}_{H^{(1)}}$-freeness of $\mathcal{O}_L$. In order to do this, we need a suitable description of elements of $\mathcal{O}_L$. For this reason, we make again the hypothesis that E/K and F/K are arithmetically disjoint, which implies that $\mathcal{O}_L = \mathcal{O}_E \otimes_{\mathcal{O}_K} \mathcal{O}_F$.

Let $\{\alpha_i\}_{i=1}^r$ be an $\mathcal{O}_K$-basis of $\mathcal{O}_E$ and let $\{z_j\}_{j=1}^u$ be an $\mathcal{O}_K$-basis of $\mathcal{O}_F$. Since $\mathcal{O}_L = \mathcal{O}_E \otimes_{\mathcal{O}_K} \mathcal{O}_F$, $\{\alpha_i z_j\}_{i,j}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Proposition 5.48. *If E/K and F/K are arithmetically disjoint, then $\mathfrak{A}_{H^{(1)}} = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathcal{O}_F$.*

Proof. First, we prove that $\mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathcal{O}_F \subset \mathfrak{A}_{H^{(1)}}$. It is clearly contained in $H_1 \otimes_{\mathcal{O}_K} F = H_1 \otimes_K F = H^{(1)}$. On the other hand, it acts $\mathcal{O}_K$-linearly on $\mathcal{O}_L$ componentwise since $\mathcal{O}_L = \mathcal{O}_E \otimes_{\mathcal{O}_K} \mathcal{O}_F$. This proves the claim.

For the reverse inclusion, let $h \in \mathfrak{A}_{H^{(1)}}$. Trivially, $h \in H^{(1)} = H_1 \otimes_K F$. Since $\{z_j\}_{j=1}^u$ is a K-basis of F and H_1 is K-flat, it is also an H_1-basis of $H^{(1)}$. Then,

$$h = \sum_{j=1}^u h^{(j)} z_j,\, h^{(j)} \in H_1.$$

The result will follow from the fact that $h^{(j)} \in \mathfrak{A}_{H_1}$ for all $1 \leq j \leq u$. In order to prove this, we may check that $h^{(j)} \cdot \gamma \in \mathcal{O}_E$ for all $\gamma \in \mathcal{O}_E$. Take any such $\gamma \in \mathcal{O}_E$. In particular $\gamma \in \mathcal{O}_L$, and since $h \in \mathfrak{A}_{H^{(1)}}$, we have that $h \cdot_L \gamma \in \mathcal{O}_L$. But

$$h \cdot_L \gamma = \left(\sum_{j=1}^u h^{(j)} z_j\right) \cdot_L \gamma = \sum_{j=1}^u (h^{(j)} \cdot_E \gamma) z_j \in \mathcal{O}_L.$$

Now, $\{z_j\}_{j=1}^u$ is an $\mathcal{O}_E$-basis of $\mathcal{O}_L$ because $\mathcal{O}_E$ is $\mathcal{O}_K$-flat. Hence, the previous expression yields that $h^{(j)} \cdot_E \gamma \in \mathcal{O}_E$ for all $1 \leq j \leq u$. □

With this result, we have determined how the associated order changes when we tensor with an arithmetically disjoint extension. It is, together with Corollary 5.42, the direct generalization of the first part in Proposition 5.11. Now, we move to the question of the freeness of $\mathcal{O}_L$ as $\mathfrak{A}_{H^{(1)}}$-module. We have:

Corollary 5.49. *Assume that E/K and F/K are arithmetically disjoint. If $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free, then $\mathcal{O}_L$ is $\mathfrak{A}_{H^{(1)}}$-free.*

Proof. Since $\mathcal{O}_F$ is $\mathcal{O}_K$-flat, $\mathcal{O}_E \otimes_{\mathcal{O}_K} \mathcal{O}_F = \mathcal{O}_L$ is $\mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathcal{O}_F$-free. By the previous result, $\mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathcal{O}_F = \mathfrak{A}_{H^{(1)}}$ and the claim follows. □

This result and Theorem 5.47 generalize the second part of Proposition 5.11.

Chapter 6

Dihedral degree $2p$ extensions of $\mathbb{Q}_p$

Let p be an odd prime number. The standard setup in this chapter is a Galois extension $L/\mathbb{Q}_p$ of p-adic fields (i.e, a finite field extension of $\mathbb{Q}_p$) whose Galois group G is isomorphic to the dihedral group of order $2p$, for a prime $p \geq 3$. We establish the following presentation of G henceforth:

$$G = \langle \sigma, \tau \,|\, \sigma^p = \tau^2 = 1, \, \tau\sigma = \sigma^{p-1}\tau \rangle.$$

We carry out a detailed study on the arithmetic setting and the Hopf Galois module structure of such an extension.

Regarding the problem of determining Hopf Galois structures, we will take a dihedral degree $2p$ extension L/K of arbitrary fields, as restrictions over the fields themselves are not required. This problem was solved by Byott in his paper [Byo04] in the more general case of extensions of degree pq, for p and q different primes such that q divides $p-1$. We recover dihedral degree $2p$ extensions by considering the ones with $q=2$ and non-abelian Galois group. It turns out that L/K has 2 Hopf Galois structures of type D_p, the classical and the canonical non-classical (which define different Hopf Galois structures because D_p is not abelian), and p Hopf Galois structures of type C_{2p}. We will see that the last ones are just the induced Hopf Galois structures of L/K, which we computed in Examples 5.20 and 5.26.

Going back to the case of a dihedral degree $2p$ extension of $\mathbb{Q}_p$, the Hopf Galois module structure is almost completely described for the dihedral Hopf Galois structures thank to results of Truman and Johnston, and completed by using the reduction method. For the cyclic ones, even though we have not solved the problem in its more general situation, we have obtained complete answers for the cases $p=3$ and $p=5$.

Furthermore, we consider the extension L/F, where $F/\mathbb{Q}_p$ is the unique quadratic subextension of $L/\mathbb{Q}_p$, which consequently is a cyclic degree p extension. These extensions have a unique Hopf Galois structure and their local setting has been deeply studied. Descriptions of the associated order $\mathfrak{A}_{L/F}$ and the freeness over $\mathfrak{A}_{L/F}$ are available (see for example [Fer74]). For $p=3$, we shall compute the associated order using the reduction method.

6.1 Description of the Hopf Galois structures

Let L/K be a dihedral degree $2p$ extension of arbitrary fields, for a prime $p \geq 3$ and call G its Galois group. By the Greither-Pareigis theorem, Hopf Galois structures of L/K are in one-to-one correspondence with regular subgroups of $\mathrm{Perm}(G)$ normalized by $\lambda(G)$, where $\lambda\colon G \longrightarrow \mathrm{Perm}(G)$ is the left regular representation of G. By [Byo04, Theorem 6.2], the permutation subgroups giving Hopf Galois structures of L/K are the following:

- **Dihedral type**: The regular subgroup N is isomorphic to D_p. There are two such Hopf Galois structures: the classical one, corresponding to $N_c = \rho(G)$, and the canonical non-classical one, corresponding to $N_\lambda = \lambda(G)$.
- **Cyclic type**: The regular subgroup N is isomorphic to C_{2p}. There are p such Hopf Galois structures, corresponding to $N^{(d)} = \langle \mu, \eta_d\rangle$ for $0 \leq d \leq p-1$, where:
$$\begin{array}{rccl} \mu\colon & \sigma^k\tau^l & \longmapsto & \sigma^{k+1}\tau^l \\ \eta_d\colon & \sigma^k\tau^l & \longmapsto & \sigma^{k+(-1)^{l+1}d}\tau^{l+1} \end{array}$$

Let us focus on the Hopf Galois structures of cyclic type. Note that in Example 5.26, all the permutation subgroups N are cyclic, so induced Hopf Galois structures are of cyclic type. Since there are a total of p, this gives that the cyclic Hopf Galois structures are the induced ones. Then, each $N^{(d)}$ is actually induced by permutation subgroups of $\mathrm{Perm}(J)$ and $\mathrm{Perm}(G')$ as in the Induction Theorem 5.21, for some decomposition $G = J \rtimes G'$ of the Galois group G as a semidirect product. Let us identify those subgroups.

First, we study the generators μ and η_d. After the remark that $\mu = \lambda(\sigma)$, it is immediate that the element μ has order p. As for η_d, we claim that it coincides with $\rho(\sigma^d\tau)$, where $\rho\colon G \longrightarrow \mathrm{Perm}(G)$ is the right translation map of G. Indeed, we have

$$\rho(\sigma^d\tau)(\sigma^k\tau^l) = \sigma^k\tau^l\sigma^{-d}\tau. \tag{6.1}$$

Since $\tau\sigma^{-d} = \sigma^d\tau$ and $\tau\sigma^d = \sigma^{-d}\tau$ by definition of G, one obtains by induction that $\tau^l\sigma^{-d} = \sigma^{(-1)^{l+1}d}\tau^l$. Carrying this to (6.1), we obtain

$$\rho(\sigma^d\tau)(\sigma^k\tau^l) = \sigma^{k+(-1)^{l+1}d}\tau^{l+1} = \eta_d(\sigma^k\tau^l),$$

which proves the claim. Consequently, η_d is of order 2.

Theorem 6.1. *Fix $0 \leq d \leq p-1$ and define $J = \langle\sigma\rangle$ and $G' = \langle\sigma^d\tau\rangle$, which gives a decomposition of G as semidirect product. Then,*

$$N^{(d)} = \iota(N_1 \times N_2),$$

where $N_1 = \lambda^J(J)$ and $N_2 = \lambda^{G'}(G')$, and $\lambda^{G'}\colon G' \longrightarrow \mathrm{Perm}(G')$ (resp. $\lambda^J\colon J \longrightarrow \mathrm{Perm}(J)$) is the left regular representation of G' (resp. J).

Proof. We have
$$\mu = \lambda(\sigma) = \iota\circ\chi(\sigma) = \iota(\lambda^J(\sigma), 1).$$

Then N_1 is an order p subgroup of $\mathrm{Perm}(J)$, and it is clearly regular and normalized by $\lambda_c(G)$. On the other hand, we know that $\eta_d = \rho(\sigma^d\tau)$. Since $\eta_i(1) = \sigma^d\tau$ and $\eta_i(\sigma^d\tau) = 1$, this permutation restricts to G', and that restriction coincides with

$\lambda^{G'}(\sigma^d\tau)$. But this element is the generator of N_2, which is a regular order 2 subgroup of $\mathrm{Perm}(G')$ normalized by itself.

Now, $\mu\eta_i$ generates N and verifies

$$\mu\eta_i = \lambda(\sigma)\rho(\sigma^i\tau) = \iota(\lambda^J(\sigma), \lambda^{G'}(\sigma^i\tau)) \in \iota(N_1 \times N_2).$$

In order to check the last equality, we remark that $\lambda(\sigma)\rho(\sigma^i\tau)(\sigma^k\tau^l) = \sigma^{k+1+(-1)^{l+1}i}\tau^{l+1}$ and compute

$$\begin{aligned}
\iota(\lambda^J(\sigma), \lambda^{G'}(\sigma^i\tau))(\sigma^k) &= \sigma^{k+1}\sigma^i\tau \\
&= \lambda(\sigma)\sigma^k\sigma^i\tau \\
&= \lambda(\sigma)\rho(\sigma^i\tau)(\sigma^k), \\
\iota(\lambda^J(\sigma), \lambda^{G'}(\sigma^i\tau))(\sigma^k\tau) &= \sigma^{k+1+i}(\sigma^i\tau)^2 \\
&= \sigma^{k+1+i}\tau \\
&= \lambda(\sigma)\rho(\sigma^i\tau)(\sigma^k\tau).
\end{aligned}$$

Then $N \leq \iota(N_1 \times N_2)$, and since their orders are equal, they coincide. □

6.1.1 The Hopf algebras involved

For each of the Hopf Galois structures of L/K, let us describe the corresponding Hopf algebra.

For the classical Galois structure, given by $\rho(G)$, it is well known that the corresponding Hopf algebra is the K-group algebra $H_c = K[\rho(G)]$, which we can identify (as Hopf algebras) with $K[G]$, so the elements of G form a K-basis. Regarding the canonical non-classical structure, by the Greither-Pareigis theorem the Hopf algebra is given by $H_\lambda = K[\lambda(G)]^{\lambda(G)}$. Let us call $\mu = \lambda(\sigma)$ and $\eta = \lambda(\tau)$. By [Koc+19, Section 6], it holds that

$$H_\lambda = \{a_0 + \sum_{i=1}^{\frac{p-1}{2}}(a_i\mu^i + \tau(a_i)\mu^{-i}) + b_0\eta + \sum_{i=1}^{p-1}\sigma^{i\frac{p-1}{2}}(b_0)\eta^{-i} \,|\, a_0 \in K,\, a_i \in F,\, b_0 \in E\},$$

where $E = L^{\langle\tau\rangle}$ and $F = L^{\langle\sigma\rangle}$.

Now, we determine the Hopf algebras of the cyclic Hopf Galois structures, which is the same as determining those of the induced Hopf Galois structures. Let H be such a Hopf Galois structure. By Corollary 5.31, $H = H_1 \otimes H_2$, where H_1 is a Hopf Galois structure of E/K, H_2 is a Hopf Galois structure of F/K, and $E = L^{G'}$, $F = L^J$ for some decomposition $G = J \rtimes G'$ of the Galois group as a semidirect product.

We determine, then, the Hopf Galois structures of these subextensions. For E/K it is just what we did in Chapter 3: By Theorem 4.1, $H_1 = K[z(\mu - \mu^{-1})]$. On the other hand, F/K is a quadratic extension, so the classical Galois structure is its unique Hopf Galois structure. Its Hopf algebra $K[G/J]$ is isomorphic to $K[\eta_d]$, where d corresponds to the choice of the generator $\sigma^d\tau$ of G' in the decomposition $G = J \rtimes G'$.

Once we have described the Hopf Galois structures of H_1 and H_2, we obtain the explicit expression of $H = H_1 \otimes H_2$.

Corollary 6.2. *The cyclic Hopf Galois structures of L/K are those with Hopf algebras of the form*

$$H_d = K[z(\mu - \mu^{-1}), \eta_d],$$

where $z \in F - K$ is such that $z^2 \in K$, $\mu = \lambda(\sigma)$, $\eta_d = \rho(\sigma^d\tau)$ and $0 \leq d \leq p-1$.

6.2 The arithmetic of the extension

For this section and for the remainder of the chapter, we take a dihedral degree $2p$ extension $L/\mathbb{Q}_p$ of p-adic fields.

6.2.1 Integral bases

First, we compute a $\mathbb{Q}_p$-integral basis of L, as this is needed in order to apply the reduction method. Since L is the splitting field of a p-Eisenstein polynomial, all its degree p subextensions $E/\mathbb{Q}_p$ are totally ramified. Equivalently, $L/\mathbb{Q}_p$ is totally ramified if and only if so is its unique quadratic subextension $F/\mathbb{Q}_p$. We may try to build an integral basis of L from integral bases of E and F. Let α be a root of the Amano polynomial defining $E/\mathbb{Q}_p$ and let $z = \sqrt{d} \in \mathcal{O}_F$ with $d \in \mathbb{Z}_p - \mathbb{Z}_p^2$ and $v_p(d) \leq 1$. Then, $\{1, \alpha, \ldots, \alpha^{p-1}\}$ (resp. $\{1, z\}$) is an integral basis of E (resp. F).

The easiest case is when $F/\mathbb{Q}_p$ is unramified. If so, we have that $E/\mathbb{Q}_p$ and $F/\mathbb{Q}_p$ are arithmetically disjoint, so by the definition, $\mathcal{O}_L = \mathcal{O}_E \otimes_{\mathbb{Z}_p} \mathcal{O}_F$. Hence, the product of integral bases of E and F is an integral basis of L. For the ones above, we have

$$B = \{1, z, \alpha, \alpha z, \ldots, \alpha^{p-1}, \alpha^{p-1}z\}.$$

Now, let us assume that $F/\mathbb{Q}_p$ has ramification, so $L/\mathbb{Q}_p$ is totally ramified. Then the basis B is still a basis of L but it is not integral. In this case we use the following result:

Proposition 6.3. *If $L/\mathbb{Q}_p$ is a totally ramified dihedral degree $2p$ extension of p-adic fields, then*

$$\gamma = \frac{z}{\alpha^{\frac{p-1}{2}}}$$

is an uniformising parameter of $\mathcal{O}_L$, where α and z are as above. Consequently,

$$B' = \{1, \gamma, \ldots, \gamma^{2p-1}\}$$

is an integral basis of L.

Proof. It is enough to check that γ has L-valuation 1. Since $v_F(z) = 1$ and $e(L/F) = p$ (as it has ramification), $v_L(z) = p$. On the other hand, since $F/\mathbb{Q}_p$ has ramification index 2 and is linearly disjoint with $E/\mathbb{Q}_p$, L/E also has ramification index 2. Then, $v_E(\alpha) = 1$ implies that $v_L(\alpha) = 2$. Finally,

$$v_L(\gamma) = p - 2\frac{p-1}{2} = 1.$$

□

We summarize the results obtained in this section:

Corollary 6.4. *Let $L/\mathbb{Q}_p$ be a dihedral degree $2p$ extension of p-adic fields. Let α be a root of the Amano polynomial of which L is the splitting field over $\mathbb{Q}_p$ and let z be an uniformising parameter of the unique quadratic subextension of $L/\mathbb{Q}_p$. An integral basis of L is given as follows:*

1. *If $L/\mathbb{Q}_p$ is not totally ramified, $B = \{1, z, \alpha, \alpha z, \dots, \alpha^{p-1}, \alpha^{p-1}z\}$.*
2. *If $L/\mathbb{Q}_p$ is totally ramified, $B' = \{1, \gamma, \dots, \gamma^{2p-1}\}$.*

6.2.2 Discriminant and ramification

We determine the discriminant and the chain of ramification groups of $L/\mathbb{Q}_p$. We will first compute the discriminant of a degree p subextension $E/\mathbb{Q}_p$. By Theorem 4.5, E is generated by the root of one of the Amano polynomials listed there. Let f be the defining Amano polynomial and α one of its roots. Since the powers of α up to $p-1$ form an integral basis, $\operatorname{disc}(E/\mathbb{Q}_p) = \operatorname{disc}(f)$. We then compute the discriminant of the Amano polynomials by using the Ore condition.

Theorem 6.5 (Ore condition). *Given $j_0 \in$, there exist totally ramified extensions $E/\mathbb{Q}_p$ of degree p and with discriminant exponent $c(E/\mathbb{Q}_p) = p + j_0 - 1$ if and only if $1 \leq j_0 \leq p$. In that case, if $f(x) = x^p + \sum_{i=0}^{p-1} f_i x^i \in \mathbb{Z}_p[x]$ is an Eisenstein polynomial, we have:*

1. *For $j_0 = p$, $v_p(\operatorname{disc}(f)) = 2p - 1$ if*
$$v_p(f_i) \geq 2 \textit{ for } 1 \leq i \leq p-1.$$
2. *For $0 < j_0 < p$, $v_p(\operatorname{disc}(f)) = p + j_0 - 1$ if*
$$v_p(f_i) \geq 2 \textit{ for } 1 \leq i < p-1,\ i \neq j_0, \textit{ and } v_p(f_{j_0}) = 1.$$

Proof. See [Ore24] or [PR01, Proposition 3.1 and Lemma 5.1]. □

We apply the lemma to our situation. We begin with the polynomials $x^3 + 3a$ with $a \in \{1, 4, 7\}$. If we take $j_0 = 3$, what the first part of Theorem 6.5 says is that there are degree 3 extensions of $\mathbb{Q}_p$ with discriminant exponent 5. Since $v_3(f_2) = v_3(f_1) = \infty > 2$, we can then apply the first statement of the second part in the theorem to obtain $v_3(\operatorname{disc}(f)) = 5$.

We move on to the case of the polynomials $x^p + 2px^{\frac{p-1}{2}} + p$, $x^p + p(p-2)x^{\frac{p-1}{2}} + p$, for which we take $j_0 = \frac{p-1}{2}$. Since

$$v_p(f_{p-1}) = \cdots = v_p(f_{\frac{p+1}{2}}) = v_p(f_{\frac{p-3}{2}}) = \cdots = v_p(f_1) = \infty > 2$$

if $p > 3$ and $v_p(f_{\frac{p-1}{2}}) = 1$, $v_p(\operatorname{disc}(f)) = p + \frac{p-1}{2} - 1 = \frac{3(p-1)}{2}$.

Finally, for the polynomial $x^p + px^{p-1} + p$, we take $j_0 = p-1$, for which $v_p(f_1) = ... = v_p(f_{p-2}) = \infty > 2$ and $v_p(f_{p-1}) = 1$, so $v_p(\operatorname{disc}(f)) = p + j_0 - 1 = 2(p-1)$.

We represent in the following table the information above together with the last line of Theorem 4.5 concerning the inertia group.

	Polynomial	G_0	$c(E/\mathbb{Q}_p)$
$p=3$	$x^3+3a \quad (a \in \{1,4,7\})$	D_3	5
$p \geq 3$	$x^p+(p-2)px^{\frac{p-1}{2}}+p$	D_p	$\frac{3(p-1)}{2}$
	$x^p+2px^{\frac{p-1}{2}}+p$	D_p	$\frac{3(p-1)}{2}$
	$x^p+px^{p-1}+p$	C_p	$2(p-1)$

We can obtain the discriminant of $L/\mathbb{Q}_p$ by using the relative discriminant formula

$$\mathrm{disc}(L/\mathbb{Q}_p) = N_{E/\mathbb{Q}_p}(\mathrm{disc}(L/E))\mathrm{disc}(E/\mathbb{Q}_p)^2.$$

Since the ramification index is multiplicative in towers, L/E is unramified if and only if so is $F/\mathbb{Q}_p$. For the polynomial $x^p+px^{p-1}+p$ with $p \geq 3$ the inertia group is $G_0 \cong C_p$, so the extension L/E is indeed unramified, and then $\mathrm{disc}(L/E) \in \mathcal{O}_E^*$. Applying the formula above, $\mathrm{disc}(L/\mathbb{Q}_p) = \mathrm{disc}(E/\mathbb{Q}_p)^2$. Otherwise, since L/E is a quadratic extension of p-adic fields, $v_E(\mathrm{disc}(L/E)) = 1$, and then $\mathrm{disc}(L/\mathbb{Q}_p) = p\mathrm{disc}(E/\mathbb{Q}_p)^2$. Then, one obtains the following table.

	Polynomial	G_0	$c(E/\mathbb{Q}_p)$	$c(L/\mathbb{Q}_p)$
$p=3$	$x^3+3a \quad (a \in \{1,4,7\})$	D_3	5	11
$p \geq 3$	$x^p+(p-2)px^{\frac{p-1}{2}}+p$	D_p	$\frac{3(p-1)}{2}$	$3p-2$
	$x^p+2px^{\frac{p-1}{2}}+p$	D_p	$\frac{3(p-1)}{2}$	$3p-2$
	$x^p+px^{p-1}+p$	C_p	$2(p-1)$	$4(p-1)$

Finally, we compute the chain of ramification groups by means of the formula of Proposition 1.24

$$c(L/\mathbb{Q}_p) = f(L/\mathbb{Q}_p)\sum_{i=0}^{\infty}(|G_i|-1).$$

If $p=3$ and the polynomial is one of x^3+3a, $a \in \{1,4,7\}$, then $f(L/\mathbb{Q}_p) = 1$ and $v_3(\mathrm{disc}(L/\mathbb{Q}_3)) = 11$, and replacing in the previous formula, $\sum_{i=0}^{\infty}(|G_i|-1) = 11$. Since $|G_0| = 6$, it must be $|G_1| = |G_2| = |G_3| = 2$. Then, the chain of ramification groups is

$$D_3 \supseteq C_3 \supseteq C_3 \supseteq C_3 \supseteq \{1\}.$$

If the polynomial is one of $x^p+apx^{\frac{p-1}{2}}+p$, $a \in \{2, p-2\}$, we have again $f(L/\mathbb{Q}_p) = 1$, and $\sum_{i=0}^{\infty}(|G_i|-1) = 3p-2$. We know that $|G_0| = 2p$, so it must be $|G_1| = p$ and $|G_i| = 1$ for all $i > 1$. Then, the chain of ramification groups is

$$D_p \supseteq C_p \supseteq \{1\}.$$

For the polynomial $x^p+px^{p-1}+p$, $f(L/\mathbb{Q}_p) = 2$ and $v_p(\mathrm{disc}(L/\mathbb{Q}_p)) = 4(p-1)$, so $\sum_{i=0}^{\infty}(|G_i|-1) = 2(p-1)$. Since $|G_0| = p$, it must be $|G_1| = p$ and $|G_i| = 1$ for all $i > 1$. Then, the chain of ramification groups is

$$C_p \supseteq C_p \supseteq \{1\}.$$

Finally, the chain of ramification groups of L/F is obtained as the intersection of the one of $L/\mathbb{Q}_p$ with $\mathrm{Gal}(L/F) \cong C_p$. Then, it becomes the same but with inertia C_p (and without changes for the last polynomial). Then, the ramification number $t(L/F)$ is 3 for the polynomials x^3+3a and 1 otherwise. To sum up:

Theorem 6.6. *Let $L/\mathbb{Q}_p$ be an absolute dihedral degree $2p$ extension of p-adic fields. The discriminant and ramification of $L/\mathbb{Q}_p$ is given by the following table:*

	Polynomial	$c(L/\mathbb{Q}_p)$	Ramification groups	$t(L/F)$
$p=3$	$x^3+3a \quad (a \in \{1,4,7\})$	11	$D_3 \supseteq C_3 \supseteq C_3 \supseteq C_3 \supseteq \{1\}$	3
$p \geq 3$	$x^p+(p-2)px^{\frac{p-1}{2}}+p$	$3p-2$	$D_p \supseteq C_p \supseteq \{1\}$	1
	$x^p+2px^{\frac{p-1}{2}}+p$	$3p-2$	$D_p \supseteq C_p \supseteq \{1\}$	1
	$x^p+px^{p-1}+p$	$4(p-1)$	$C_p \supseteq C_p \supseteq \{1\}$	1

It can be observed that the extensions corresponding to the non-radical polynomials are weakly ramified. Then, the classification of dihedral extensions $L/\mathbb{Q}_p$ of degree $2p$ can be presented in a more convenient way:

Corollary 6.7. *Let p be an odd prime number and let $L/\mathbb{Q}_p$ be a dihedral degree $2p$ extension of p-adic fields.*

1. *If $L/\mathbb{Q}_p$ is weakly ramified, then L is the splitting field over $\mathbb{Q}_p$ of one of the polynomials*

$$x^p+2px^{\frac{p-1}{2}}+p, \quad x^p+p(p-2)x^{\frac{p-1}{2}}+p, \quad x^p+px^{p-1}+p.$$

2. *Otherwise, $p=3$ and L is the splitting field over $\mathbb{Q}_3$ of one of the polynomials*

$$x^3+3, \quad x^3+12, \quad x^3+21.$$

6.3 Dihedral Hopf Galois module structure

In this part we consider the problem of determining both the associated order and the freeness over it for the Hopf Galois structures of dihedral type, that is, the classical Galois structure H_c and the canonical non-classical Hopf Galois structure H_λ. The strategy will be completely different depending on whether $L/\mathbb{Q}_p$ is weakly ramified or not.

6.3.1 Weakly ramified cases

If $L/\mathbb{Q}_p$ is weakly ramified, by Corollary 6.7 it is the splitting field of $x^p+2px^{\frac{p-1}{2}}+p$, $x^p+(p-2)px^{\frac{p-1}{2}}+p$ or $x^p+px^{p-1}+p$. To study the classical Galois structure, we can make use of the results of Johnston in [Joh15], while for the canonical non-classical structure, Truman studies its relation with the former in [Tru16].

The associated order

Concerning the classical Galois structure, as $L/\mathbb{Q}_p$ is always wildly ramified (since its degree p subextensions are totally ramified), Johnston's result [Joh15, Theorem 1.2] gives that

$$\mathfrak{A}_{L/\mathbb{Q}_p} = \mathbb{Z}_p[G]\left[\frac{\mathrm{Tr}_{G_0}}{p}\right]$$

and $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_p}$-free.

For the canonical non-classical Hopf Galois structure H_λ, we have:

Theorem 6.8. *Let L/K be a non-abelian Galois extension of fields with Galois group G. If $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free with generator x and $\{h_i\}_{i=1}^n$ is an $\mathcal{O}_K$-basis of $\mathfrak{A}_{L/K}$, then there is an $\mathcal{O}_K$-basis of $\mathfrak{A}_{H_\lambda}$ formed by*

$$\widehat{h_i} = \sum_{g \in G} \left(\sum_{\sigma \in G} \sigma(x_i) g^{-1} \sigma(\widehat{x}) \right) \lambda(g),$$

where $x_i = h_i(x)$ for every i and $\hat{x} \in L$ is such that $\{\sigma(\widehat{x})\}_{\sigma \in G}$ is the dual basis of the normal basis $\{\sigma(x)\}_{\sigma \in G}$ of L.

Proof. The existence of an element $\widehat{x}$ with the aforementioned property is justified by [Tru16, Lemma 3.1]. The proof that $\{\widehat{h_i}\}$ is an $\mathcal{O}_K$-basis of $\mathfrak{A}_{H_\lambda}$ follows from the proof of [Tru16, Proposition 4.1]. □

Since $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_p}$-free, this solves the problem of the description of the associated order.

Module structure over the associated order

Concerning the freeness, we already know that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_p}$-free by Johnston's result. Moreover, he constructs explictly the form of a normal integral basis generator (see [Joh15, Theorem 4.1]). On the other hand, for the canonical non-classical structure, we have:

Theorem 6.9. *Let L/K be a non-abelian Galois extension of fields with Galois group G. Then, $\mathcal{O}_L$ is free as $\mathfrak{A}_{L/K}$-module if and only if so is as $\mathfrak{A}_{H_\lambda}$-module.*

Proof. This the main result of [Tru16, Theorem 1.1]. □

In our case, since $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_p}$-free, Truman's result yields that it is also free over the associated order in the canonical non-classical structure.

6.3.2 The radical cases

Now we assume that $L/\mathbb{Q}_p$ is not weakly ramified, which by Corollary 6.7 implies that $p = 3$ and f is one of the radical Amano polynomials, that is, $f(x) = x^3 + 3a$ with $a \in \{1, 4, 7\}$. To study the associated order and the module structure of $\mathcal{O}_L$, we will use the reduction method. Since the Galois group is still not abelian, we can use Theorems 6.8 and 6.9, so it is enough to study the classical Galois module structure.

In these cases $L/\mathbb{Q}_p$ is totally ramified, so by Proposition 6.3, the powers of $\frac{z}{\alpha}$ up to 5 form a basis of $\mathcal{O}_L$, where α is a root of f and $z = \sqrt{d} \in L$ with $d \in \mathbb{Z}_p - \mathbb{Z}_p^2$. Let $t = \sqrt{a} \in \mathbb{Z}_3^*$. For convenience we will take as integral basis the powers up to 5 of

$$\gamma = t\frac{z}{\alpha}.$$

In order to completely determine this integral basis, we will look for possible values for z. Since the Galois group of $L/\mathbb{Q}_3$ is isomorphic to D_3, then the discriminant of f is not a perfect square, so its square root generates the unique quadratic subextension of $L/\mathbb{Q}_3$. Thus, z can be chosen as any element of L such that $\mathbb{Q}_3(\sqrt{\mathrm{disc}(f)}) = \mathbb{Q}_3(z)$. Now,

$$\mathrm{disc}(f) = -27 \cdot 3^2 \cdot a^2 = -3^5 a^2,$$

and since $v_3(a) = 0$, we may choose $z = \sqrt{-3}$.

On the other hand, we have that $\alpha^3 = -3a$, so $\frac{1}{\alpha} = -\frac{\alpha^2}{3a}$. Thus, we have

$$\gamma^2 = -\frac{3a}{\alpha^2} = \alpha, \quad \gamma^3 = tz, \quad \gamma^4 = \alpha^2, \quad \gamma^5 = t\alpha z.$$

Next, we need to determine the Galois action on the powers of γ. Since all of them are products of α and z, we determine the action on these elements. The action on the latter is much easier: $\sigma(z) = z$ and $\tau(z) = -z$. On the other hand, we may assume that α is the root of f that is fixed by τ (so that the other two are fixed by $\sigma\tau$ and $\sigma^2\tau$). Then, $\tau(\alpha) = \alpha$ by choice and $\sigma(\alpha)$ is a conjugate of α. For τ, this gives that $\tau(\gamma) = -\gamma$. Since f is radical, it may be checked that the conjugates of α are $\zeta_3\alpha$ and $\zeta_3^2\alpha$, where $\zeta_3 = \frac{-1+z}{2}$ is a primitive third root of unity. We can assume without loss of generality that $\sigma(\alpha) = \zeta_3\alpha$ (otherwise we would replace σ by σ^2), and then $\sigma(\gamma) = \zeta_3^2\gamma$. With these assumptions, we obtain the Gram matrix:

$$G(H,L) = \begin{pmatrix} 1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 \\ 1 & -\frac{1}{2}\gamma - \frac{1}{2t}\gamma^4 & -\frac{1}{2}\gamma^2 + \frac{1}{2t}\gamma^5 & \gamma^3 & \frac{3t}{2}\gamma - \frac{1}{2}\gamma^4 & \frac{3t}{2}\gamma^2 - \frac{1}{2}\gamma^5 \\ 1 & -\frac{1}{2}\gamma + \frac{1}{2t}\gamma^4 & -\frac{1}{2}\gamma^2 - \frac{1}{2t}\gamma^5 & \gamma^3 & -\frac{3t}{2}\gamma - \frac{1}{2}\gamma^4 & -\frac{3t}{2}\gamma^2 - \frac{1}{2}\gamma^5 \\ 1 & -\gamma & \gamma^2 & -\gamma^3 & \gamma^4 & -\gamma^5 \\ 1 & \frac{1}{2}\gamma + \frac{1}{2t}\gamma^4 & -\frac{1}{2}\gamma^2 + \frac{1}{2t}\gamma^5 & -\gamma^3 & \frac{3t}{2}\gamma - \frac{1}{2}\gamma^4 & -\frac{3t}{2}\gamma^2 + \frac{1}{2}\gamma^5 \\ 1 & \frac{1}{2}\gamma - \frac{1}{2t}\gamma^4 & -\frac{1}{2}\gamma^2 - \frac{1}{2t}\gamma^5 & -\gamma^3 & -\frac{3t}{2}\gamma - \frac{1}{2}\gamma^4 & \frac{3t}{2}\gamma^2 + \frac{1}{2}\gamma^5 \end{pmatrix}.$$

We can build the matrix of the action $M(H,L)$ from this, and as the fixed basis of L is integral, reducing this matrix gives a basis of the associated order $\mathfrak{A}_{L/K}$. The Hermite normal form of $M(H,L)$ is

$$D = \begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

The columns of D^{-1} provide the basis of $\mathfrak{A}_{L/K}$

$$\left\{1_G, \sigma, \frac{1_G + \sigma + \sigma^2}{3}, \tau, \sigma\tau, \frac{\tau + \sigma\tau + \sigma^2\tau}{3}\right\}.$$

Although this is not an induced Hopf Galois structure, the matrix D is a Kronecker product and consequently the associated order $\mathfrak{A}_{L/K}$ is a tensor product of $\mathcal{O}_K$-modules.

Let us move on to the freeness over $\mathfrak{A}_{L/K}$. Since 3 appears twice in the diagonal of D, the index of the classical Galois structure is $I(H_c, L) = 2$. Now, given $\beta = \sum_{i=1}^{6} \beta_i \gamma^{i-1}$, we have

$$D_\beta(H,L) = -\frac{2\beta_1\beta_4(\beta_2\beta_3 - 3a\beta_5\beta_6)(\beta_2\beta_3 + 3a\beta_5\beta_6)}{t^2}.$$

In particular, if we take $\beta = 1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5$, then

$$D_\beta(H, L) = \frac{18(1 - 9a^2)}{a},$$

and since 3 does not divide $1 - 9a^2$, $v_3(D_\beta(H, L)) = 2 = I(H_c, L)$. Hence, β indeed generates $\mathcal{O}_L$ as an $\mathfrak{A}_{L/\mathbb{Q}_3}$-module.

The following summarizes the results obtained in this section:

Corollary 6.10. *Let $L/\mathbb{Q}_3$ be a dihedral degree 6 extension defined by one of the radical polynomials. Then:*

1. *$\{1, -t\frac{\alpha^2 z}{3a}, \alpha, z, \alpha^2, \alpha z\}$ is an integral basis of L.*
2. *$\left\{1_G, \sigma, \dfrac{1_G + \sigma + \sigma^2}{3}, \tau, \sigma\tau, \dfrac{\tau + \sigma\tau + \sigma^2\tau}{3}\right\}$ is a $\mathbb{Z}_3$-basis of $\mathfrak{A}_{L/\mathbb{Q}_3}$.*
3. *$\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}_3}$-free and $\beta = 1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5$ is a normal integral basis generator.*

6.4 Cyclic Hopf Galois module structure

Now, we consider the Hopf Galois structures of $L/\mathbb{Q}_p$ of type C_{2p} and consider the problem of determining the associated order and the module structure of $\mathcal{O}_L$ in each of them. Recall that the Hopf Galois structures of cyclic type of a dihedral degree $2p$ extension are the induced ones and were completely described in Theorem 6.1. We know that $H = H_1 \otimes H_2$, where H_1 is a Hopf Galois structure of some degree p subextension $E/\mathbb{Q}_p$ and H_2 is a Hopf Galois structure of the unique quadratic subextension $F/\mathbb{Q}_p$. As in Corollary 6.4 the form of an integral basis depended on the ramification of $F/\mathbb{Q}_p$, we make the same distinction again.

Corollary 6.11. *Assume that $F/\mathbb{Q}_p$ is unramified. Then:*

1. *$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_p} \mathfrak{A}_{H_2}$.*
2. *If $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free and the product of normal integral basis generators of E and F gives a normal integral basis generator of L.*

Proof. Since $F/\mathbb{Q}_p$ is unramified, $E/\mathbb{Q}_p$ and $F/\mathbb{Q}_p$ are arithmetically disjoint. Then, Corollary 5.42 gives that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_p} \mathfrak{A}_{H_2}$. For the second part, by assumption $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free, and the hypothesis that $F/\mathbb{Q}_p$ is unramified gives that $\mathcal{O}_F$ is $\mathfrak{A}_{H_2}$-free. Then we apply Theorem 5.47. □

Next, we assume that $F/\mathbb{Q}_p$ is ramified, which implies that $L/\mathbb{Q}_p$ is totally ramified. By Proposition 6.3, the powers of the uniformising parameter $\gamma = \frac{z}{\alpha^{\frac{p-1}{2}}}$ form an integral basis

$$B' = \{1, \gamma, \gamma^2, \cdots, \gamma^{2p-1}\}$$

of L. Since the action of H on L is the tensor product of the actions of H_1 on E and of H_2 on F, it is clear that

$$G(H_W, L_B) = G(H_1, E) \otimes G(H_2, F).$$

Besides, we know that $G(H_W, L_{B'}) = G(H_W, L_B)P_B^{B'}$.

Then, in practice, carrying out the product of matrices above, one can compute the Gram matrix where in L we fix an integral basis. However, powers of γ greater than $2p-1$ normally appear in the result. In order to reduce them, we need the minimal polynomial of γ. To this end, we use the following fact about the resultant:

Proposition 6.12. *If K is a field and $f, g \in K[x]$ are polynomials with f monic, then*

$$\mathrm{Res}_x(f,g) = \prod_{f(\alpha)=0} g(\alpha)$$

and it gives an explicit polynomial expression in the coefficients of f and g.

We take the expression of γ in terms of the tensor basis B and define a polynomial $\Gamma \in F[x]$ obtained by replacing α by an indeterminate x in the expression of γ. Let Y be another indeterminate. Then, $\mathrm{Res}_x(f, Y-\Gamma) = \prod_{i=1}^{p}(Y - \Gamma(\alpha_i))$ gives an explicit polynomial expression

$$Y^p + c_1 Y^{p-1} + \cdots + c_{p-1}Y + c_p$$

in Y with coefficients $c_i \in F$ and root γ. Let us write $c_i = a_i + b_i z$, $a_i, b_i \in \mathbb{Q}_p$. Then,

$$(Y^p + a_1 Y^{p-1} + \cdots a_{p-1}Y + a_p)^2 - z^2(b_1 Y^{p-1} + \cdots + b_{p-1}Y + b_p)^2$$

is a polynomial of degree $2p$ with root γ, which turns out to be its minimal polynomial.

This yields the following method to compute $M(H_W, L_{B'})$:

1. Write the powers of γ in terms of the tensor basis B to compute the matrix $P_B^{B'}$.
2. Compute the minimal polynomial of γ.
3. Compute the Kronecker product $G(H_1, E) \otimes G(H_2, F)$ and multiply on left side by $P_B^{B'}$, obtaining $G(H_W, L_{B'})$.
4. Compute $M(H_W, L_{B'})$ from the entries of $G(H_W, L_{B'})$.

Once we have computed $M(H_W, L_{B'})$, since B' is an integral basis of L, we can apply the reduction method to compute a basis of $\mathfrak{A}_H$ and determine the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$.

6.4.1 The case $p = 3$

If $p = 3$, we know that L is the splitting field over $\mathbb{Q}_3$ of one of the polynomials

$$x^3+3, \quad x^3+12, \quad x^3+21, \quad x^3+3x+3, \quad x^3+6x+3, \quad x^3+3x^2+3.$$

We adopt the terminology of Section 4.4. We can solve the singular case easily. In this case, we have that $F/\mathbb{Q}_3$ is unramified and we know by Proposition 4.11 that $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free, so we apply Corollary 6.11 to conclude that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$ and $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with normal integral basis generator the product of normal integral basis generators of E and F.

So assume that $L/\mathbb{Q}_3$ is totally ramified, that is, f is one of the first five polynomials.

Change basis matrix

Let $H = H_1 \otimes H_2$ be an induced Hopf Galois structure. We fix as $\mathbb{Q}_3$-basis of H the product of the bases in H_1 and H_2, that is,

$$W := \{w_1\eta_1, w_1\eta_2, w_2\eta_1, w_2\eta_2, w_3\eta_1, w_3\eta_2\}.$$

Since $L/\mathbb{Q}_3$ is totally ramified, by Proposition 6.3, the basis B' given by the powers of $\frac{z}{\alpha}$ up to 5 is integral, where z is the square root of a non-square in $\mathbb{Z}_3$ and α is a root of f. We determine the change basis matrix from the product basis B to the basis B'.

As usual, we begin with the radical cases $f(x) = x^3 + 3a$, $a \in \{1, 4, 7\}$. We have that

$$\frac{z}{\alpha} = -\frac{\alpha^2 z}{3a}$$

with $z = \sqrt{-3}$. Let $t = \sqrt{a}$. In order to simplify computations, we will choose

$$\gamma := -t\frac{\alpha^2 z}{3a},$$

which is also an uniformizing parameter of $\mathcal{O}_L$ because $t \in \mathbb{Z}_3^*$. Now, we compute the powers of γ:

$$\gamma^2 = \alpha, \quad \gamma^3 = tz, \quad \gamma^4 = \alpha^2, \quad \gamma^5 = t\alpha z.$$

Then, the change of basis matrix from the tensor basis B to the basis B' of the powers of γ is

$$P_B^{B'} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & t & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & t \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -\frac{1}{3t} & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let us move to the second group. In this case,

$$\frac{z}{\alpha} = -\frac{(\alpha^2 + 3a)z}{3}.$$

If $a = 1$, we take

$$\gamma = -\frac{(\alpha^2 + 3)tz}{3},$$

where $z = \sqrt{-39}$ and $t = \sqrt{\frac{1}{13}}$, so $tz = \sqrt{-3}$. The powers of γ are

$$\gamma^2 = -\alpha^2 + \alpha - 3, \quad \gamma^3 = t\alpha^2 z - t\alpha z + 4tz,$$

$$\gamma^4 = 4\alpha^2 - 3\alpha + 15, \quad \gamma^5 = -5t\alpha^2 z + 4t\alpha z - 18tz.$$

Hence, in this case

$$P_B^{B'} = \begin{pmatrix} 1 & 0 & -3 & 0 & 15 & 0 \\ 0 & -t & 0 & 4\,t & 0 & -18\,t \\ 0 & 0 & 1 & 0 & -3 & 0 \\ 0 & 0 & 0 & -t & 0 & 4\,t \\ 0 & 0 & -1 & 0 & 4 & 0 \\ 0 & -\frac{t}{3} & 0 & t & 0 & -5\,t \end{pmatrix}.$$

If $a = 2$, we choose again $\gamma = -\frac{(\alpha^2+3)tz}{3}$, but now $t = \sqrt{-\frac{1}{41}}$ and $z = \sqrt{-123}$, so $tz = -\sqrt{3}$. The powers of γ are

$$\gamma^2 = 2\alpha^2 - \alpha + 12, \quad \gamma^3 = -4t\alpha^2 z + 2t\alpha z - 25tz,$$

$$\gamma^4 = 25\alpha^2 - 12\alpha + 156, \quad \gamma^5 = -52t\alpha^2 z + 25t\alpha z - 324tz.$$

Hence, we obtain

$$P_B^{B'} = \begin{pmatrix} 1 & 0 & 12 & 0 & 156 & 0 \\ 0 & -2\,t & 0 & -25\,t & 0 & -324\,t \\ 0 & 0 & -1 & 0 & -12 & 0 \\ 0 & 0 & 0 & 2\,t & 0 & 25\,t \\ 0 & 0 & 2 & 0 & 25 & 0 \\ 0 & -\frac{t}{3} & 0 & -4\,t & 0 & -52\,t \end{pmatrix}.$$

The minimal polynomial of γ

To compute the minimal polynomial of γ for the radical cases it is enough to remark that

$$\gamma^6 = (\gamma^3)^2 = (tz)^2 = -3a,$$

so γ is a root of $Y^6 + 3a$.

For polynomials of the second group, we use the resultant. For $a = 1$, we have

$$\mathrm{Res}_x\left(x^3 + 3x + 3, Y - \left(-\frac{(\alpha^2+3)tz}{3}\right)\right) = Y^3 + tzY^2 - tz = Y^3 + (Y^2 t - t)z.$$

Recall by Proposition 6.12 that this has root γ as a polynomial in Y. Then, evaluating in γ and rising to the square gives that

$$Y^6 - (Y^2 t - t)^2 z^2 = Y^6 + 3Y^4 - 6Y^2 + 3$$

is the minimal polynomial of γ. For $a = 2$, similarly we find the polynomial

$$Y^6 - 12Y^4 - 12Y^2 - 3.$$

The action on $L/\mathbb{Q}_3$

For the first three cases,

$$G(H_1, E) \otimes G(H_2, F) = \begin{pmatrix} 1 & z & \alpha & \alpha\,z & \alpha^2 & \alpha^2 z \\ 1 & -z & \alpha & -\alpha\,z & \alpha^2 & -\alpha^2 z \\ 0 & 0 & -3\,\alpha & -3\,\alpha\,z & 3\,\alpha^2 & 3\,\alpha^2 z \\ 0 & 0 & -3\,\alpha & 3\,\alpha\,z & 3\,\alpha^2 & -3\,\alpha^2 z \\ 2 & 2\,z & -\alpha & -\alpha\,z & -\alpha^2 & -\alpha^2 z \\ 2 & -2\,z & -\alpha & \alpha\,z & -\alpha^2 & \alpha^2 z \end{pmatrix},$$

whence we compute the Gram matrix

$$G(H_W, L_{B'}) = (G(H_1, E) \otimes G(H_2, F))P_B^{B'}$$
$$= \begin{pmatrix} 1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 \\ 1 & -\gamma & \gamma^2 & -\gamma^3 & \gamma^4 & -\gamma^5 \\ 0 & 3\gamma & -3\gamma^2 & 0 & 3\gamma^4 & -3\gamma^5 \\ 0 & -3\gamma & -3\gamma^2 & 0 & 3\gamma^4 & 3\gamma^5 \\ 2 & -\gamma & -\gamma^2 & 2\gamma^3 & -\gamma^4 & -\gamma^5 \\ 2 & \gamma & -\gamma^2 & -2\gamma^3 & -\gamma^4 & \gamma^5 \end{pmatrix},$$

where we have used that $\gamma^7 = 3a\gamma$ to determine the entries of the second column. For the fourth and fifth polynomial the matrix $G(H_W, L_{B'})$ is obtained in a completely analogous way and their entries can be checked in (B.22) and (B.23) respectively.

Basis of $\mathfrak{A}_H$

From the previous step we compute the matrix $M(H_W, L_{B'})$, and since B' is an integral basis of L, reducing this matrix provides a basis of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module.

For the first class of polynomials, the Hermite normal form of $M(H_W, L_{B'})$ is

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix},$$

with inverse

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 1 & 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{3} \end{pmatrix}.$$

Then, we obtain the basis of the associated order $\mathfrak{A}_H$

$$\left\{ w_1\eta_1, w_1\eta_2, \frac{w_2\eta_1}{3}, \frac{w_2\eta_2}{3}, \frac{w_1\eta_1 + w_3\eta_1}{3}, \frac{w_1\eta_2 + w_3\eta_2}{3} \right\}.$$

Taking into account the basis of $\mathfrak{A}_{H_1}$ in Theorem 4.11 and the basis of $\mathfrak{A}_{H_2}$ computed using Theorem 2.50, we see that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes \mathfrak{A}_{H_2}$.

Although this is enough for our purposes, it is worth taking a deeper look at this case. Note that we can also use that B' is an eigenvectors basis with eigenvalues matrix

$$\Lambda = \begin{pmatrix} 1 & 1 & 0 & 0 & 2 & 2 \\ 1 & -1 & 0 & 0 & 2 & -2 \\ 1 & 1 & 3 & 3 & -1 & -1 \\ 1 & -1 & 3 & -3 & -1 & 1 \\ 1 & 1 & -3 & -3 & -1 & -1 \\ 1 & -1 & -3 & 3 & -1 & 1 \end{pmatrix},$$

which gives the basis of pairwise orthogonal idempotents

$$\left\{\frac{w_1\eta_1+w_1\eta_2+w_3\eta_1+w_3\eta_2}{6}, \frac{w_1\eta_1-w_1\eta_2+w_3\eta_1-w_3\eta_2}{6},\right.$$
$$\frac{2w_1\eta_1+2w_1\eta_2+w_2\eta_1+w_2\eta_2-w_3\eta_1-w_3\eta_2}{6},$$
$$\frac{2w_1\eta_1-2w_1\eta_2+w_2\eta_1-w_2\eta_2-w_3\eta_1+w_3\eta_2}{6},$$
$$\frac{2w_1\eta_1+2w_1\eta_2-w_2\eta_1-w_2\eta_2-w_3\eta_1-w_3\eta_2}{6},$$
$$\left.\frac{2w_1\eta_1-2w_1\eta_2-w_2\eta_1+w_2\eta_2-w_3\eta_1-w_3\eta_2}{6}\right\}$$

In addition, we see that B is a (non-integral) basis of eigenvectors and the eigenvalues matrix in this case is obtained from erasing the zero rows of $M(H_1, E) \otimes M(H_2, F)$, that is,

$$\Lambda' = \begin{pmatrix} 1 & 1 & 0 & 0 & 2 & 2 \\ 1 & -1 & -3 & 3 & -1 & 1 \\ 1 & 1 & 3 & 3 & -1 & -1 \\ 1 & -1 & 0 & 0 & 2 & -2 \\ 1 & 1 & -3 & -3 & -1 & -1 \\ 1 & -1 & 3 & -3 & -1 & 1 \end{pmatrix},$$

and this matrix is obtained from permuting the rows of Λ, which was obtained by erasing the zero rows of $M(H_W, L_{B'})$. That is, there is a permutation matrix P such that $PM(H_W, L_{B'}) = M(H_1, E) \otimes M(H_2, F)$, which proves that the basis B' is induced. Consequently, B' is an example of integral induced basis in which the pieces $E/\mathbb{Q}_3$ and $F/\mathbb{Q}_3$ are not arithmetically disjoint. Furthermore, since B' is an integral induced basis, we can also reach the conclusion that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes \mathfrak{A}_{H_2}$ using Theorem 5.41.

For the second group of polynomials we get

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix},$$

with inverse

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 0 & 1 & 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & 1 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{3} \end{pmatrix}.$$

and the associated order $\mathfrak{A}_H$ has $\mathbb{Z}_3$-basis

$$\left\{w_1\eta_1, w_1\eta_2, w_2\eta_1, \frac{w_2}{3}(\eta_1+\eta_2), w_3\eta_1, \frac{w_1+w_3}{3}(\eta_1+\eta_2)\right\}.$$

In this case $\mathfrak{A}_H \neq \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$ since $\frac{w_2}{3}\eta_1 \in \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$ and $\frac{w_2}{3}\eta_1 \notin \mathfrak{A}_H$.

Freeness over $\mathfrak{A}_H$

For the first three polynomials we have $I(H,L)=4$ and the matrix associated to an element $\beta=\sum_{i=1}^6\beta_i\gamma^{i-1}$ has determinant

$$D_\beta(H,L)=-2592\beta_1\beta_2\beta_3\beta_4\beta_5\beta_6.$$

Since $v_3(2592)=4$, for $\beta=1+\gamma+\gamma^2+\gamma^3+\gamma^4+\gamma^5$ we have the equality $v_3(D_\beta(H,L))=I(H,L)$. Hence, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free and β is a generator.

For the fourth polynomial

$$D_\beta(H,L)=-288\left(3\,{\beta_3}^2-23\,\beta_3\,\beta_5+43\,{\beta_5}^2\right)(\beta_2-6\,\beta_4+24\,\beta_6)$$
$$\left({\beta_2}^2-15\,\beta_2\,\beta_4+66\,\beta_6\,\beta_2+27\,{\beta_4}^2-261\,\beta_6\,\beta_4+621\,{\beta_6}^2\right)(\beta_1-\beta_3+7\,\beta_5)\,.$$

If $\beta=\gamma+\gamma^4$, then the determinant is -86688, which has 3-adic valuation 2. Since $I(H,L)=2$, we conclude that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

For the fifth polynomial

$$D_\beta(H,L)=-288\left(20\,{\beta_3}^2+499\,\beta_3\,\beta_5+3112\,{\beta_5}^2\right)(2\,\beta_2+27\,\beta_4+348\,\beta_6)\left(4\,{\beta_2}^2\right.$$
$$\left.+114\,\beta_2\,\beta_4+1473\,\beta_6\,\beta_2+720\,{\beta_4}^2+18684\,\beta_6\,\beta_4+121194\,{\beta_6}^2\right)(\beta_1+4\,\beta_3+56\,\beta_5)\,.$$

We take again $\beta=\gamma+\gamma^4$. In such case, the determinant is -401522688, which has 3-adic valuation 2, and then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

The product of generators

Let us check that the product β' of the generators ϵ of $\mathcal{O}_E$ as $\mathfrak{A}_{H_1}$-module and δ of $\mathcal{O}_F$ as $\mathfrak{A}_{H_2}$-module is not a generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module.

Such a product is of the form

$$\beta'=(\epsilon_1+\epsilon_2\alpha+\epsilon_3\alpha^2)(\delta_1+\delta_2z)=\epsilon_1\delta_1+\epsilon_1\delta_2z+\epsilon_2\delta_1\alpha+\epsilon_2\delta_2\alpha z+\epsilon_3\delta_1\alpha^2+\epsilon_3\delta_2\alpha^2z$$

with $\epsilon_i,\delta_j\in\mathbb{Z}_3$ such that $\epsilon_1\epsilon_2\epsilon_3,\ \delta_1\delta_2\in\mathbb{Z}_3^*$.

For the first three polynomials, changing coordinates to the basis of the powers of γ gives

$$P_{B'}^{B}\beta'_B=\begin{pmatrix}1&0&0&0&0&0\\0&0&0&0&0&-3t\\0&0&1&0&0&0\\0&\frac{1}{t}&0&0&0&0\\0&0&0&0&1&0\\0&0&0&\frac{1}{t}&0&0\end{pmatrix}\begin{pmatrix}\epsilon_1\delta_1\\\epsilon_1\delta_2\\\epsilon_2\delta_1\\\epsilon_2\delta_2\\\epsilon_3\delta_1\\\epsilon_3\delta_2\end{pmatrix}=\begin{pmatrix}\epsilon_1\delta_1\\-3t\epsilon_3\delta_2\\\epsilon_2\delta_1\\\frac{\epsilon_1\delta_2}{t}\\\epsilon_3\delta_1\\\frac{\epsilon_2\delta_2}{t}\end{pmatrix},$$

that is, $\beta'=\epsilon_1\delta_1-3t\epsilon_3\delta_2\gamma+\epsilon_2\delta_1\gamma^2+\frac{\epsilon_1\delta_2}{t}\gamma^3+\epsilon_3\delta_1\gamma^4+\frac{\epsilon_2\delta_2}{t}\gamma^5$. Then,

$$D_{\beta'}(H,L)=7776\,\frac{{\epsilon_2}^2{\delta_2}^3{\epsilon_3}^2{\delta_1}^3{\epsilon_1}^2}{t}.$$

Since $v_3(7776) = 5$, we have that $v_3(D_{\beta'}(H,L)) > 4$, proving that β' is not a generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module.

Let us consider the second class of polynomials. If $a = 1$,

$$D_{\beta'}(H,L) = 7776\,\frac{{\delta_1}^3\left({\epsilon_2}^2 + 3\,\epsilon_2\,\epsilon_3 - {\epsilon_3}^2\right)^2 {\delta_2}^3\,(\epsilon_1 - 2\,\epsilon_3)^2}{t^3}.$$

and if $a = 2$,

$$D_{\beta'}(H,L) = 31104\,\frac{{\delta_1}^3\left({\epsilon_2}^2 + \frac{3}{2}\,\epsilon_2\,\epsilon_3 - 2\,{\epsilon_3}^2\right)^2 {\delta_2}^3\,(\epsilon_1 - 4\,\epsilon_3)^2}{t^3}$$

In both cases, since $v_3(D_{\beta'}(H,L)) \geq 5 > I(H,L)$, β' is not a free generator.

Summary of results

We summarize the results we have obtained for the case $p = 3$. With the notation used throughout this section:

Theorem 6.13 (Associated orders). *1. For the first three polynomials and the last one, $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$.*

2. For the fourth and the fifth polynomials $\mathfrak{A}_H \neq \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$ and a basis of $\mathfrak{A}_H$ is

$$\left\{w_1\eta_1, w_1\eta_2, w_2\eta_1, \frac{w_2}{3}(\eta_1+\eta_2), w_3\eta_1, \frac{w_1+w_3}{3}(\eta_1+\eta_2)\right\}.$$

Theorem 6.14 (Freeness). *$\mathcal{O}_L$ is $\mathfrak{A}_H$-free in all cases. For the last polynomial the product of a generator of $\mathcal{O}_E$ as $\mathfrak{A}_{H_1}$-module and a generator of $\mathcal{O}_F$ as $\mathfrak{A}_{H_2}$-module is a generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module, while in the rest of the cases such a product is never a generator.*

6.4.2 The case $p = 5$

We consider the dihedral degree 10 extension $L/\mathbb{Q}_5$. Recall that L is the splitting field over $\mathbb{Q}_5$ of one of the polynomials

$$x^5 + 15x^2 + 5, \quad x^5 + 10x^2 + 5, \quad x^5 + 5x^4 + 5.$$

We have seen in Section 6.2.2 that the unique case in which $F/\mathbb{Q}_5$ is unramified is the third one. In that case, Corollary 6.11 gives us again that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_5} \mathfrak{A}_{H_2}$. On the other hand, Theorem 4.12 gives us that $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free, and by Theorem 2.50, $\mathcal{O}_F$ is $\mathfrak{A}_{H_2}$-free. Then, applying Corollary 6.11, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator a product of generators of $\mathcal{O}_E$ and $\mathcal{O}_F$. Hence, throughout this section we consider the first two cases.

Integral basis of L

By Proposition 6.3, the powers of $\frac{z}{\alpha^2}$ form an integral basis B' of L.

For the first case, recall that the polynomial

$$x^5 - 15x^3 - 10x^2 + 75x + 30$$

defines the same extension. In this case, we take

$$\gamma = 12t\frac{z}{\alpha^2} = \frac{1}{5}\left(5\,\alpha^4 - 2\,\alpha^3 - 75\,\alpha^2 - 20\,\alpha + 395\right)tz,$$

where $t = -\sqrt{-\frac{3}{13}}$ (and then $tz = \sqrt{5}$, since $z = -\sqrt{-\frac{65}{3}}$), which is also an uniformizer because $12t \in \mathbb{Z}_5^*$. The other powers of γ that complete B' are expressed in (B.24).

In the other case, we take

$$\gamma = 40t\frac{z}{\alpha^2} = \frac{1}{5}\left(5\,\alpha^4 - 2\,\alpha^3 - 175\,\alpha + 320\right)tz,$$

where $t = -\sqrt{-\frac{2}{47}}$ (and then $tz = \sqrt{10}$, since $z = \sqrt{-235}$). The other powers of γ are in (B.25).

The minimal polynomial of γ

For the first case, we have

$$Res_x\left(x^5 - 15\,x^3 - 10\,x^2 + 75\,x + 30, Y - zt\left(x^4 - \frac{2}{5}\,x^3 - 15\,x^2 - 4\,x + 79\right), x\right) =$$
$$-\frac{6912\,z^5t^5}{25} + \frac{3456\,z^4t^4Y}{5} - 720\,z^3t^3Y^2 + 376\,z^2t^2Y^3 - 83\,ztY^4 + Y^5.$$

Writing this in the form $c_1 + c_2z$ with c_1, c_2 polynomials in Y and rising to the square, one obtains that

$$Y^{10} - 30685\,Y^8 + 580960\,Y^6 - 5564160\,Y^4 + 49766400\,Y^2 - 238878720$$

is the minimal polynomial of γ.

For the second case, we similarly find the minimal polynomial

$$Y^{10} - 56920\,Y^8 + 1844800\,Y^6 - 29163520\,Y^4 - 209715200\,Y^2 - 671088640.$$

Basis of $\mathfrak{A}_H$

We recall the procedure for both cases:

- From the Gram matrix $G(H_1, E)$ computed in Section 4.5.1 and the Gram matrix $G(H_2, F)$ computed in the case of Theorem 2.50, we compute the Kronecker product $G(H_1, E) \otimes G(H_2, F)$.
- We apply the matrix $P_B^{B'}$, whose columns are the coordinates of the powers of γ with respect to the tensor basis B, computed in Section 6.4.2. We obtain $G(H_W, L_{B'})$.
- We use the minimal polynomial of γ computed in Section 6.4.2 to obtain the coordinates of all entries with respect to the basis of γ.
- Now, we are able to determine $M(H_W, L_{B'})$.

We show directly the Hermite normal form of $M(H_W, L_{B'})$ for the totally ramified cases.

For the first polynomial, the Hermite normal form is

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix},$$

which gives the basis of $\mathfrak{A}_H$

$$\Big\{w_1\eta_1, w_1\eta_2, w_2\eta_1, w_2\eta_2, w_3\eta_1, \frac{-2w_2+w_3}{5}(\eta_1+\eta_2), \\ w_4\eta_1, w_4\eta_2, w_5\eta_1, \frac{w_1+w_4+w_5}{5}(\eta_1+\eta_2)\Big\}.$$

For the second one, we obtain as Hermite normal form

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix},$$

giving the basis of $\mathfrak{A}_H$

$$\Big\{w_1\eta_1, w_1\eta_2, w_2\eta_1, w_2\eta_2, w_3\eta_1, \frac{2w_2+w_3}{5}(\eta_1+\eta_2), \\ w_4\eta_1, w_4\eta_2, w_5\eta_1, \frac{w_1+w_4+w_5}{5}(\eta_1+\eta_2)\Big\}.$$

In both cases, $\mathfrak{A}_H \neq \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_5} \mathfrak{A}_{H_2}$.

Freeness over $\mathfrak{A}_H$

Let $\beta = \sum_{i=1}^{6} \beta_i \gamma^{i-1} \in \mathcal{O}_L$. Using the matrix $M(H_W, L_B)$ that we have computed in the previous section, we can determine the matrix $M_\beta(H_W, L_B)$ associated to β, whose determinant allows us to determine whether or not $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. In both cases, we have $I(H, L) = 2$, and if

$$\beta = 1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5 + \gamma^6 + \gamma^7 + \gamma^8 + \gamma^9,$$

$v_5(D_\beta(H,L)) = 2$, so $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

Let us study whether or not the product of generators is a generator. Let $\epsilon = \sum_{i=1}^{5} \epsilon_i \alpha^{i-1}$ be an $\mathfrak{A}_{H_1}$-generator of $\mathcal{O}_E$ and $\delta = \delta_1 + \delta_2 z$ an $\mathfrak{A}_{H_2}$-generator of $\mathcal{O}_F$. Such product is

$$\begin{aligned}\beta' = \epsilon_1\delta_1 + \epsilon_1\delta_2 z + \epsilon_2\delta_1\alpha + \epsilon_2\delta_2\alpha z + \epsilon_3\delta_1\alpha^2 + \epsilon_3\delta_2\alpha^2 z + \epsilon_4\delta_1\alpha^3 + \epsilon_4\delta_2\alpha^3 z\\ + \epsilon_5\delta_1\alpha^4 + \epsilon_5\delta_2\alpha^4 z,\end{aligned}$$

and applying $P_{B'}^{B}$ on the column of its coordinates, we obtain its vector of coordinates $(\beta_i')_{i=1}^{10}$ with respect to B'. The vectors for each case are shown in (B.26) and (B.27). If we set these coordinates to the previously computed determinant $D_\beta(H,L)$, we find that $v_5(D_{\beta'}(H,L)) > 2$, so β' is not a $\mathfrak{A}_H$-generator of $\mathcal{O}_L$.

Summary of results

For $p = 5$, we obtain the following results:

Theorem 6.15 (Associated orders). 1. *The equality $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_5} \mathfrak{A}_{H_2}$ holds only for the third polynomial.*

2. *For the first polynomial, a basis of $\mathfrak{A}_H$ is*

$$\Big\{ w_1\eta_1, w_1\eta_2, w_2\eta_1, w_2\eta_2, w_3\eta_1, \frac{-2w_2 + w_3}{5}(\eta_1+\eta_2),$$
$$w_4\eta_1, w_4\eta_2, w_5\eta_1, \frac{w_1+w_4+w_5}{5}(\eta_1+\eta_2) \Big\},$$

while for the second polynomial, a basis is

$$\Big\{ w_1\eta_1, w_1\eta_2, w_2\eta_1, w_2\eta_2, w_3\eta_1, \frac{2w_2 + w_3}{5}(\eta_1+\eta_2),$$
$$w_4\eta_1, w_4\eta_2, w_5\eta_1, \frac{w_1+w_4+w_5}{5}(\eta_1+\eta_2) \Big\}.$$

Theorem 6.16 (Freeness). *$\mathcal{O}_L$ is $\mathfrak{A}_H$-free for all cases. Only for the last polynomial the product of a generator of $\mathcal{O}_E$ as $\mathfrak{A}_{H_1}$-module and a generator of $\mathcal{O}_F$ as $\mathfrak{A}_{H_2}$-module is a generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module.*

Remark 6.17. Since $\mathcal{O}_E$ is always free by Theorem 4.12 and $\mathcal{O}_F$ is always $\mathfrak{A}_{H_2}$-free by Theorem 2.50, we see that the first statement of Theorem 5.47 hold for this case even though $E/\mathbb{Q}_5$ and $F/\mathbb{Q}_5$ are not arithmetically disjoint.

6.5 The extension L/F

As usual in this chapter, let $L/\mathbb{Q}_p$ be a dihedral degree $2p$ extension of p-adic fields, and let $F/\mathbb{Q}_p$ be its unique quadratic subextension. In this section we are interested in the extension L/F rather than in $L/\mathbb{Q}_p$. Since this is a cyclic degree p extension, the classical Galois structure is its unique Hopf Galois structure. Actually, this structure can be seen as the tensor product of the (almost classically Galois) Hopf Galois structure of any degree p subextension $E/\mathbb{Q}_p$ by F. Concerning the integral setting, we want to study the extension L/F so as to compare the information obtained from the one of $E/\mathbb{Q}_p$, that has been already determined.

In order to compare $\mathfrak{A}_{L/F}$ with $\mathfrak{A}_{E/\mathbb{Q}_3}$, since the latter is inside $L[\lambda(J)]$, we will consider $\mathfrak{A}_{L/F}$ inside $F[\lambda(J)]$. In general, we do not identify anymore the Galois group of an extension with its image by the left translation λ when considering the Hopf algebra of the classical Galois structure.

As in the previous sections, the easiest case is the singular one, when the defining polynomial is $x^p + px^{p-1} + p$. In that case, $E/\mathbb{Q}_p$ and $F/\mathbb{Q}_p$ are arithmetically disjoint, so:

- By Proposition 5.48, $\mathfrak{A}_{L/F} = \mathfrak{A}_{E/\mathbb{Q}_p} \otimes \mathcal{O}_F$.
- By Corollary 5.49, whenever $\mathcal{O}_E$ is $\mathfrak{A}_{E/\mathbb{Q}_p}$-free, $\mathcal{O}_L$ is $\mathfrak{A}_{L/F}$-free with the same generator.

The second item does not solve completely the problem in that case but gives a sufficient condition, which is satisfied for both $p = 3$ and $p = 5$ (see Theorems 4.11 and 4.12).

For the remainder of the section, we assume that $L/\mathbb{Q}_p$ is totally ramified. In that case, by Proposition 6.3, $\frac{z}{\alpha^{\frac{p-1}{2}}}$ is an uniformising parameter of L and consequently its powers up to $2p-1$ form an integral basis of L/K.

6.5.1 The associated order $\mathfrak{A}_{L/F}$

Radical cases

Let us assume that $f(x) = x^3 + 3a$ with $a \in \{1, 4, 7\}$. Let us define again $\gamma = \frac{tz}{\alpha}$ for $t = \sqrt{a} \in \mathcal{O}_F^*$. Let us call $\delta = -\frac{tz}{3a} \in F$, which has valuation $v_F(\delta) = -1$. Since L/F is totally ramified, the powers of γ up to 2 form an integral basis

$$B = \{1, \alpha, \delta\alpha^2\}$$

of L/F. We compute the corresponding Gram matrix:

$$G(H_c, L_B) = \begin{pmatrix} 1 & \alpha & \delta\alpha^2 \\ 1 & \zeta_3^2\alpha & \zeta_3\delta\alpha^2 \\ 1 & \zeta_3\alpha & \zeta_3^2\delta\alpha \end{pmatrix}.$$

Then, B is a basis of eigenvectors with eigenvalues basis

$$\Lambda = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3^2 & \zeta_3 \\ 1 & \zeta_3 & \zeta_3^2 \end{pmatrix}.$$

The inverse of this matrix is

$$\Omega = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{pmatrix},$$

which gives the basis of $\mathfrak{A}_{L/F}$

$$\left\{ \frac{\mathrm{Id} + \mu + \mu^2}{3}, \frac{\mathrm{Id} + \zeta_3\mu + \zeta_3^2\mu^2}{3}, \frac{\mathrm{Id} + \zeta_3^2\mu + \zeta_3\mu^2}{3} \right\}.$$

This is coherent with [Fer74, Section 2.1], according to which the associated order $\mathfrak{A}_{L/F}$ is the maximal $\mathcal{O}_K$-order in $F[\lambda(J)]$ since $t = 3 \equiv 0 \pmod 3$.

Now, let us compare $\mathfrak{A}_{L/F}$ with $\mathfrak{A}_{E/\mathbb{Q}_3} \otimes_{\mathbb{Z}_3} \mathcal{O}_F$, which is another $\mathcal{O}_F$-order in $F[\lambda(J)]$ (in this case we cannot apply Proposition 5.48). We know by Theorem 4.11 that the elements

$$w_1 = \mathrm{Id}, \quad \frac{w_2}{3} = \frac{z(\mu - \mu^2)}{3}, \quad \frac{w_1 + w_3}{3} = \frac{\mathrm{Id} + \mu + \mu^2}{3}$$

form a $\mathbb{Z}_3$-basis of $\mathfrak{A}_{E/\mathbb{Q}_3}$, and hence an $\mathcal{O}_F$-basis of $\mathfrak{A}_{E/\mathbb{Q}_3}$. We have the equalities

$$\begin{cases} \frac{\mathrm{Id}+\mu+\mu^2}{3} & = \frac{\mathrm{Id}+\mu+\mu^2}{3} \\ \frac{\mathrm{Id}+\xi_3\mu+\xi_3^2\mu^2}{3} & = \frac{1}{2}\mathrm{Id} + \frac{1}{2}\frac{z(\mu-\mu^2)}{3} - \frac{1}{2}\frac{\mathrm{Id}+\mu+\mu^2}{3} \\ \frac{\mathrm{Id}+\xi_3^2\mu+\xi_3\mu^2}{3} & = \frac{1}{2}\mathrm{Id} - \frac{1}{2}\frac{z(\mu-\mu^2)}{3} - \frac{1}{2}\frac{\mathrm{Id}+\mu+\mu^2}{3} \end{cases}.$$

Hence, the matrix of the change of basis is

$$\begin{pmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \\ 1 & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

The determinant is $-1 \in \mathcal{O}_F^*$, so $\mathfrak{A}_{L/F} = \mathfrak{A}_{E/\mathbb{Q}_3} \otimes_{\mathbb{Z}_3} \mathcal{O}_F$.

We summarize the results that we have obtained.

Theorem 6.18. *Let $L/\mathbb{Q}_3$ be a radical degree 6 extension of 3-adic fields. Then, $\mathfrak{A}_{L/F}$ has $\mathbb{Z}_3$-basis*

$$\left\{\frac{\mathrm{Id} + \mu + \mu^2}{3}, \frac{\mathrm{Id} + \xi_3\mu + \xi_3^2\mu^2}{3}, \frac{\mathrm{Id} + \xi_3^2\mu + \xi_3\mu^2}{3}\right\}.$$

Moreover, $\mathfrak{A}_{L/F} = \mathfrak{A}_{E/\mathbb{Q}_3} \otimes_{\mathbb{Z}_3} \mathcal{O}_F$.

Weakly ramified cases

We will use the reduction method to determine a basis of the associated order $\mathfrak{A}_{L/F}$. Due to the high volume of computations, we will work only with the case $p = 3$. Then, the defining polynomial f of L is one of $x^3 + 3ax + 3$, with $a \in \{1, 2\}$.

First, we must determine an integral basis B of L/F. As in the radical case, the powers up to 2 of a uniformising parameter γ of L/K determine an integral basis of L/F. We take the value of γ given in Section 6.4.1, but renaming tz by z, so $\gamma = -\frac{(\alpha^2+3a)z}{3}$ with $z = \sqrt{-3}$ if $a = 1$ and $z = -\sqrt{3}$ if $a = 2$. By the computations in the aforementioned section, $\gamma^2 = (-1)^a(a\alpha^2 - \alpha + 3a^2)$. Then, the change basis matrix is

$$P_{B_c}^B = \begin{pmatrix} 1 & -az & (-1)^a 3a^2 \\ 0 & 0 & (-1)^{a+1} \\ 0 & -\frac{z}{3} & (-1)^a a \end{pmatrix}.$$

In order to compute the Gram matrix with respect to B_c, we must deal with the conjugates of α. Indeed, since the classical Galois structure has basis $\{1, \mu, \mu^2\}$ for $\mu = \lambda^J(\sigma)$, that matrix is

$$G(H_c, L_{B_c}) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \sigma^2(\alpha) & \sigma^2(\alpha^2) \\ 1 & \sigma(\alpha) & \sigma(\alpha^2) \end{pmatrix}.$$

We computed the conjugates of α in Section 4.4.1. By convention, we choose $\sigma = (\alpha_1, \alpha_2, \alpha_3)$ with $\alpha_1 = \alpha$ and

$$\alpha_2 = a\omega\alpha^2 - \frac{1+3a\omega}{2}\alpha + 2a\omega,$$

$$\alpha_3 = -a\omega\alpha^2 + \frac{-1+3a\omega}{2}\alpha - 2a\omega,$$

where $\omega = \sqrt{-\frac{3}{13}}$ if $a = 1$ and $\omega = \sqrt{-\frac{3}{41}}$ if $a = 2$. Hence, we have:

$$G(H_c, L_{B_c}) = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & -a\omega\,\alpha^2 + \left(\frac{3}{2}\,a\omega - \frac{1}{2}\right)\alpha - 2\,a\omega & \alpha_3^2 \\ 1 & a\omega\,\alpha^2 - \left(\frac{3}{2}\,a\omega + \frac{1}{2}\right)\alpha + 2\,a\omega & \alpha_2^2 \end{pmatrix},$$

with

$$\begin{aligned} \alpha_2^2 =& \Big(a^3\omega^2 + \frac{9}{4}\,a^2\omega^2 + \frac{3}{2}\,a\omega + \frac{1}{4}\Big)\alpha^2 + \\ & \Big(3\,a^3\omega^2 - 3\,a^2\omega^2 + a^2\omega\Big)\alpha + 4\,a^4\omega^2 + 9\,a^2\omega^2 + 3\,a\omega, \\ \alpha_3^2 =& \Big(a^3\omega^2 + \frac{9}{4}\,a^2\omega^2 - \frac{3}{2}\,a\omega + \frac{1}{4}\Big)\alpha^2 + \\ & \Big(3\,a^3\omega^2 - 3\,a^2\omega^2 - a^2\omega\Big)\alpha + 4\,a^4\omega^2 + 9\,a^2\omega^2 - 3\,a\omega. \end{aligned}$$

Now, we have that $G(H_c, L_B) = G(H_c, L_{B_c})P^B_{B_c}$, and from this we can compute the matrix of the action $M(H_c, L_B)$.

If $a = 1$, we have that

$$M(H_c, L_B) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -\frac{1}{2}\,z\,(1+\omega) & \frac{1}{2}\,z\,(-1+\omega) \\ 1 & -\frac{5}{2}\,\omega - \frac{1}{2} & \frac{5}{2}\,\omega - \frac{1}{2} \\ 0 & \frac{1}{3}\,\omega\,z & -\frac{1}{3}\,\omega\,z \\ 0 & -\frac{3}{2} - \frac{\omega}{2} & -\frac{3}{2} + \frac{\omega}{2} \\ 0 & -9\,\frac{\omega}{z} & 9\,\frac{\omega}{z} \\ 1 & \frac{5}{2}\,\omega - \frac{1}{2} & -\frac{5}{2}\,\omega - \frac{1}{2} \end{pmatrix}.$$

On the other hand, for $a = 2$, the matrix of the action is

$$M(H_c, L_B) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & -\frac{127\,z}{82} - 4\,\omega\,z & -\frac{127\,z}{82} + 4\,\omega\,z \\ 1 & -\frac{11}{4} - 11\,\omega & -\frac{11}{4} + 11\,\omega \\ 0 & -\frac{12\,z}{41} - \frac{4}{3}\,\omega\,z & -\frac{12\,z}{41} + \frac{4}{3}\,\omega\,z \\ 0 & 16\,\omega + \frac{381}{41} & -16\,\omega + \frac{381}{41} \\ 0 & \frac{3}{2}\,\frac{52\,\omega+9}{z} & -\frac{3}{2}\,\frac{52\,\omega-9}{z} \\ 1 & \frac{103}{82} + 11\,\omega & \frac{103}{82} - 11\,\omega \end{pmatrix}.$$

In both cases, the Hermite normal form is

$$D = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & z \end{pmatrix}.$$

Hence, $\mathfrak{A}_{L/F}$ has $\mathcal{O}_F$-basis

$$\Big\{\mathrm{Id}, \mu, \frac{\mathrm{Id} + \mu + \mu^2}{z}\Big\}.$$

If instead we apply [Fer74, Proposition 2], the basis of $\mathfrak{A}_{L/F}$ obtained is

$$\Big\{\mathrm{Id}, -\mathrm{Id} + \mu, \frac{\mathrm{Id} - 2\mu + \mu^2}{z}\Big\},$$

which is easily seen to be equivalent to the one provided by the reduction method, since the change basis matrix is unimodular.

Let us check if $\mathfrak{A}_{L/F}$ coincides with $\mathfrak{A}_{E/\mathbb{Q}_3} \otimes_{\mathcal{O}_K} \mathcal{O}_F$. Again by Theorem 4.11, this last order has $\mathcal{O}_F$-basis formed by

$$w_1 = \mathrm{Id}, \quad \frac{w_2}{3} = \frac{z(\mu - \mu^2)}{3}, \quad \frac{w_1 + w_3}{3} = \frac{\mathrm{Id} + \mu + \mu^2}{3}.$$

We write those elements with respect to the basis of $\mathfrak{A}_{L/F}$ computed in this section:

$$\begin{cases} w_1 = \mathrm{Id}, \\ \frac{w_3}{3} = \frac{z}{3}\mathrm{Id} + \frac{2z}{3}\mu + (-1)^{a-1}\frac{\mathrm{Id}+\mu+\mu^2}{z}, \\ \frac{w_1+w_3}{3} = \frac{(-1)^a}{z}\frac{\mathrm{Id}+\mu+\mu^2}{z}. \end{cases}$$

Then, the matrix of the change of basis is

$$P = \begin{pmatrix} 1 & \frac{z}{3} & 0 \\ 0 & \frac{2z}{3} & 0 \\ 0 & (-1)^{a-1} & \frac{(-1)^a}{z} \end{pmatrix}.$$

Now, $\det(P) = (-1)^a\frac{2}{3} \notin \mathcal{O}_F^*$. Thus, $\mathfrak{A}_{L/F} \neq \mathfrak{A}_{E/\mathbb{Q}_3} \otimes_{\mathbb{Z}_3} \mathcal{O}_F$.

To sum up:

Theorem 6.19. *Let $L/\mathbb{Q}_3$ be a weakly ramified degree 6 extension of 3-adic fields. Then, $\mathfrak{A}_{L/F}$ has $\mathbb{Z}_3$-basis*

$$\left\{\mathrm{Id}, \mu, \frac{\mathrm{Id}+\mu+\mu^2}{z}\right\}.$$

Moreover, $\mathfrak{A}_{L/F} \neq \mathfrak{A}_{E/\mathbb{Q}_3} \otimes_{\mathbb{Z}_3} \mathcal{O}_F$.

6.5.2 Module structure of $\mathcal{O}_L$ over $\mathfrak{A}_{L/F}$

We apply Proposition 1.33 to our situation with the cyclic degree p extension L/F, which is totally ramified. The ramification number can be obtained from the table in Theorem 6.6: it is $t = 1$ when $p > 3$ and $t \in \{1, 3\}$ when $p = 3$, depending on whether the extension is weakly ramified or not.

For $p > 3$, we have that p does not divide t, and since $t < p$, we deduce $a = t$. If the defining polynomial is one of the first two, then $F/\mathbb{Q}_p$ is ramified and $e(F/\mathbb{Q}_p) = 2$, thus

$$\frac{pe(F/\mathbb{Q}_p)}{p-1} - 1 = \frac{2p}{p-1} - 1 = \frac{p+1}{p-1},$$

and $t < \frac{p+1}{p-1}$. Since t divides $p-1$, $\mathcal{O}_L$ is $\mathfrak{A}_{L/F}$-free. For the last polynomial, $F/\mathbb{Q}_p$ is unramified and $e(F/\mathbb{Q}_p) = 1$, so

$$\frac{pe(F/\mathbb{Q}_p)}{p-1} - 1 = \frac{p}{p-1} - 1 = \frac{1}{p-1}$$

and then $\frac{1}{p-1} < t < \frac{p}{p-1}$. The expansion of $\frac{1}{p}$ is trivial, so $\mathcal{O}_L$ is $\mathfrak{A}_{L/F}$-free.

Now assume $p = 3$. For the radical cases, we have that $t = 3$ and $e(F/\mathbb{Q}_3) = 2$. Hence

$$\frac{3e(F/\mathbb{Q}_3)}{2} - 1 = \frac{6}{2} - 1 = 2,$$

and then $t = \frac{3e(F/\mathbb{Q}_3)}{2}$. The expansion of $\frac{3}{3} = 1$ is again trivial, so $\mathfrak{A}_{L/F}$-free. Now, if $L/\mathbb{Q}_3$ is weakly ramified, for the totally ramified cases we have $t = 1$ and $e(F/\mathbb{Q}_3) = 2$, so $t < \frac{3e(F/\mathbb{Q}_3)}{2} - 1$ and as it divides 2, $\mathcal{O}_L$ is $\mathfrak{A}_{L/F}$-free. Finally, if $L/\mathbb{Q}_3$ is weakly ramified and it is not totally ramified (the last polynomial), then $t = e(F/\mathbb{Q}_3) = 1$, so

$$\frac{3e(F/\mathbb{Q}_3)}{2} - 1 = \frac{3}{2} - 1 = \frac{1}{2}$$

and $t > \frac{1}{2}$. Since the expansion of $\frac{1}{3}$ is trivial, $\mathcal{O}_L$ is $\mathfrak{A}_{L/F}$-free.

In summary, we obtain:

Corollary 6.20. *Let $L/\mathbb{Q}_p$ be a dihedral degree $2p$ extension and let F be its unique subfield of degree p over $\mathbb{Q}_p$. Then, $\mathcal{O}_L$ is $\mathfrak{A}_{L/F}$-free.*

In particular, this result holds for $p = 3$ and $p = 5$, and for those cases we have obtained that $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free. Then, we have that Corollary 5.49 is valid for dihedral degree 6 and 10 extensions, even though $E/\mathbb{Q}_p$ and $F/\mathbb{Q}_p$ are not arithmetically disjoint. Then, Corollary 6.20 together with Theorems 6.14 and 6.16 suggest a connection between freeness and induced Hopf Galois structures stronger than arithmetic disjointness.

Conclusions

The initial and main aim of this project was to achieve a better comprehension of the Hopf Galois module structure of dihedral degree $2p$ extensions of p-adic fields. In general, for an H-Galois extension L/K of local or global fields, studying the Hopf Galois module structure means to provide answers to the following three questions:

1. Find an $\mathcal{O}_K$-basis of the associated order $\mathfrak{A}_H$.
2. Determine whether $\mathcal{O}_L$ is $\mathfrak{A}_H$-free or not.
3. If $\mathcal{O}_L$ is indeed $\mathfrak{A}_H$-free, find a free generator of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module.

The dichotomy of induced Hopf Galois structures

Recovering an expression used in Chapter 5, dihedral degree $2p$ extensions can be seen by *pieces*, i.e. $L = EF$ with E/K a separable degree p extension and F/K a quadratic extension, K-linearly disjoint with each other. It was the study of a particular degree 3 extension of $\mathbb{Q}_3$ that motivated the development of the reduction method, which is presented in all its generality in Chapter 2. The results therein show that the reduction method provides a complete answer to the three questions above whenever an integral basis and the action of H on this basis are known explicitly. In practice, these requirements reduce the range of its applicability to extensions of very low degree.

From a theoretical point of view, the reduction method is a key ingredient to prove the results of Chapter 5 concerning the induced Hopf Galois module structure of $\mathcal{O}_L$. These results show that the Hopf algebras and the actions of induced Hopf Galois structures also can be seen by pieces, as well as the associated order $\mathfrak{A}_H$ and the $\mathfrak{A}_H$-module structure of $\mathcal{O}_L$, when E/K and F/K are arithmetically disjoint. In this sense, the study of induced Hopf Galois structures translates the separation of L/K by pieces to the context of its Hopf Galois structures. For this reason, it could be preferable to talk about *products of Hopf Galois structures* rather than induced Hopf Galois structures.

Separable degree p extensions in literature: scaffolds

It is not the first time that the notion of the Hopf Galois module structure of a separable degree p extension appears in literature. In the paper [Eld18], Elder deals with what he calls typical degree p extensions: totally ramified degree p extensions L/K of local fields that **are not** generated by the p-th root of an uniformiser of K. The techniques used in that paper to study the Hopf Galois module structure of these extensions is the theory of scaffolds, which is developed in its most general form available in his paper [BCE18] with Byott and Childs. Roughly speaking, for a degree p^n totally ramified extension, a scaffold is a collection of elements $\{\Psi_i\}_{i=1}^n$ in an algebra A acting on L together with another collection $\{\lambda_t\}_{t\in\mathbb{Z}}$ of elements of L such that the valuations $v_L(\Psi_i \cdot \lambda_t)$ are determined with a prescribed precision.

In [Eld18, Corollary 3.6], Elder constructs a scaffold for any typical extension and uses it to provide criteria for the freeness of $\mathcal{O}_L$ as module over its associated order $\mathfrak{A}_H$ (and actually for an arbitrary fractional ideal in L instead of $\mathcal{O}_L$). A requirement to apply these criteria is that the ramification number l of L/K (see [Ser, Chapter IV §3 Remark 2] for the definition for a non-Galois extension) satisfies

$$l < \frac{pv_K(p)}{p-1} - 2.$$

In our case, following the classification in Theorem 4.5 of separable degree p extensions $E/\mathbb{Q}_p$, only the non-radical ones are typical (which is not a restriction if $p > 3$). By [Eld18, Theorem 2.2], $l = \frac{t}{2}$ where t is the ramification number of L/F. Recall that $t = 1$ (since we exclude the radical cases), so $l = \frac{1}{2}$. As for the right hand side, $\frac{pv_p(p)}{p-1} - 2 = -\frac{p-2}{p-1}$, so the inequality is never satisfied. This means that [Eld18, Corollary 3.6] cannot be applied to determine the $\mathfrak{A}_{H_1}$-freeness of $\mathcal{O}_E$. Hence, the results of Chapter 4 can be seen as the beginning of an extension of the results of Elder.

The results of the computations in Chapter 4 answer the three questions above for $p = 3$ and $p = 5$. The most important conclusion is that $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free for all cases that we have studied. Moreover, we have been able to show in Section 6.2.2 that the ramification of the extension L/F (and then the generalized ramification number of $E/\mathbb{Q}_p$) is always the same. The aforementioned result of Elder shows that there is a strong connection between the ramification of a typical degree p extension and the Hopf Galois module structure of its valuation ring. Then, it seems reasonable to expect that $\mathcal{O}_E$ is always $\mathfrak{A}_{H_1}$-free, or at least, that the behaviour is the same for the two totally ramified dihedral degree $2p$ extensions of $\mathbb{Q}_p$.

The likeness between degree p and $2p$ extensions

In Chapter 6, the results on the induced Hopf Galois module structure of a Hermite extension of fields made effective the step from separable degree p extensions with D_p-Galois closure to the Galois closure itself, and we were able to give complete answers again for $p = 3$ and $p = 5$. It is remarkable that the freeness of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module is the same as the one of $\mathcal{O}_E$ as $\mathfrak{A}_{H_1}$-module, which suggests that this relation could hold in the general case. But even more remarkable is the resemblance of the Hermite normal forms of $M(H_1, E)$ and $M(H, L)$. For instance, when $L/\mathbb{Q}_3$ is defined by $x^3 + 3x + 3$, we have:

$$D_E = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \qquad D_L = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

With our choice of bases of H_1, H_2, E and F, all our particular cases (except the radical ones if $p = 3$) satisfy the following:

- An entry 1 in the diagonal of D_E translates into a block $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in the diagonal of D_L.
- An entry p in the diagonal of D_E becomes a block $\begin{pmatrix} 1 & -1 \\ 0 & p \end{pmatrix}$ in the diagonal of D_L.
- An entry x over a p in the diagonal of D_E corresponds to a block $\begin{pmatrix} 0 & -x \\ 0 & -x \end{pmatrix}$ in the corresponding position of D_L.

Thus, even though $\mathfrak{A}_H \neq \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_p} \mathfrak{A}_{H_2}$, these rules translate into an alternative description of $\mathfrak{A}_H$ in terms of $\mathfrak{A}_{H_1}$ and $\mathfrak{A}_{H_2}$.

Quartic extensions: What is known and curiosities

The presence of Chapter 3 in this thesis responds to the necessity of testing the reduction method in a bunch of cases which are substantially different from dihedral degree $2p$ extensions. The most interesting result is the criteria obtained for the freeness of biquadratic extensions of $\mathbb{Q}$, which for each Hopf Galois structure depends on the existence of solutions of a generalized Pell equation. However, we obtained that $\mathcal{O}_L$ is free at every Hopf Galois structure for cyclic quartic extensions of $\mathbb{Q}$, as well as both cyclic and biquadratic extensions of $\mathbb{Q}_2$. We see that, as in the Galois case, H-Galois extensions L/K such that $\mathcal{O}_L$ is not $\mathfrak{A}_H$-free are not common.

Regarding the application of the techniques in Chapter 2 themselves, we can note that $D_\beta(H,L)$ is always a product of homogeneous polynomials on $\{\beta_i\}_{i=1}^4$ of degree at most 2. This behaviour also occurs in all examples of this thesis (for dihedral degree $2p$ extensions, $p \in \{3,5\}$, the maximal degree of the homogeneous polynomials is $p-1$). In the case of cyclic quartic extensions $\mathbb{Q}(\sqrt{a(d+b\sqrt{d})}/\mathbb{Q}$, this fact facilitated us to derive criteria for the freeness in terms of the parameters a, b, c and d. Another curious fact for those extensions is that for every $\beta \in \mathcal{O}_L$, $\beta_3^2+\beta_4^2$ is one of the factors of $D_\beta(H,L)$, unless d is odd and H is the classical Galois structure. As a consequence, in all these cases a free generator β must accomplish $\{|\beta_3|,|\beta_4|\}=\{0,1\}$.

Some precedent papers in the study of quartic extensions other than the already mentioned [Tru12] are [Eld98] or [BE02], which, for a biquadratic totally ramified extension L/K of number fields, give an explicit expression of $\mathcal{O}_L$ (or any fractional ideal) as $\mathbb{Z}[G]$-module. On the other hand, the Hopf Galois module structure of quartic Galois extensions has been studied as a particular case of the more general context of Galois degree p^2 extensions. For example, in [Byo02], Byott considers Galois degree p^2 extensions L/K of p-adic fields and gives a necessary and sufficient condition for $\mathcal{O}_L$ to be $\mathfrak{A}_H$-Galois for each Hopf Galois structure H of L/K. The definition of a Hopf Galois structure of an extension of rings is completely analogous to the case of fields (see for example [Chi00, Definition 2.7]). Galois degree p^2 of local fields with characteristic p are studied, among others, in the paper of Byott and Elder [BE13] and the thesis of Chetcharungkit [Che18], with the theory of scaffolds as main tool.

Future work

Most of the results in this thesis concerning the Hopf Galois module structure of rings of integers are only explicit for extensions of very low degree. We have seen that there are some patterns that could motivate more general results. Consequently, there are many open questions that could take part of future works. For instance:

- Is there an explicit relation between freeness over associated order and induced Hopf Galois structures? Theorem 5.47 is quite unsatisfactory because arithmetic disjointness is a very restrictive condition, but as aforesaid, freeness is preserved on induced Hopf Galois structures for dihedral degree 6 and 10 extensions.

- What about the associated order of an induced Hopf Galois structure $H = H_1 \otimes_K H_2$ in terms of the associated orders of H_1 and H_2? In this case, we obtained a sufficient condition for the equality $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$ stronger than arithmetic disjointness, namely the existence of integral induced bases (see Theorem 5.41). Is that condition necessary? If not, is there a characterization?

- How is the general behaviour in the Hopf Galois module structure of dihedral degree $2p$ extensions? Althought $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$ does not hold for all cases, there could be another relation.

- We have seen that bases of eigenvectors normally arise when the corresponding extensions are radical (see Examples 2.2, 2.45 and Section 4.4.2). Is there a general relation between these two notions?

It seems unlikely that the mere application of the reduction method will provide a complete answer to any of the questions above. However, it could be applied more efficiently to support or discard the corresponding suspicions. On the other hand, our techniques completely ignore the comultiplication, counit and coinverse operations of the Hopf algebras acting on fields, and perhaps one cannot dispense with this additional structure anymore to obtain further information. But at the same time, the techniques and results in this thesis bring to light the importance of the Hopf Galois representations of Hopf Galois structures, as well as the suitability of such objects to study the Hopf Galois module structure of rings of integers. Are they useful beyond the study of rings of integers? If so, it might be interesting to explore the development of a theory of Hopf Galois representations.

Appendix A

Separable degree p^n extensions with Frobenius Galois closure

Let p be an odd prime number and let $n \in \mathbb{Z}_{\geq 1}$. In this part we consider separable degree p^n extensions with Galois closure a Frobenius group, that is, of the form

$$G = J \rtimes G',$$

with J an order p^n normal subgroup of G and G' a subgroup of G with order r divisor of $p^n - 1$ (and then coprime with p). Since G is a Galois group, it is transitive. Let us assume that J and G' are cyclic, say $J = \langle \sigma \rangle$ and $G' = \langle \tau \rangle$. Then the group G has a presentation

$$G = \langle \sigma, \tau \,|\, \sigma^{p^n} = \tau^r = 1 \, \tau\sigma = \sigma^g \tau \rangle,$$

where g is an integer number of order r modulo p^n. Let $E = L^{G'}$ and $F = L^J$. By the fundamental theorem of Galois theory, $L = EF$ with E and F K-linearly disjoint.

We make an extra hypothesis: the extension F/K is Kummer, that is, K contains some (any) primitive r-th root of unity ζ_r. Consequently, there is an element $z \in F$ such that $z \notin K$ and $z^r \in K$. The conjugates of z are the elements $\zeta_r^l z$, with $0 \leq l \leq r-1$. On the other hand, $E = K(\alpha)$ with α a root of an irreducible degree p^n polynomial f. We may assume without loss of generality that $\tau(z) = \zeta_r^g z$ (otherwise we would replace either τ or ζ_r by a suitable power).

Now p^n is not a Burnside number unless $n = 1$, so the extension E/K does not need to have a unique Hopf Galois structure. But we may choose a distinguished one: its almost classically Galois structure (which is indeed the unique one if $n = 1$). If $\lambda \colon G \longrightarrow \mathrm{Perm}(G/G')$ is the left translation map, that structure is the one given by the subgroup $N_1 = \lambda(J)$ of $\mathrm{Perm}(G/G')$ (note that $N_1^{\mathrm{opp}} = N_1$ because N_1 is abelian). Its Hopf algebra is

$$H_1 = L[N_1]^G = \{x \in L[N_1] : \, g(x) = x \text{ for all } g \in G\}.$$

Let $\mu = \lambda(\sigma)$. It is easily verified that

$$\sigma(\mu) = \mu, \, \tau(\mu) = \mu^g.$$

Theorem A.1. *Assume that J and G' are cyclic groups. The Hopf algebra H_1 has a K-basis formed by the identity* Id *and the elements*

$$w_{jk} = z^j \left(\sum_{l=0}^{r-1} \zeta_r^{lj} \mu^{g^l i_k} \right), \, 0 \leq j \leq r-1, \, 1 \leq k \leq a,$$

where $a = \frac{p^n-1}{r}$ and $\{i_1, ..., i_a\}$ is a system of representatives of the orbits of the action of g on $\mathbb{Z}/p^n\mathbb{Z}$.

Proof. Let us take $x \in H_1$. Then $x = \sum_{i=0}^{p^n-1} x_i\mu^i$ with $x_i \in L$ and $g(x) = x$ for all $g \in G$. In particular, we have

$$\sum_{i=0}^{p^n-1} x_i\mu^i = \sigma\left(\sum_{i=0}^{p^n-1} x_i\mu^i\right) = \sum_{i=0}^{p^n-1} \sigma(x_i)\mu^i,$$

which implies that $x_i = \sigma(x_i)$ for all $0 \leq i \leq p^n - 1$. That is, $x_i \in F$ for every $0 \leq i \leq p^n - 1$. Hence,

$$x_i = \sum_{j=0}^{r-1} x_{ij}z^j,\ x_{ij} \in K.$$

On the other hand,

$$\begin{aligned}\sum_{i=0}^{p^n-1} x_i\mu^i &= \tau\left(\sum_{i=0}^{p^n-1} x_i\mu^i\right)\\ &= \sum_{i=0}^{p^n-1} \tau(x_i)\mu^{gi}.\end{aligned}$$

We deduce that $\tau(x_i) = x_{gi}$ for every $0 \leq i \leq p^n - 1$. In particular, for $i = 0$, $\tau(x_0) = x_0$, so $x_0 \in K$. We focus in the other terms. For $i > 0$, we have that

$$\sum_{j=0}^{r-1} x_{gi,j}z^j = x_{gi} = \tau(x_i) = \sum_{j=0}^{r-1} x_{ij}\zeta_r^j z^j,$$

whence $x_{gi,j} = x_{ij}\zeta_r^j$. By induction, one has

$$x_{g^l i,j} = x_{ij}\zeta_r^{lj} \tag{A.1}$$

for every $1 \leq i \leq p^n - 1$, $0 \leq j \leq r - 1$ and $0 \leq l \leq r - 1$, where the left index is taken modulo p^n. Now, we have

$$\begin{aligned}x &= \sum_{i=0}^{p^n-1} x_i\mu^i\\ &= x_0\mathrm{Id} + \sum_{i=1}^{p^n-1}\sum_{j=0}^{r-1} x_{ij}z^j\mu^i.\end{aligned}$$

At this point, we must group the addends which have the same coefficient x_{ij}, taking (A.1) into account. The subgroup $\langle g\rangle$ of $\mathbb{Z}$ acts transitively on $\mathbb{Z}/p^n\mathbb{Z} - \{0\}$ by means of $g(\overline{x}) = \overline{gx}$. Let a be the positive integer such that $p^n - 1 = ar$. Then the action of $\langle g\rangle$ on $\mathbb{Z}/p^n\mathbb{Z} - \{0\}$ yields a orbits of r elements each. Let $\{i_1, ..., i_a\}$ be a system of representatives of the orbits of such action. Then,

$$\begin{aligned}x - x_0\mathrm{Id} &= \sum_{k=1}^{a}\sum_{l=0}^{r-1}\sum_{j=0}^{r-1} x_{g^l i_k,j}z^j\mu^{g^l i_k}\\ &= \sum_{k=1}^{a}\sum_{l=0}^{r-1}\sum_{j=0}^{r-1} x_{i_k,j}\zeta_r^{lj}\mu^{g^l i_k}\\ &= \sum_{j=0}^{r-1}\sum_{k=1}^{a} x_{i_k,j}z^j\left(\sum_{l=0}^{r-1}\zeta_r^{lj}\mu^{g^l i_k}\right).\end{aligned}$$

We obtain that

$$\{\mathrm{Id}\} \cup \left\{ z^j \left(\sum_{l=0}^{r-1} \xi_r^{lj} \mu^{g^l i_k} \right) \,\middle|\, 0 \leq j \leq r-1,\, 1 \leq k \leq a \right\}$$

is a system of generators of H_1. Since $ar = p^n - 1$, it has p^n elements in total, and all of them are K-linearly independent. Hence, they form a K-basis of H_1. □

Example A.2. If we choose $n = 1$ and $r = 2$, we recover Theorem 4.1. Indeed, in that case every field contains the primitive square root of unity, which is -1, and since $g = -1$, the action of $\langle g \rangle$ on $\mathbb{Z}/p\mathbb{Z}^*$ has $a = \frac{p-1}{2}$ orbits with 2 elements each. We take as representatives $\{1, 2, \dots, \frac{p-1}{2}\}$. Then, the non-trivial basic elements according to Theorem A.1 are

$$w_{jk} = z^j \left(\sum_{l=0}^{1} (-1)^{lj} \mu^{(-1)^l k} \right)$$

for $j \in \{0, 1\}$ and $1 \leq k \leq \frac{p-1}{2}$. Then,

$$w_{0k} = \mu^k + \mu^{-k}, \quad w_{1k} = z(\mu^k - \mu^{-k}),$$

for every $1 \leq k \leq \frac{p-1}{2}$, which are the basic elements in Theorem 4.1.

Example A.3. Let us pick $p = 5$, $n = 1$, $r = 4$, which means that the Galois group of the normal closure of E/K is the Frobenius group F_5 of order 20. In this case, $g = 2$ is an element of order 4 modulo 5. Its action on $\mathbb{Z}/5\mathbb{Z}$ yields one orbit of 4 elements, which is $\{1, 2, 4, 3\}$. Moreover, $\xi_4 = i$ (a root of $x^2 + 1$) is a primitive 4-th root of unity. We obtain the non-trivial basic elements

$$w_{01} = \mu + \mu^2 + \mu^3 + \mu^4, \qquad w_{11} = (\mu + i\mu^2 - i\mu^3 - \mu^4)z,$$

$$w_{21} = (\mu - \mu^2 - \mu^3 + \mu^4)z, \qquad w_{31} = (\mu - i\mu^2 + i\mu^3 - \mu^4)z^3.$$

As a final remark, if we assume that the extension E/K is of p-adic fields, then K contains the primitive r-th roots of unity, because r is coprime with p and one can apply Hensel's lemma. Then, we can use Theorem A.1 to describe its almost classically Galois structure.

Appendix B

Complete form of some items

Quartic Galois extensions of $\mathbb{Q}$

For a Hopf Galois structure A, $U(A,L)$ is the matrix that reduces $M(A,L)$ to a reduced matrix or a previous form.

Cyclic quartic extensions

Case 1

$$U(H,L)=\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&-1&0&0&0&0&0\\
1&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&-1&0&0&0&0&1
\end{pmatrix} \tag{B.1}$$

Case 2

$$U(H,L) = \begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} \tag{B.2}$$

Case 3

$$U(H,L) = \begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} \tag{B.3}$$

Case 4

$$U(H,L) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & -2 & -2 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 4 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{B.4}$$

Case 5

$$U(H,L) = \begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & -2 & -2 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 4 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 1 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \tag{B.5}$$

Biquadratic extensions

Case 1

$$U(H_1, L) = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 1
\end{pmatrix} \tag{B.6}$$

$$U(H_2, L) = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 & 1
\end{pmatrix} \tag{B.7}$$

$$U(H_3, L) = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -2 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 & 1
\end{pmatrix} \tag{B.8}$$

Case 2

$$U(H_1, L) = \begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 3 & 2 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & -2 & -1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \tag{B.9}$$

$$U(H_2, L) = \begin{pmatrix}
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & -3 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 & 0 \\
2 & 0 & 0 & 0 & -3 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2d & d & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & -2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-2 & 0 & 0 & 0 & 4 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -2 & 0 \\
1 & 0 & 0 & 0 & -2 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 & 1
\end{pmatrix} \tag{B.10}$$

$$U(H_3, L) = \begin{pmatrix}
1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -2 & 0 & 0 \\
1 & 0 & 0 & 0 & -2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & -4 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & -2 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 2 & 1
\end{pmatrix} \tag{B.11}$$

Case 3

$$U(H_c, L) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & 0 & 4 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -3 & 0 & 0 & 0 & 4 & 2 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \end{pmatrix} \tag{B.12}$$

$$U(H_1, L) = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & -\frac{m}{d} & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \end{pmatrix} \tag{B.13}$$

$$U(H_2, L) =$$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & \frac{d+3m}{2d} & 0 & 0 & -\frac{d+m}{2d} & -\frac{d+3m}{2d} & 0 & 0 & 0 & -3 & -2 & -3 & 0 \\
0 & 0 & 0 & 0 & \frac{-3(d+3m)}{2d} & 0 & 0 & \frac{d+3m}{2d} & \frac{-d+9m}{2d} & 0 & 0 & 0 & 5 & 2 & 7 & 0 \\
0 & 0 & 0 & 0 & \frac{-3(d+m)}{2d} & 0 & 0 & \frac{d+m}{2d} & \frac{d+3m}{2d} & 0 & 0 & 0 & 3 & 2 & 3 & 0 \\
-1 & 0 & 0 & 0 & -2 & 0 & 3 & \frac{d+2m}{d} & 0 & 0 & 0 & 0 & 8 & 6 & 4 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & -1 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & -2 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 4 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & -4 & -2 & -2 & 0 \\
0 & 0 & 0 & 0 & 4 & 1 & 2 & 0 & -2 & 0 & -1 & 0 & -4 & -2 & -2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{m}{d} & 0 & 0 & 0 & -2\,\frac{m}{d} & -\frac{m}{d} & \frac{d-m}{d} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-2 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 0 & 4 & 2 & 2 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \tag{B.14}$$

$$U(H_3, L) =$$

$$\begin{pmatrix}
0 & 0 & 0 & 0 & \frac{3\,d-m}{2d} & 1 & \frac{d-m}{2d} & 0 & \frac{-d+m}{2d} & 0 & 0 & 0 & -1 & \frac{-d-m}{2d} & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{3\,d-m}{2d} & 0 & \frac{d-m}{2d} & 0 & \frac{-d+m}{2d} & 0 & 0 & 0 & -1 & \frac{-d-m}{2d} & 0 & 0 \\
0 & 0 & 0 & 0 & \frac{d+m}{2d} & 0 & \frac{d+m}{2d} & 0 & \frac{-d-m}{2d} & 0 & 0 & 0 & 1 & \frac{d+m}{2d} & 0 & 0 \\
-\frac{m}{d} & -\frac{m}{d} & 0 & 0 & \frac{d+m}{d} & \frac{m}{d} & 0 & 0 & \frac{m}{d} & 0 & 0 & 0 & -2 & -\frac{m}{d} & 0 & 0 \\
-\frac{m}{d} & 0 & 0 & 0 & \frac{d+m}{d} & \frac{m}{d} & 0 & 0 & \frac{m}{d} & 0 & 0 & 0 & -2 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
-\frac{m}{d} & 2 & 0 & 0 & 0 & -1 & 0 & 0 & 2\,\frac{m}{d} & 0 & \frac{m}{d} & 0 & 0 & 2 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \tag{B.15}$$

Separable degree 5 extensions with Galois closure D_{10}

Matrices of the action

$f(x) = x^5 + 15x^2 + 5:$

$$M(H_1, E) = \frac{1}{6}\begin{pmatrix}
6 & 0 & 0 & 12 & 12 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & -30 & -30 & 30 & -30 \\
6 & -110 & -270 & -18 & 12 \\
0 & -25 & -75 & -11 & 11 \\
0 & 15 & 25 & 1 & -1 \\
0 & 3 & 11 & 1 & -1 \\
0 & 120 & -360 & 120 & 60 \\
0 & 205 & -15 & 45 & -45 \\
6 & 55 & 55 & 7 & -13 \\
0 & -25 & 5 & -5 & 5 \\
0 & -10 & 0 & -2 & 2 \\
0 & 150 & 750 & 210 & -30 \\
0 & -245 & -1815 & -285 & 285 \\
0 & -160 & -700 & -110 & 110 \\
6 & 60 & 150 & 22 & -28 \\
0 & 15 & 85 & 13 & -13 \\
0 & 450 & -5250 & 1110 & -210 \\
0 & -1100 & -2250 & 600 & -600 \\
0 & -135 & 255 & 55 & -55 \\
0 & 85 & 295 & -65 & 65 \\
6 & -5 & 65 & -23 & 17
\end{pmatrix}. \tag{B.16}$$

$f(x) = x^5 + 10x^2 + 5:$

$$M(H_1, E) = \frac{1}{42} \begin{pmatrix} 42 & 0 & 0 & 84 & 84 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -3570 & -190 & -170 & 170 \\ 42 & 735 & -2195 & -1 & -41 \\ 0 & 420 & 260 & 16 & -16 \\ 0 & 210 & 110 & 10 & -10 \\ 0 & 21 & 53 & 1 & -1 \\ 0 & 10160 & 2180 & -160 & 160 \\ 0 & -14975 & -275 & 655 & -655 \\ 42 & 830 & 1040 & -106 & 64 \\ 0 & 440 & 20 & -40 & 40 \\ 0 & 485 & 65 & -25 & 25 \\ 0 & -3000 & 13850 & 3380 & 1030 \\ 0 & 29790 & 17320 & -830 & 830 \\ 0 & -3930 & -6010 & 50 & -50 \\ 42 & -1800 & -2050 & -16 & -26 \\ 0 & -1020 & -730 & 32 & -32 \\ 0 & -128150 & -15650 & -9990 & 1590 \\ 0 & 34625 & -109675 & -375 & 375 \\ 0 & 15520 & 15160 & 540 & -540 \\ 0 & 6550 & 6850 & 390 & -390 \\ 42 & 235 & 3205 & 39 & -81 \end{pmatrix} \tag{B.17}$$

$f(x) = x^5 + 5x^4 + 5:$

$$M(H_1, E) = \frac{1}{22}\begin{pmatrix}
22 & 0 & 0 & 44 & 44 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 720 & 120 & -40 & -180 \\
22 & 895 & 415 & 199 & -221 \\
0 & 402 & 254 & 150 & -150 \\
0 & 86 & 62 & 38 & -38 \\
0 & 9 & 7 & 5 & -5 \\
0 & -4410 & -330 & -830 & 830 \\
0 & -6025 & -1155 & -1555 & 1555 \\
22 & -2960 & -550 & -996 & 974 \\
0 & -656 & -132 & -240 & 240 \\
0 & -73 & -11 & -31 & 31 \\
0 & 11520 & -2010 & 6020 & -3270 \\
0 & 17950 & -3500 & 6510 & -6510 \\
0 & 9930 & -2830 & 3550 & -3550 \\
22 & 2300 & -670 & 804 & -826 \\
0 & 276 & -98 & 100 & -100 \\
0 & 16620 & 23040 & -19700 & 6500 \\
0 & 10535 & 46845 & -11525 & 11525 \\
0 & -1550 & 28550 & -3730 & 3730 \\
0 & -950 & 6690 & -590 & 590 \\
22 & -235 & 805 & -51 & 29
\end{pmatrix} \tag{B.18}$$

Non-constant factors of $D_\epsilon(H_1, E)$

$f(x) = x^5 + 15x^2 + 5$:

$$
\begin{aligned}
& q_1(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4,\epsilon_5) = -\frac{1}{27}\Big(11\,\epsilon_2{}^4 + 35\,\epsilon_2{}^3\epsilon_3 + 215\,\epsilon_2{}^3\epsilon_4 + 830\,\epsilon_2{}^3\epsilon_5 - 75\,\epsilon_2{}^2\epsilon_3{}^2 \\
& + 795\,\epsilon_2{}^2\epsilon_3\,\epsilon_4 - 465\,\epsilon_2{}^2\epsilon_3\,\epsilon_5 + 1080\,\epsilon_2{}^2\epsilon_4{}^2 + 16485\,\epsilon_2{}^2\epsilon_4\,\epsilon_5 + 9000\,\epsilon_2{}^2\epsilon_5{}^2 \\
& + 5\,\epsilon_2\,\epsilon_3{}^3 - 615\,\epsilon_2\,\epsilon_3{}^2\epsilon_4 - 1650\,\epsilon_2\,\epsilon_3{}^2\epsilon_5 + 4080\,\epsilon_2\,\epsilon_3\,\epsilon_4{}^2 + 8550\,\epsilon_2\,\epsilon_3\,\epsilon_4\,\epsilon_5 \\
& - 30075\,\epsilon_2\,\epsilon_3\,\epsilon_5{}^2 + 200\,\epsilon_2\,\epsilon_4{}^3 + 79650\,\epsilon_2\,\epsilon_4{}^2\epsilon_5 + 240525\,\epsilon_2\,\epsilon_4\,\epsilon_5{}^2 - 112750\,\epsilon_2\,\epsilon_5{}^3 \\
& + 5\,\epsilon_3{}^4 - 205\,\epsilon_3{}^3\epsilon_4 + 725\,\epsilon_3{}^3\epsilon_5 + 1680\,\epsilon_3{}^2\epsilon_4{}^2 - 24975\,\epsilon_3{}^2\epsilon_4\,\epsilon_5 + 18825\,\epsilon_3{}^2\epsilon_5{}^2 \\
& - 3430\,\epsilon_3\,\epsilon_4{}^3 + 135450\,\epsilon_3\,\epsilon_4{}^2\epsilon_5 - 373725\,\epsilon_3\,\epsilon_4\,\epsilon_5{}^2 + 148625\,\epsilon_3\,\epsilon_5{}^3 - 1045\,\epsilon_4{}^4 \\
& - 16600\,\epsilon_4{}^3\epsilon_5 + 1473450\,\epsilon_4{}^2\epsilon_5{}^2 - 1173625\,\epsilon_4\,\epsilon_5{}^3 + 210125\,\epsilon_5{}^4\Big)\,(\epsilon_1 + 6\,\epsilon_3 + 6\,\epsilon_4 + 30\,\epsilon_5)\,.
\end{aligned}
\tag{B.19}
$$

$f(x) = x^5 + 10x^2 + 5$:

$$
\begin{aligned}
& q_2(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4,\epsilon_5) = -\frac{1}{21}\Big(50\,\epsilon_2{}^4 - 750\,\epsilon_2{}^3\epsilon_3 - 500\,\epsilon_2{}^3\epsilon_4 + 13000\,\epsilon_2{}^3\epsilon_5 \\
& - 24250\,\epsilon_2{}^2\epsilon_3{}^2 + 99250\,\epsilon_2{}^2\epsilon_3\,\epsilon_4 - 61250\,\epsilon_2{}^2\epsilon_3\,\epsilon_5 - 77500\,\epsilon_2{}^2\epsilon_4{}^2 - 218000\,\epsilon_2{}^2\epsilon_4\,\epsilon_5 \\
& + 1137500\,\epsilon_2{}^2\epsilon_5{}^2 + 48750\,\epsilon_2\,\epsilon_3{}^3 + 21250\,\epsilon_2\,\epsilon_3{}^2\epsilon_4 - 1792500\,\epsilon_2\,\epsilon_3{}^2\epsilon_5 - 597750\,\epsilon_2\,\epsilon_3\,\epsilon_4{}^2 \\
& + 7095000\,\epsilon_2\,\epsilon_3\,\epsilon_4\,\epsilon_5 - 1711250\,\epsilon_2\,\epsilon_3\,\epsilon_5{}^2 + 628750\,\epsilon_2\,\epsilon_4{}^3 - 4655000\,\epsilon_2\,\epsilon_4{}^2\epsilon_5 \\
& - 14302500\,\epsilon_2\,\epsilon_4\,\epsilon_5{}^2 + 40375000\,\epsilon_2\,\epsilon_5{}^3 - 23750\,\epsilon_3{}^4 - 97500\,\epsilon_3{}^3\epsilon_4 + 1756250\,\epsilon_3{}^3\epsilon_5 \\
& + 900000\,\epsilon_3{}^2\epsilon_4{}^2 - 908750\,\epsilon_3{}^2\epsilon_4\,\epsilon_5 - 31756250\,\epsilon_3{}^2\epsilon_5{}^2 - 1651250\,\epsilon_3\,\epsilon_4{}^3 \\
& - 15948750\,\epsilon_3\,\epsilon_4{}^2\epsilon_5 + 125468750\,\epsilon_3\,\epsilon_4\,\epsilon_5{}^2 - 18518750\,\epsilon_3\,\epsilon_5{}^3 + 907250\,\epsilon_4{}^4 \\
& + 18321250\,\epsilon_4{}^3\epsilon_5 - 73877500\,\epsilon_4{}^2\epsilon_5{}^2 - 240725000\,\epsilon_4\,\epsilon_5{}^3 + 495931250\,\epsilon_5{}^4\Big) \\
& (\epsilon_1 + 21\,\epsilon_4 - 40\,\epsilon_5)\,.
\end{aligned}
\tag{B.20}
$$

$f(x) = x^5 + 5x^4 + 5$:

$$
\begin{aligned}
& q_3(\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4,\epsilon_5) = \frac{1}{11}(\epsilon_1 - 2\,\epsilon_2 + 25\,\epsilon_4 - 120\,\epsilon_5)\Big(\epsilon_2{}^4 - 25\,\epsilon_2{}^3\epsilon_3 + 70\,\epsilon_2{}^3\epsilon_4 + 50\,\epsilon_2{}^3\epsilon_5 \\
& + 215\,\epsilon_2{}^2\epsilon_3{}^2 - 1035\,\epsilon_2{}^2\epsilon_3\,\epsilon_4 - 1895\,\epsilon_2{}^2\epsilon_3\,\epsilon_5 + 810\,\epsilon_2{}^2\epsilon_4{}^2 + 10050\,\epsilon_2{}^2\epsilon_4\,\epsilon_5 - 13300\,\epsilon_2{}^2\epsilon_5{}^2 \\
& - 755\,\epsilon_2\,\epsilon_3{}^3 + 4585\,\epsilon_2\,\epsilon_3{}^2\epsilon_4 + 15000\,\epsilon_2\,\epsilon_3{}^2\epsilon_5 - 4725\,\epsilon_2\,\epsilon_3\,\epsilon_4{}^2 - 115900\,\epsilon_2\,\epsilon_3\,\epsilon_4\,\epsilon_5 \\
& + 70725\,\epsilon_2\,\epsilon_3\,\epsilon_5{}^2 - 3275\,\epsilon_2\,\epsilon_4{}^3 + 144750\,\epsilon_2\,\epsilon_4{}^2\epsilon_5 + 230050\,\epsilon_2\,\epsilon_4\,\epsilon_5{}^2 - 949250\,\epsilon_2\,\epsilon_5{}^3 \\
& + 895\,\epsilon_3{}^4 - 5600\,\epsilon_3{}^3\epsilon_4 - 32525\,\epsilon_3{}^3\epsilon_5 + 650\,\epsilon_3{}^2\epsilon_4{}^2 + 293025\,\epsilon_3{}^2\epsilon_4\,\epsilon_5 + 38925\,\epsilon_3{}^2\epsilon_5{}^2 \\
& + 30575\,\epsilon_3\,\epsilon_4{}^3 - 496025\,\epsilon_3\,\epsilon_4{}^2\epsilon_5 - 2641125\,\epsilon_3\,\epsilon_4\,\epsilon_5{}^2 + 4970875\,\epsilon_3\,\epsilon_5{}^3 - 20225\,\epsilon_4{}^4 \\
& - 212875\,\epsilon_4{}^3\epsilon_5 + 6795500\,\epsilon_4{}^2\epsilon_5{}^2 - 10711250\,\epsilon_4\,\epsilon_5{}^3 - 8010125\,\epsilon_5{}^4\Big)\,.
\end{aligned}
\tag{B.21}
$$

Weakly ramified dihedral degree 6 extensions

Gram matrices

$f(x) = x^3 + 3x + 3:$

$$G(H_W, L_B) = \begin{pmatrix} 1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 \\ 1 & -\gamma & \gamma^2 & -\gamma^3 & \gamma^4 & -\gamma^5 \\ 0 & g_{32} & g_{33} & g_{34} & g_{35} & g_{36} \\ 0 & g_{42} & g_{43} & g_{44} & g_{45} & g_{46} \\ 2 & g_{52} & -\gamma^2 - 3 & g_{54} & -\gamma^4 + 21 & g_{56} \\ 2 & g_{62} & -\gamma^2 - 3 & g_{64} & -\gamma^4 + 21 & g_{66} \end{pmatrix} \tag{B.22}$$

$$g_{32} = -\gamma^5 - 6\gamma^3 - 12\gamma, \quad g_{33} = 18\gamma^4 + 69\gamma^2 - 57, \quad g_{34} = -12\gamma^5 - 33\gamma^3 + 90\gamma,$$
$$g_{35} = -69\gamma^4 - 258\gamma^2 + 225, \quad g_{36} = 45\gamma^5 + 114\gamma^3 - 396\gamma,$$
$$g_{42} = \gamma^5 + 6\gamma^3 + 12\gamma, \quad g_{43} = 18\gamma^4 + 69\gamma^2 - 57, \quad g_{44} = 12\gamma^5 + 33\gamma^3 - 90\gamma,$$
$$g_{45} = -69\gamma^4 - 258\gamma^2 + 225, \quad g_{46} = -45\gamma^5 - 114\gamma^3 + 396\gamma,$$
$$g_{52} = -\gamma^5 - 4\gamma^3 + 2\gamma, \quad g_{54} = 6\gamma^5 + 23\gamma^3 - 18\gamma, \quad g_{56} = -25\gamma^5 - 96\gamma^3 + 72\gamma,$$
$$g_{62} = \gamma^5 + 4\gamma^3 - 2\gamma, \quad g_{64} = -6\gamma^5 - 23\gamma^3 + 18\gamma, \quad g_{66} = 25\gamma^5 + 96\gamma^3 - 72\gamma.$$

$f(x) = x^3 + 6x + 3:$

$$G(H_W, L_B) = \begin{pmatrix} 1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 \\ 1 & -\gamma & \gamma^2 & -\gamma^3 & \gamma^4 & -\gamma^5 \\ 0 & g_{32} & g_{33} & g_{34} & g_{35} & g_{36} \\ 0 & g_{42} & g_{43} & g_{44} & g_{45} & g_{46} \\ 2 & g_{52} & -\gamma^2 + 12 & g_{54} & -\gamma^4 + 168 & g_{56} \\ 2 & g_{62} & -\gamma^2 + 12 & g_{64} & -\gamma^4 + 168 & g_{66} \end{pmatrix} \tag{B.23}$$

$$g_{32} = -4\gamma^5 + 54\gamma^3 - 33\gamma, \quad g_{33} = -120\gamma^4 + 1497\gamma^2 + 732, \quad g_{34} = 66\gamma^5 - 768\gamma^3 - 1116\gamma,$$
$$g_{35} = -1497\gamma^4 + 18672\gamma^2 + 9144, \quad g_{36} = 801\gamma^5 - 9276\gamma^3 - 14148\gamma,$$
$$g_{42} = 4\gamma^5 - 54\gamma^3 + 33\gamma, \quad g_{43} = -120\gamma^4 + 1497\gamma^2 + 732, \quad g_{44} = -66\gamma^5 + 768\gamma^3 + 1116\gamma,$$
$$g_{45} = -1497\gamma^4 + 18672\gamma^2 + 9144, \quad g_{46} = -801\gamma^5 + 9276\gamma^3 + 14148\gamma,$$
$$g_{52} = -4\gamma^5 + 50\gamma^3 + 23\gamma, \quad g_{54} = -54\gamma^5 + 674\gamma^3 + 324\gamma,$$
$$g_{56} = -697\gamma^5 + 8700\gamma^3 + 4176\gamma, \quad g_{62} = 4\gamma^5 - 50\gamma^3 - 23\gamma,$$
$$g_{64} = 54\gamma^5 - 674\gamma^3 - 324\gamma, \quad g_{66} = 697\gamma^5 - 8700\gamma^3 - 4176.$$

Dihedral degree 10 extensions

Powers of γ

$f(x) = x^5 + 15x^2 + 5$:

$$
\begin{aligned}
\gamma^2 &= 403\,\alpha^4 - 158\,\alpha^3 - 5985\,\alpha^2 - 1684\,\alpha + 30905,\\
\gamma^3 &= 2420195tz - 132252tz\alpha - 468843tz\alpha^2 - 12362tz\alpha^3 + \frac{157893tz\alpha^4}{5},\\
\gamma^4 &= 12365479\,\alpha^4 - 4840390\,\alpha^3 - 183587469\,\alpha^2 - 51790660\,\alpha + 947684245,\\
\gamma^5 &= 968400509tz\alpha^4 - 379073698tz\alpha^3 - 14377621887tz\alpha^2 - 4055984300tz\alpha\\
&\quad + 74217725527tz,\\
\gamma^6 &= 379200596235\,\alpha^4 - 148435451054\,\alpha^3 - 5629904912985\,\alpha^2\\
&\quad - 1588218618420\,\alpha + 29061741914945,\\
\gamma^7 &= 29697029362313tz\alpha^4 - 11624696765978tz\alpha^3 - 440905033279875tz\alpha^2\\
&\quad - 124381067546108tz\alpha + 2275965310877435tz,\\
\gamma^8 &= 1162858868947939\,1\alpha^4 - 4551930621754870\,\alpha^3 - 172647008580452085\,\alpha^2\\
&\quad - 48704409374429540\,\alpha + 891209155931710525,\\
\gamma^9 &= 9106909196814823\,41tz\alpha^4 - 356483662372684210tz\alpha^3\\
&\quad - 13520820730948482423tz\alpha^2 - 3814277428685618700tz\alpha\\
&\quad + 69794891496872592655tz.
\end{aligned}
\tag{B.24}
$$

$f(x) = x^5 + 10x^2 + 5$:

$$
\begin{aligned}
\gamma^2 &= 780\,\alpha^4 - 256\,\alpha^3 + 80\,\alpha^2 - 27332\,\alpha + 47960,\\
\gamma^3 &= \frac{294464tz\alpha^4}{5} - 19184tz\alpha^3 + 6240tz\alpha^2 - 2063296tz\alpha + 3616720tz,\\
\gamma^4 &= 44420384\,\alpha^4 - 14466880\,\alpha^3 + 4711424\,\alpha^2 - 1556248160\,\alpha + 2727859200,\\
\gamma^5 &= 3350358464tz\alpha^4 - 1091143680tz\alpha^3 + 355363072tz\alpha^2 - 117378281280tz\alpha\\
&\quad + 205745643392tz,\\
\gamma^6 &= 252696955904\,0\alpha^4 - 822982573568\,\alpha^3 + 268028677120\,\alpha^2 - 88531226060800\,\alpha\\
&\quad + 155181297072640,\\
\gamma^7 &= 190593787496960tz\alpha^4 - 62072518829056tz\alpha^3 + 20215756472320tz\alpha^2\\
&\quad - 6677366422982144tz\alpha + 11704371763281920tz,\\
\gamma^8 &= 143753183324747776\,\alpha^4 - 46817487053127680\,\alpha^3 + 15247502999756800\,\alpha^2\\
&\quad - 5036327217872496640\,\alpha + 8827888473614643200,\\
\gamma^9 &= 108424193607636418\,56tz\alpha^4 - 35311553894458572\,80tz\alpha^3\\
&\quad + 11500254665979822\,08tz\alpha^2 - 3798592175231524864\,00tz\alpha\\
&\quad + 6658333866927851520\,00tz.
\end{aligned}
\tag{B.25}
$$

Product of generators

$f(x) = x^5 + 15x^2 + 5:$

$$\beta' = \begin{pmatrix} \epsilon_1\,\delta_1 + \frac{1716415065\,\epsilon_2\,\delta_1}{642386524} + \frac{344708445\,\epsilon_3\,\delta_1}{24707174} + \frac{13637321545\,\epsilon_4\,\delta_1}{642386524} + 150\,\epsilon_5\,\delta_1 \\ \frac{114902815\,\epsilon_1\,\delta_2}{98828696\,t} + \frac{13637321545\,\epsilon_2\,\delta_2}{7708638288\,t} + \frac{25}{2}\,\frac{\epsilon_3\,\delta_2}{t} + \frac{3045443610\,\epsilon_4\,\delta_2}{160596631\,t} + \frac{33002652875\,\epsilon_5\,\delta_2}{296486088\,t} \\ -\frac{1236455183\,\epsilon_2\,\delta_1}{5139092192} - \frac{3740722775\,\epsilon_3\,\delta_1}{3557833056} - \frac{12064716635\,\epsilon_4\,\delta_1}{30834553152} - \frac{805\,\epsilon_5\,\delta_1}{48} \\ -\frac{3740722775\,\epsilon_1\,\delta_2}{42693996672\,t} - \frac{12064716635\,\epsilon_2\,\delta_2}{370014637824\,t} - \frac{805\,\epsilon_3\,\delta_2}{576\,t} + \frac{153714326975\,\epsilon_4\,\delta_2}{1110043913472\,t} - \frac{25112657245\,\epsilon_5\,\delta_2}{1778916528\,t} \\ \frac{429885670895\,\epsilon_2\,\delta_1}{6660263480832} + \frac{15317808053\,\epsilon_3\,\delta_1}{170775986688} + \frac{1690569125905\,\epsilon_4\,\delta_1}{4440175653888} + \frac{18155\,\epsilon_5\,\delta_1}{10368} \\ \frac{15317808053\,\epsilon_1\,\delta_2}{2049311840256\,t} + \frac{1690569125905\,\epsilon_2\,\delta_2}{53282107846656\,t} + \frac{18155\,\epsilon_3\,\delta_2}{124416\,t} + \frac{2615627812535\,\epsilon_4\,\delta_2}{17760702615552\,t} + \frac{457036180625\,\epsilon_5\,\delta_2}{256163980032\,t} \\ -\frac{861830682163\,\epsilon_2\,\delta_1}{213128431386624} - \frac{5731464085\,\epsilon_3\,\delta_1}{1366207893504} - \frac{1203824325611\,\epsilon_4\,\delta_1}{35521405231104} - \frac{30685\,\epsilon_5\,\delta_1}{331776} \\ -\frac{5731464085\,\epsilon_1\,\delta_2}{16394494722048\,t} - \frac{1203824325611\,\epsilon_2\,\delta_2}{426256862773248\,t} - \frac{30685\,\epsilon_3\,\delta_2}{3981312\,t} - \frac{5849774679485\,\epsilon_4\,\delta_2}{284171241848832\,t} - \frac{3525523930915\,\epsilon_5\,\delta_2}{32788989444096\,t} \\ \frac{28089103\,\epsilon_2\,\delta_1}{213128431386624} + \frac{186769\,\epsilon_3\,\delta_1}{1366207893504} + \frac{39241535\,\epsilon_4\,\delta_1}{35521405231104} + \frac{\epsilon_5\,\delta_1}{331776} \\ \frac{186769\,\epsilon_1\,\delta_2}{16394494722048\,t} + \frac{39241535\,\epsilon_2\,\delta_2}{426256862773248\,t} + \frac{\epsilon_3\,\delta_2}{3981312\,t} + \frac{190712785\,\epsilon_4\,\delta_2}{284171241848832\,t} + \frac{114902815\,\epsilon_5\,\delta_2}{32788989444096\,t} \end{pmatrix} \tag{B.26}$$

$f(x) = x^5 + 10x^2 + 5:$

$$\beta' = \begin{pmatrix} \epsilon_1\,\delta_1 - \frac{4066158490\,\epsilon_2\,\delta_1}{954111429} + \frac{11621900\,\epsilon_3\,\delta_1}{2321439} + \frac{32953801295\,\epsilon_4\,\delta_1}{954111429} - 200\,\epsilon_5\,\delta_1 \\ \frac{2905475\,\epsilon_1\,\delta_2}{4642878\,t} + \frac{32953801295\,\epsilon_2\,\delta_2}{7632891432\,t} - 25\,\frac{\epsilon_3\,\delta_2}{t} + \frac{87851681855\,\epsilon_4\,\delta_2}{1908222858\,t} + \frac{2423056375\,\epsilon_5\,\delta_2}{18571512\,t} \\ -\frac{2565694281\,\epsilon_2\,\delta_1}{3392396192} + \frac{949487275\,\epsilon_3\,\delta_1}{297144192} - \frac{61041394225\,\epsilon_4\,\delta_1}{20354377152} - \frac{445\,\epsilon_5\,\delta_1}{16} \\ \frac{949487275\,\epsilon_1\,\delta_2}{2377153536\,t} - \frac{61041394225\,\epsilon_2\,\delta_2}{162835017216\,t} - \frac{445\,\epsilon_3\,\delta_2}{128\,t} + \frac{6092208052225\,\epsilon_4\,\delta_2}{325670034432\,t} - \frac{18542187595\,\epsilon_5\,\delta_2}{594288384\,t} \\ \frac{760219986455\,\epsilon_2\,\delta_1}{15632161652736} - \frac{546579773\,\epsilon_3\,\delta_1}{3169538048} + \frac{223522035595\,\epsilon_4\,\delta_1}{1954020206592} + \frac{28825\,\epsilon_5\,\delta_1}{16384} \\ -\frac{546579773\,\epsilon_1\,\delta_2}{25356304384\,t} + \frac{223522035595\,\epsilon_2\,\delta_2}{15632161652736\,t} + \frac{28825\,\epsilon_3\,\delta_2}{131072\,t} - \frac{66180799869005\,\epsilon_4\,\delta_2}{62528646610944\,t} + \frac{36935998025\,\epsilon_5\,\delta_2}{25356304384\,t} \\ -\frac{21048029533\,\epsilon_2\,\delta_1}{13895254802432} + \frac{338220965\,\epsilon_3\,\delta_1}{76068913152} - \frac{11879343659\,\epsilon_4\,\delta_1}{5210720550912} - \frac{7115\,\epsilon_5\,\delta_1}{131072} \\ \frac{338220965\,\epsilon_1\,\delta_2}{608551305216\,t} - \frac{11879343659\,\epsilon_2\,\delta_2}{41685764407296\,t} - \frac{7115\,\epsilon_3\,\delta_2}{1048576\,t} + \frac{4822141269325\,\epsilon_4\,\delta_2}{166743057629184\,t} - \frac{20676257105\,\epsilon_5\,\delta_2}{608551305216\,t} \\ \frac{26624495\,\epsilon_2\,\delta_1}{1000458345775104} - \frac{47531\,\epsilon_3\,\delta_1}{608551305216} + \frac{5007295\,\epsilon_4\,\delta_1}{125057293221888} + \frac{\epsilon_5\,\delta_1}{1048576} \\ -\frac{47531\,\epsilon_1\,\delta_2}{4868410441728\,t} + \frac{5007295\,\epsilon_2\,\delta_2}{1000458345775104\,t} + \frac{\epsilon_3\,\delta_2}{8388608\,t} - \frac{2033079245\,\epsilon_4\,\delta_2}{4001833383100416\,t} + \frac{2905475\,\epsilon_5\,\delta_2}{4868410441728\,t} \end{pmatrix} \tag{B.27}$$

Bibliography

[AE12] C. Awtrey and T. Edwards. “Dihedral p-adic fields of prime degree”. In: *International Journal of Pure and Applied Mathematics* 75 [2012], pp. 185–194.

[AW92] William A. Adkins and Steven H. Weintraub. *Algebra: An Approach Via Module Theory*. Graduate Texts in Mathematics. Springer, 1992.

[BCE18] Nigel P. Byott, Lindsay N. Childs, and G. Griffith Elder. “Scaffolds and generalized integral Galois module structure”. In: *Annales de l'Institut Fourier* 68.3 [2018], pp. 965–1010. DOI: 10.5802/aif.3182. URL: https://aif.centre-mersenne.org/item/AIF_2018__68_3_965_0/.

[BE02] Nigel P. Byott and G. Griffith Elder. “Biquadratic Extensions with One Break”. In: *Canadian Mathematical Bulletin* 45.2 [2002], pp. 168–179. DOI: 10.4153/CMB-2002-020-3.

[BE13] Nigel P. Byott and G. Griffith Elder. “Galois scaffolds and Galois module structure in extensions of characteristic p local fields of degree p2”. In: *Journal of Number Theory* 133.11 [2013], pp. 3598–3610. ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2013.04.021. URL: https://www.sciencedirect.com/science/article/pii/S0022314X1300142X.

[BL96] Nigel P. Byott and Günter Lettl. “Relative Galois module structure of integers of abelian fields”. In: *Journal de Théorie des Nombres de Bordeaux* 8 [Oct. 1996], pp. 125–141. DOI: 10.5802/jtnb.160.

[Byo02] Nigel P. Byott. “Integral Hopf–Galois Structures on Degree p^2 Extensions of p-adic Fields”. In: *Journal of Algebra* 248.1 [2002], pp. 334–365. ISSN: 0021-8693. DOI: https://doi.org/10.1006/jabr.2001.9053.

[Byo04] Nigel P. Byott. “Hopf–Galois structures on Galois field extensions of degree pq”. In: *Journal of Pure and Applied Algebra* 188.1 [2004], pp. 45–57. ISSN: 0022-4049. DOI: https://doi.org/10.1016/j.jpaa.2003.10.010.

[Byo96] Nigel P. Byott. “Uniqueness of Hopf Galois Structure for Separable Field Extensions”. In: *Communications in Algebra* 24.10 [1996], pp. 3217–3228. DOI: 10.1080/00927879608825743. URL: https://doi.org/10.1080/00927879608825743.

[Che18] Chinnawat Chetcharungkit. “Scaffolds in Non-classical Hopf-Galois Structures”. PhD thesis. University of Exeter, 2018.

[Chi00] Lindsay N. Childs. *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*. 1st ed. Mathematical Surveys and Monographs 80. American Mathematical Society, 2000. ISBN: 0-8218-2131-8.

[Chi87] Lindsay N. Childs. “Taming Wild Extensions with Hopf Algebras”. In: *Transactions of the American Mathematical Society* 304.1 [1987], pp. 111–140. URL: http://www.jstor.org/stable/2000707.

[Cla] Pete L. Clark. “Field theory”. Available at http://alpha.math.uga.edu/~pete/FieldTheory.pdf.

[Coh07] Henri Cohen. *Number Theory: Volume I: Tools and Diophantine Equations*. 1st ed. Graduate Texts in Mathematics 239. Springer-Verlag New York, 2007. ISBN: 0387499229, 9780387499222, 9780387499239.

[Coh91] P. M. Cohn. *Algebra Volume 3, 2nd Edition*. 2 Sub. 1991. ISBN: 9780471928409.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*. 3rd, Corr. Print. Graduate Texts in Mathematics. Springer, 1993.

[Con] Keith Conrad. "Hensel's lemma". Available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf.

[CRV16] Teresa Crespo, Anna Rio, and Montserrat Vela. "Induced Hopf Galois structures". In: *Journal of Algebra* 457 [2016], pp. 312–322. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2016.03.012. URL: https://www.sciencedirect.com/science/article/pii/S0021869316001526.

[CS69] Stephen U. Chase and Moss E. Sweedler. *Hopf Algebras and Galois Theory*. 1st ed. Lecture Notes in Mathematics. Springer, 1969.

[Eld18] G. Griffith Elder. "Ramified extensions of degree *p* and their Hopf-Galois module structure". In: *Journal de Théorie des Nombres de Bordeaux* 30.1 [2018], pp. 19–40. DOI: 10.5802/jtnb.1014. URL: https://jtnb.centre-mersenne.org/item/JTNB_2018__30_1_19_0/.

[Eld98] G. Griffith Elder. "Galois Module Structure of Ambiguous Ideals in Biquadratic Extensions". In: *Canadian Journal of Mathematics* 50.5 [1998], pp. 1007–1047. DOI: 10.4153/CJM-1998-050-4.

[Fer74] Marie-Josée Ferton. "Sur l'anneau des entiers d'extensions cycliques d'un corps local". In: *Journées arithmétiques (Grenoble, 1973)*. Mémoires de la Société Mathématique de France 37. Société mathématique de France, 1974, pp. 69–74. DOI: 10.24033/msmf.130. URL: www.numdam.org/item/MSMF_1974__37__69_0/.

[FT92] A. Fröhlich and M. J. Taylor. *Algebraic number theory*. CUP. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1992.

[GP87] Cornelius Greither and Bodo Pareigis. "Hopf Galois theory for separable field extensions". In: *Journal of Algebra* 106.1 [1987], pp. 239–258. ISSN: 0021-8693. DOI: https://doi.org/10.1016/0021-8693(87)90029-9. URL: https://www.sciencedirect.com/science/article/pii/0021869387900299.

[GR] Daniel Gil-Muñoz and Anna Rio. "On Induced Hopf Galois structures and their Local Hopf Galois Modules". To appear in Publicacions Matemàtiques. URL: https://arxiv.org/abs/1910.06083.

[Har+87] Kenneth Hardy et al. "Calculation of the Class Numbers of Imaginary Cyclic Quartic Fields". In: *Mathematics of Computation* 49.180 [1987], pp. 615–620. ISSN: 00255718, 10886842. URL: http://www.jstor.org/stable/2008334.

[HW90] R.H. Hudson and K. S. Williams. "The integers of a cyclic quartic field". In: *Rocky Mountain Journal of Mathematics* 20.1 [1990], pp. 145–150. DOI: 10.1216/rmjm/1181073167. URL: https://doi.org/10.1216/rmjm/1181073167.

[Joh15] Henri Johnston. "Explicit integral Galois module structure of weakly ramified extensions of local fields". In: *Proceedings of the American Mathematical Society* 143 [Dec. 2015], pp. 5059–5071. DOI: 10.1090/proc/12634.

[Kap49] I. Kaplansky. “Elementary divisors and modules”. In: *Transactions of the American Mathematical Society* 66 [1949], pp. 464–491.

[Koc+19] Alan Koch et al. “The Structure of Hopf Algebras Acting on Dihedral Extensions”. In: *Advances in Algebra*. Ed. by Jörg Feldvoss et al. Cham: Springer International Publishing, 2019, pp. 201–218. ISBN: 978-3-030-11521-0.

[Lan02] Serge Lang. *Algebra*. 3rd ed. Graduate Texts in Mathematics 211. Springer-Verlag New York, 2002. ISBN: 9780387953854,038795385X.

[Let98] G. Lettl. “Relative Galois module structure of integers of local abelian fields”. In: *Acta Arithmetica* 85 [1998], pp. 235–238.

[LL07] Falko Lorenz and Silvio Levy. *Algebra: Volume II: Fields with Structure, Algebras and Advanced Topics*. 1st ed. Universitext. Springer, 2007.

[LMFDB] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. http://www.lmfdb.org. 2021.

[Mar77] Daniel A. Marcus. *Number fields*. Universitext. Springer, 1977.

[Mat02] Keith Matthews. “The Diophantine equation ax^2 + bxy + cy^2 = N, D = b^2 - 4ac > 0”. In: *Journal de Théorie des Nombres de Bordeaux* 14.1 [2002], pp. 257–270. ISSN: 12467405, 21188572. URL: http://www.jstor.org/stable/43972654.

[Ore24] O. Ore. “Bemerkungen zur Theorie der Differente”. In: *Mathematische Zeitschrift* 25 [1924], pp. 1–8.

[PR01] Sebastian Pauli and Xavier-François Roblot. “On the computation of all extensions of a p-adic field of a given degree”. In: *Math. Comp* 70 [2001], pp. 1641–1659.

[Rio95] Anna Rio. “Representacions de Galois octaèdriques”. PhD thesis. Universitat de Barcelona, 1995.

[Ser] Jean-Pierre Serre. *Local Fields*. Graduate Texts in Mathematics.

[Tho10] Lara Thomas. “On the Galois module structure of extensions of local fields”. In: *Publications mathématiques de Besançon* [2010], pp. 157–194.

[Tru09] Paul J. Truman. “Hopf-Galois Module Structure of Some Tamely Ramified Extensions”. PhD thesis. University of Exeter, 2009.

[Tru12] Paul J. Truman. “Hopf-Galois module structure of tame biquadratic extensions”. In: *Journal de Théorie des Nombres de Bordeaux* 24.1 [Mar. 2012], pp. 173–199. URL: http://eudml.org/doc/251057.

[Tru16] Paul J. Truman. “Canonical Nonclassical Hopf-Galois Module Structure of Nonabelian Galois Extensions”. In: *Communications in Algebra* 44 [2016], pp. 1119–1130. DOI: 10.1080/00927872.2014.999930.

[Tru18] Paul J. Truman. “Commutative Hopf–Galois module structure of tame extensions”. In: *Journal of Algebra* 503 [2018], pp. 389–408. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2018.01.047.

[Tru20] Paul J. Truman. “Hopf-Galois module structure of tamely ramified radical extensions of prime degree”. In: *Journal of Pure and Applied Algebra* 224.5 [2020]. ISSN: 0022-4049. DOI: https://doi.org/10.1016/j.jpaa.2019.106231.

[Und15] Robert G. Underwood. *Fundamentals of Hopf Algebras*. 1st ed. Universitext. Springer, 2015.