Hopf-Galois module structure of a class of tame quaternionic fields

Stuart Jonathon Taylor

A thesis presented for the degree of
Doctor of Philosophy in Mathematics

June 2020

Keele University

Abstract

We study the Hopf-Galois module structure of rings of integers in tame Galois extensions L/F of global fields with Galois group isomorphic to the quaternion group of order 8. We determine explicitly the Hopf algebras giving Hopf-Galois structures on such extensions and study which of these are isomorphic as Hopf algebras or as F-algebras. We study "quotient" structures in order to understand the Hopf-Galois module structure in such extensions corresponding to Hopf algebras of cyclic type.

Next we specialise to a certain family of tame quaternionic extensions, $L/\mathbb{Q}$, employing a construction of Fujisaki. We show that for these extensions the ring of algebraic integers, $\mathfrak{O}_L$, is locally free over its associated order in each of the Hopf-Galois structures. We find explicit local generators for all but the structures of cyclic type. We then employ the machinery of locally free class groups to study the structures of dihedral type and give necessary and sufficient conditions for $\mathfrak{O}_L$ to be free over its associated order in each of these structures.

Declaration

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where stated otherwise, by reference or acknowledgement, the work presented is entirely my own.

Acknowledgements

I would like to thank my supervisor Dr. Paul Truman, for his dedication to supporting me over the past three years, and during my undergraduate degree. I am grateful to Keele University for funding my Ph.D. and for providing such a nurturing and supportive environment. I would also like to thank Dr. Griff Elder for welcoming me to two very productive conferences in Omaha.

I would like to thank my parents for their eternal love and support in managing my life during a difficult time. I would also like to thank my brother, Graeme, my sister-in-law Hollie, and their wonderful child, and my niece, Luna, for their love and constant willingness to provide distraction when it was needed most.

Contents

Chapter 1

Introduction

A prominent classical question of algebraic number theory surrounds finding a description of the ring of the algebraic integers in a finite Galois extension of number fields. Let L/F be such an extension with Galois group G. The *normal basis theorem* states that there exists an element $x \in L$ such that the set $\{\sigma(x) \,|\, \sigma \in G\}$ is an F-basis for L. We can rephrase this; the existence of a *normal basis* of L over F is equivalent to L being a free module of rank one over the *group ring* $F[G]$. However, the integral analogue of this question has no such sleek answer; does there exist an element $x \in \mathfrak{O}_L$ such that the set $\{\sigma(x) \,|\, \sigma \in G\}$ is an $\mathfrak{O}_F$-basis of $\mathfrak{O}_L$, or equivalently, is $\mathfrak{O}_L$ a free module of rank one over $\mathfrak{O}_F[G]$? The Hilbert-Speiser theorem is the first result in this investigation for global fields and states that if an extension $L/\mathbb{Q}$ is abelian and *tame* (that is, the ramification indices of each prime ideal are all relatively prime to the corresponding residue characteristic) then $\mathfrak{O}_L$ is a free $\mathbb{Z}[G]$-module of rank one.

We may investigate the consequences of removing either of the two assumptions made in the Hilbert-Speiser theorem. If one removes the requirement that the extension be abelian then we may look to Martinet's work. He found that if $L/\mathbb{Q}$ is a tame Galois extension with Galois group isomorphic to the dihedral group of order 6 then $\mathfrak{O}_L$ is a free $\mathbb{Z}[G]$-module of rank one

(see [Mar69]). However, Martinet also found examples of tame extensions $L/\mathbb{Q}$ with Galois group isomorphic to the quaternion group of order 8 such that $\mathfrak{O}_L$ is not a free $\mathbb{Z}[G]$-module (see [Mar71]). These examples motivated intensive study of Galois module structure of tame extensions of $\mathbb{Q}$ which culminated in Taylor's result that the structure of $\mathfrak{O}_L$ over $\mathbb{Z}[G]$ is governed by the behaviour of certain L-functions (see [Tay81]).

With these examples it is clear that the tame condition of the Hilbert-Speiser theorem is also insufficient when the abelian condition is removed. In fact, in general when L and F are global fields, there is no guarantee that any basis exists for $\mathfrak{O}_L$ over $\mathfrak{O}_F$, let alone a normal integral basis. However, it is often more fruitful to consider the notion of *local freeness*, which is weaker as it is necessary but not sufficient for freeness. This concept arises via *completion*, that is, for each prime $\mathfrak{p}$ of $\mathfrak{O}_F$ we study the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}} = L \otimes \mathfrak{O}_{F,\mathfrak{p}}$, which does have a basis over the completed ring of integers $\mathfrak{O}_{F,\mathfrak{p}}$. We say $\mathfrak{O}_L$ is locally free over $\mathfrak{O}_F[G]$ if $\mathfrak{O}_{L,\mathfrak{p}}$ is a free module of rank one over $\mathfrak{O}_{F,\mathfrak{p}}[G]$ for all $\mathfrak{p}$ of $\mathfrak{O}_F$.

With this machinery we are able to understand the role of the tame condition more clearly. A theorem of Noether (see [Frö83, page 8]) states that the ring of integers of an extension L/F is locally free if and only if the extension is tame. Thus an extension that is not tame, that is *wild*, cannot hope to have a normal integral basis. Following Noether's theorem it is clear that a different technique is required to study wild extensions. One such technique is to study the structure of $\mathfrak{O}_L$, not over $\mathfrak{O}_F[G]$, but rather, over some other $\mathfrak{O}_F$-order in $F[G]$, called the associated order:

$$\mathfrak{A}_{F[G]} = \{\alpha \in F[G] \mid \alpha(\mathfrak{O}_L) = \mathfrak{O}_L\}.$$

For wild extensions the associated order properly contains the integral group ring $\mathfrak{O}_F[G]$ so is a sensible order to study in the hope of yielding more results. In fact, by construction, the associated order is the largest $\mathfrak{O}_F$-order in $F[G]$ over which $\mathfrak{O}_L$ is a module, so it is in some sense the best option.

However, this approach does not offer anything to the study of tame extensions as in these cases the associated order and the integral group ring coincide. In a different direction, that may provide fruit for the study of tame extensions, as well as wild extensions, one may consider the notion of a Hopf-Galois structure, that provides an analogue for the associated order that does give more opportunity for study in tame extensions. A Hopf-Galois structure on a finite Galois extension L/F consists of an F-Hopf algebra of dimension $[L : F]$ together with a certain F-linear action of H on L. The group ring $F[G]$ is the F-Hopf algebra for one such structure, called the *classical* structure. However, a given extension may in general be adorned with several nonclassical structures.

A theorem of Greither and Pareigis (see [GP87, Theorem 2.1]) gives a bijection between these Hopf-Galois structures and some subgroups of the permutation group on the letters of the Galois group, reducing the problem of finding the structures, to a much simpler group theoretic problem. Once one has a collection of Hopf-algebras H that give Hopf-Galois structures on the extension L/F we naturally ask for analogues to the classical picture. We have that the analogue to the normal basis theorem holds, that is L is a free H-module of rank 1. It remains to ask for the integral picture. In general, though, there is no direct analogue for $\mathfrak{O}_K[G]$ and so instead we ask for the analogue to the associated order:

$$\mathfrak{A}_H = \{\alpha \in H \mid \alpha(\mathfrak{O}_L) = \mathfrak{O}_L\}.$$

We then study $\mathfrak{O}_L$ over its associated order $\mathfrak{A}_H$ for each Hopf-algebra H that gives a Hopf-Galois structure on L/F.

In the case of wild extensions of local fields this approach has proven fruitful. For instance see [Koc15], [Eld18] and [Byo97]. In particular Byott's result shows that there are examples of wild Galois extensions of local fields L/F for which $\mathfrak{O}_L$ is not free over $\mathfrak{A}_{F[G]}$ but is free over $\mathfrak{A}_H$ for some other Hopf-algebra H giving a Hopf-Galois structure on the extension.

This line of study, though, has also been applied to tame extensions of global fields, where there is still room for improvement. For instance one may see [Tru11], [Tru12] and [Tru16]. In these cases we certainly have no hope that a different Hopf-Galois structure could give a better local picture, due to Noether's theorem, but it might be possible globally, though no such example has yet been found.

In this thesis we investigate tame Galois extensions of the rational numbers with Galois group isomorphic to the quaternion group of order 8; the first examples, due to Martinet, of extensions that could be either globally free or not in the classical case. We study these extensions using the techniques of Hopf-Galois module structure in an attempt to find the first examples of tame extensions for which we do not have global freeness in the classical sense, but attain global freeness using a nonclassical Hopf-Galois structure. Unfortunately, we are not yet able to exhibit such an example, but we do uncover interesting connections between the descriptions of the algebraic integers given by the various Hopf-Galois structures.

In Chapter 2 we collect background information on the key topics of study, from basic Galois module theory, through properties of quaternionic extensions, on to Hopf algebras, their Hopf-Galois structures, their Artin-Wedderburn decompositions, on through quaternion algebras, and then onto Hopf-Galois module theory and finally to locally free class groups that will provide a technique for understanding the global picture once the local picture has been established in enough detail.

In Chapter 3 we use the theory of Greither and Pareigis to determine explicitly the Hopf-Galois structures on quaternionic extensions. We use an established count of such structures found in [SV18] and propose the form of the subgroups in bijection with the Hopf-Galois structures due to Greither and Pareigis. We also study isomorphism properties of the corresponding Hopf algebras, considering which are isomorphic as Hopf algebras, and thus

which structures correspond to the same Hopf algebra with a different action on the extension, and which structures have different Hopf algebras. We further investigate their Artin-Wedderburn decompositions to find which structures are isomorphic as F-algebras, a weaker property than isomorphism as Hopf algebras.

In Chapter 4 we apply a recent result of Koch, Kohl, Truman and Underwood [KKTU19b] concerning "quotient" structures to questions of Hopf-Galois module structure. In particular we show that if $L/\mathbb{Q}$ is a tame quaternionic extension with a Hopf algebra H of cyclic *type* giving a Hopf-Galois structure on the extension $L/\mathbb{Q}$ then $\mathfrak{O}_L$ is not free over the associated order $\mathfrak{A}_H$, despite being locally free (see [Tru11]).

For the remainder of the thesis our focus will turn to a particular family of quaternionic extensions, which we label Fujisaki extensions, that allow us to give a more explicit description of the action of the Galois group on the elements in the extension. In Chapter 5 we will construct these extensions and derive criteria for them to be tame. We further investigate discriminants and local integral bases. We finally derive a condition for a tame Fujisaki extension to have a normal integral basis.

In Chapter 6 we prove that if $L/\mathbb{Q}$ is a tame Fujisaki extension then $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$ for all Hopf algebras H giving Hopf-Galois structures to the extension, and give explicit local generators for $\mathfrak{O}_L$ over $\mathfrak{A}_H$ for all but those H of cyclic type.

In Chapter 7 we focus on the Hopf-Galois structures that are given by Hopf algebras of dihedral type. We use the explicit local generators found in chapter 6 and idèlic machinery, that is finding the class of $\mathfrak{O}_L$ in the locally free class group, to derive necessary and sufficient conditions for $\mathfrak{O}_L$ to be globally free over $\mathfrak{A}_H$. As it turns out, the conditions found are the same as for $\mathfrak{O}_L$ being globally free over its associated order in the classical Galois situation.

Chapter 2

Background

In this chapter we collect the Galois module theory we will need in what follows before introducing the notion of a Hopf-Galois structure along with results that will allow us to understand the form of the objects involved. We then present Hopf-Galois module theory as a generalisation of classical Galois module theory before finally introducing the locally free class group as a tool for understanding the relationship between local and global module structure.

2.1 Galois module theory

In this section we present the theory of local fields and ramification in Galois extensions in order to understand the comparative notions of global and local freeness, before relating these ideas to quaternionic extensions.

2.1.1 Local fields

This presentation of the theory of local fields is mostly taken from [Neu13, chapter 2]. We start by understanding the process of completion.

Definition 2.1.1. *An* absolute value *on a field K is a function*

$$|\cdot| : K \to \mathbb{R}_+$$

such that

1. $|x| = 0$ *if and only if* $x = 0$,

2. $|xy| = |x||y|$ *for all* $x, y \in K$,

3. $|x + y| \leq |x| + |y|$ *for all* $x, y \in K$.

Definition 2.1.2. *A field K with an absolute value $|\cdot|$ is called* complete *if every Cauchy sequence $(a_n)_{n\in\mathbb{N}}$ in K converges to an element $a \in K$.*

From any field K with an absolute value we may obtain a complete field $\hat{K}$ with respect to that absolute value through the process of *completion*.

Definition 2.1.3. *A ring R is called a* discrete valuation ring *if it is a principal ideal domain which has a unique non-zero prime ideal, $\mathfrak{m}$. We have that $\mathfrak{m}$ is maximal since R is a principal ideal domain and can be written $\mathfrak{m} = \pi R$ where the generator π is called a* uniformiser *of R.*

Since $\mathfrak{m}$ is maximal every element not contained in $\mathfrak{m}$ is a unit and π is the only prime element of R up to multiplication by a unit. Thus any nonzero element of R, say x, may be written as $x = u\pi^n$ for some $u \in R^\times$ and $n \in \mathbb{N} \cup \{0\}$. Since any other choice of uniformiser must result in the same value of n we may define a *valuation* on R:

$$\nu : R \to \mathbb{N} \cup \{0\}$$

by $\nu(u\pi^n) = n$. This naturally extends to the field of fractions of R, say K, by setting $\nu(a/b) = \nu(a) - \nu(b)$ and $\nu(0) = \infty$.

We may also do the reverse of this process:

Definition 2.1.4. *Let K be a field and define a valuation $\nu : K \to \mathbb{Z} \cup \{\infty\}$ on K. Let $R = \{x \in K \mid \nu(x) \geq 0\}$. Then R is a discrete valuation ring called the* valuation ring *or the* ring of integers *of K with respect to ν.*

We can perform the process of completing a field K with respect to a valuation ν by associating the valuation with some absolute value and performing the process described above.

Definition 2.1.5. *The completion of a global field has a discrete valuation ring with a corresponding finite residue class field. Such fields are called* local fields. *Explicitly, for a global field K with valuation ν, valuation ring R with unique prime ideal $\mathfrak{m}$ we may suppose that $R/\mathfrak{m}$ is finite with q elements, say. We denote and define the* normalised absolute value *on K associated to ν by $|x|_\nu = q^{-\nu(x)}$. We call K a* local field *if it is complete with respect to this absolute value.*

Example 2.1.6. *Let K be a number field, and $\mathfrak{p}$ be a prime of the ring of integers $\mathfrak{O}_K$ lying above a prime number $p \in \mathbb{Z}$. The residue class field $\mathfrak{O}_K/\mathfrak{p}$ is finite. We define a valuation $\nu_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ by setting $\nu_\mathfrak{p}(0) = \infty$ and for all $x \in K^\times$ setting $\nu_\mathfrak{p}(x)$ to be the power of the prime $\mathfrak{p}$ that appears in the factorisation of the fractional ideal $x\mathfrak{O}_K$. We denote the associated normalized absolute value by $|\cdot|_\mathfrak{p}$ and note that K is not complete with respect to this absolute value. We denote the completion $K_\mathfrak{p}$ which is a local field with valuation ring $\mathfrak{O}_{K,\mathfrak{p}}$ which has, in turn, maximal ideal $\mathfrak{p}$. Such local fields are called* p-adic fields.

Example 2.1.7. *In particular, when $K = \mathbb{Q}$, we identify a prime of the ring of integers $\mathbb{Z}$ as the ideal $p\mathbb{Z}$ in one-to-one correspondence with prime numbers, p, in $\mathbb{Z}$. Any element of $\mathbb{Q}$ is of the form*

$$x = \pm \prod_p p^{r_p}$$

where for each prime p, $r_p \in \mathbb{Z}$. Then the valuation for any prime p is given by $\nu_p(x) = r_p$.

2.1.2 Ramification in Galois extensions

Let L/K be a finite extension of number fields with rings of integers $\mathfrak{O}_L$ and $\mathfrak{O}_K$ respectively.

Definition 2.1.8. *Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ with*

$$\mathfrak{p}\mathfrak{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

the unique factorisation of $\mathfrak{p}\mathfrak{O}_L$ into prime ideals of $\mathfrak{O}_L$ so that the e_i are the ramification indices *of their respective $\mathfrak{P}_i$. For each $i = 1, \ldots, g$ the finite field $\mathfrak{O}_L/\mathfrak{P}_i$ is a finite extension of the finite field $\mathfrak{O}_K/\mathfrak{p}$, and we denote the degree of this extension by f_i, called the* residue field degree. *Then we have the relation*

$$[L : K] = \sum_{i=1}^{g} e_i f_i.$$

Let p be the characteristic of the residue field $k_\mathfrak{p} = \mathfrak{O}_K/\mathfrak{p}$. We have the following definitions.

- *The prime $\mathfrak{p}$ is said to be* unramified *in $\mathfrak{O}_L$ if $e_i = 1$, or equivalently the extension of p-adic fields $L_{\mathfrak{P}_i}/K_\mathfrak{p}$ is unramified, for all $i = 1, \ldots, g$ and* ramified *otherwise.*

- *$\mathfrak{p}$ is said to be* tamely ramified *if it is ramified and $(e_i, p) = 1$ for all $i = 1, \ldots, g$, or equivalently the extension of p-adic fields $L_{\mathfrak{P}_i}/K_\mathfrak{p}$ is tamely ramified, and* wildly ramified *otherwise.*

We call the extension L/K unramified *if all primes of $\mathfrak{O}_K$ are unramified in $\mathfrak{O}_L$,* tamely ramified *(or* tame*) if all primes of $\mathfrak{O}_K$ which are ramified in $\mathfrak{O}_L$ are tamely ramified, and* wildly ramified *(or* wild*) if any prime of $\mathfrak{O}_K$ is wildly ramified. We may also say an extension is* at most tamely ramified *if it is either unramified or tamely ramified.*

Remark 2.1.9. *If L/K is a finite extension of number fields of prime power degree, say $[L : K] = p^n$ for some prime p, then L/K is tame if and only if $\mathfrak{p}$ is unramified in L for all $\mathfrak{p} | p\mathfrak{O}_K$.*

As the extensions we will be investigating in this thesis are tame extensions we now present equivalent conditions for an extension to be tame.

Theorem 2.1.10. *The following are equivalent:*

1. *L/K is tame,*
2. *$Tr_{L/K}(\mathfrak{O}_L) = \mathfrak{O}_K$,*
3. *there exists some $x \in \mathfrak{O}_L$ such that $Tr_{L/K}(x) = 1$.*

Proof. For the proof of the equivalency of part 1 and part 2 see [Frö83, Theorem 3]. The last statement implies the second because it implies $\mathrm{Tr}(\mathfrak{O}_L) \supseteq \mathrm{Tr}(x\mathfrak{O}_K) = \mathfrak{O}_K$ and $\mathfrak{O}_K \supseteq \mathrm{Tr}(\mathfrak{O}_L)$ since $\mathrm{Tr}(\mathfrak{O}_L)$ must lie in K and be integral. The opposite implication is obvious since $1 \in \mathfrak{O}_K$. □

We now wish to apply this ramification theory to Galois extensions appropriately for the investigations in this thesis. Suppose that L/K is Galois with group G. Then if $\mathfrak{P}$ lies above $\mathfrak{p}$ then so does $\sigma\mathfrak{P}$ for each $\sigma \in G$ since

$$\sigma\mathfrak{P} \cap \mathfrak{O}_L = \sigma(\mathfrak{P} \cap \mathfrak{O}_L) = \sigma\mathfrak{p} = \mathfrak{p}.$$

The ideals $\sigma\mathfrak{P}$ for $\sigma \in G$ are called the prime ideals *conjugate* to $\mathfrak{P}$.

Proposition 2.1.11. *G acts transitively on the set of all prime ideals $\mathfrak{P}$ of $\mathfrak{O}_L$ lying above $\mathfrak{p}$, that is these prime ideals are conjugates of one another.*

Proof. See [Neu13, §9, Proposition 9.1]. □

This leads to the following helpful corollary.

Corollary 2.1.12. *Let p be a prime of $\mathfrak{O}_K$ such that*

$$\mathfrak{p}\mathfrak{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$$

is the unique factorisation of $\mathfrak{p}\mathfrak{O}_L$ into prime ideals of $\mathfrak{O}_L$, with corresponding residue field degrees $f_1, \ldots, f_g$. Then in fact the e_i and f_i are independent of i so that

$$\mathfrak{p}\mathfrak{O}_L = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_g)^e$$

with $f = [\mathfrak{O}_L/\mathfrak{P}_i : \mathfrak{O}_K/\mathfrak{p}]$ for each $i = 1, \ldots, g$, and so $[L : K] = efg$.

Proof. See [Neu13, §9, page 55]. □

2.1.3 Global and local freeness results

As discussed in the introduction, the normal basis theorem states that for a Galois extension L/K with group G, there exists some $x \in L$ such that $\{\sigma(x) \,|\, \sigma \in G\}$ is a K-basis for L. One may investigate the existence of a normal integral basis of L over K and it is helpful to rephrase this question in terms of the group ring of $\mathfrak{O}_K$, defined here.

Definition 2.1.13. *Let R be a ring and G be a finite group. We define the* group ring *$R[G]$ to be the set $\{\sum_{g\in G} r_g g \,|\, r_g \in R, g \in G\}$ with multiplication defined by extending the multiplication on G R-linearly.*

Proposition 2.1.14. *Let L/K be a Galois extension of global or local fields with valuation rings $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. The following are equivalent:*

1. *$\mathfrak{O}_L$ is free of rank 1 over $\mathfrak{O}_K[G]$,*

2. *$\mathfrak{O}_L$ has a normal integral basis over $\mathfrak{O}_K$,*

3. *there exists $x \in \mathfrak{O}_L$ such that $\mathfrak{O}_L = \mathfrak{O}_K[G] \cdot x$.*

We may define the completion of the extensions of K in a natural way, and then find a helpful, and equally natural, decomposition for these rings.

Definition 2.1.15. *Let L/K be a finite separable extension of number fields with rings of integers $\mathfrak{O}_L$, $\mathfrak{O}_K$ respectively. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$. Then we define the $K_\mathfrak{p}$-algebra,*

$$L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L$$

and we define

$$\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{O}_L.$$

Theorem 2.1.16. *Let L/K be a finite separable extension of number fields with rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$. There is a decomposition*

$$L_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}.$$

The analogous decomposition at integral level also holds:

$$\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_L \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}} \cong \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{L,\mathfrak{P}}.$$

Proof. See [FT93, Theorem 17]. □

If $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$ then $K_\mathfrak{p}$ is a local field. We can study the effect of this completion on L and $\mathfrak{O}_L$.

Definition 2.1.17. *Let L/K be an extension of number fields with rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. We say that $\mathfrak{O}_L$ is* locally free *of rank 1 over $\mathfrak{O}_K[G]$ if for all primes $\mathfrak{p}$ of K, $\mathfrak{O}_{L,\mathfrak{p}}$ is free of rank 1 over $\mathfrak{O}_{K,\mathfrak{p}}[G]$.*

Theorem 2.1.18. ***Noether's Theorem.*** *If L/K is an extension of global fields then $\mathfrak{O}_L$ is locally free of rank 1 over $\mathfrak{O}_K[G]$ if and only if L/K is tame.*

For wildly ramified extensions a new subring of $K[G]$ is needed to be considered in the place of $\mathfrak{O}_K[G]$.

Definition 2.1.19. *We denote and define the* associated order *of* $\mathfrak{O}_L$ *in* $K[G]$ *by*

$$\mathfrak{A}_{K[G]}(\mathfrak{O}_L) = \{\alpha \in K[G] \,|\, \alpha(\mathfrak{O}_L) = \mathfrak{O}_L\}.$$

It is clear that this ring contains $\mathfrak{O}_K[G]$ but in fact the associated order is equal to $\mathfrak{O}_K[G]$ if and only if the extension L/K is tame. Thus, for tame extensions this generalisation does not help us investigate global freeness when trying to improve upon Noether's theorem. There are two main pieces left. The first is to generalise the form of $K[G]$ in a helpful manner and the second is to understand how to relate the question of local freeness to that of global freeness.

2.1.4 Quaternionic extensions

As this thesis investigates tame Galois extensions with Galois group isomorphic to the quaternion group of order 8, we now consider the previous discussions in this context.

Definition 2.1.20. *An extension of fields* L/K *is called a* quaternionic extension *if it is Galois with group* G *isomorphic to the quaternion group of order* 8.

Let L/K be a quaternionic extension with K a field of characteristic zero and let $G = \mathrm{Gal}(L/K)$. In this section we will present numerous results regarding quaternionic extensions.

Proposition 2.1.21. L/K *has a unique biquadratic subextension* E/K.

Proof. G has a unique subgroup of order 2, generated by the only element of order 2, say g. This subgroup is normal in G and the quotient group $G/\langle g\rangle$ is elementary abelian of order 4. □

In the opposite direction the following theorem relates the question of whether a biquadratic field can be embedded into a quaternionic extension

to the question of equivalency of quadratic forms. We present it as it has useful implications for our investigations.

Theorem 2.1.22. ***(Witt, 1936)*** *Let $a, b \in K$ be such that $a, b, ab \notin K^2$, and let $\alpha, \beta \in K^{alg}$ satisfy $\alpha^2 = a$, $\beta^2 = b$. Then the biquadratic extension $K(\alpha, \beta)$ can be embedded into a quaternionic extension of K if and only if the quadratic form $aX_1^2 + bX_2^2 + abX_3^2$ is equivalent to the quadratic form $Y_1^2 + Y_2^2 + Y_3^2$.*

Proof. See [Wit36] or [JY88, Theorem 1.1.1]. □

This theorem has a helpful corollary:

Corollary 2.1.23. *Let $a \in K - K^2$ and let $\alpha \in K^{alg}$ satisfy $\alpha^2 = a$. If the quadratic extension $K(\alpha)$ can be embedded into a quaternionic extension of K then a is the sum of three squares in K.*

Proof. See [JY88, Proposition I.2.8]. □

Definition 2.1.24. *A* Quaternionic Field *is a quaternionic extension of $\mathbb{Q}$.*

We must also understand the ramification of primes in the extension $K/\mathbb{Q}$. The following result gives straightforward equivalent conditions for the tameness of this extension.

Proposition 2.1.25. *Let $E/\mathbb{Q}$ be a biquadratic extension, and write $E = \mathbb{Q}(\alpha, \beta)$ with $a = \alpha^2$ and $b = \beta^2$ squarefree integers. Then $E/\mathbb{Q}$ is tamely ramified if and only if $a \equiv b \equiv 1 \pmod{4\mathbb{Z}}$.*

Proof. Let us first suppose $E/\mathbb{Q}$ is tamely ramified so that we must have $\mathbb{Q}(\alpha)/\mathbb{Q}$ is tamely ramified. Since the latter is a Galois extension of degree 2 we have that 2 is unramified in $\mathbb{Q}(\alpha)$. This implies $2 \nmid \mathfrak{d}(\mathbb{Q}(\alpha)/\mathbb{Q})$. We also have, since a is squarefree, that

$$\mathfrak{d}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \begin{cases} a & \text{if } a \equiv 1 \pmod{4\mathbb{Z}} \\ 4a & \text{otherwise.} \end{cases}$$

Thus we must have $a \equiv 1 \pmod{4\mathbb{Z}}$. Similarly, we find $b \equiv 1 \pmod{4\mathbb{Z}}$.

Conversely, suppose $a \equiv b \equiv 1 \pmod{4\mathbb{Z}}$. Then $2 \nmid \mathfrak{d}(\mathbb{Q}(\alpha)/\mathbb{Q})$ and so $\mathbb{Q}(\alpha)/\mathbb{Q}$ is tamely ramified. Since $b \equiv 1 \pmod{4\mathbb{Z}}$ we have $b \equiv 1 \pmod{\mathfrak{p}^2}$ for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_{\mathbb{Q}(\alpha)}$ lying above 2, and so $E/\mathbb{Q}(\alpha)$ is tamely ramified since $\frac{1+\alpha}{2}, \frac{1+\beta}{2} \in \mathfrak{O}_E$ and both have trace 1. Therefore $E/\mathbb{Q}$ is also tamely ramified. □

As stated in the introduction, Martinet gave the first examples of tame Galois extensions of $\mathbb{Q}$ with no normal integral basis, when the Galois group is isomorphic to the quaternion group of order 8. In fact, he gave conditions for exactly when such an extension has freeness; Martinet proved an effective method of determining whether or not $\mathfrak{O}_L$ is free over $\mathbb{Z}[G]$.

As in the proof above let us denote the unique biquadratic subfield of a quaternionic extension $L/\mathbb{Q}$ by $E = \mathbb{Q}(\alpha, \beta)$ so that E has subfields $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha\beta)$.

Theorem 2.1.26. ***Martinet's Criterion.*** *Let $L/\mathbb{Q}$ be a tame quaternionic extension with ring of integers $\mathfrak{O}_L$. Denote $\mathfrak{d}(\mathbb{Q}(\omega)/\mathbb{Q})$ by $\mathfrak{d}_\omega$. Let $\epsilon = 1$ if L is real and $\epsilon = -1$ if L is imaginary and let $\Delta = \mathfrak{d}(L/\mathbb{Q})$. Let*

$$\phi = \frac{1 + \mathfrak{d}_\alpha + \mathfrak{d}_\beta + \mathfrak{d}_{\alpha\beta}}{4}$$

and

$$\psi = \epsilon \prod_{p|\Delta} p.$$

Then $\mathfrak{O}_L$ is free over $\mathbb{Z}[G]$ if and only if

$$\phi \equiv \psi \pmod{4}. \tag{2.1}$$

Proof. See [Mar71, Proposition 3.2, Proposition 4.1] □

Example 2.1.27. *Let* $\alpha = \sqrt{5}$, $\beta = \sqrt{21}$, $\gamma^2 = \frac{5+\sqrt{5}}{2}\frac{21+\sqrt{21}}{2}$ *and* $L = K(\gamma)$. *It is verifiable that* L *is a tame quaternionic extension of* $\mathbb{Q}$. *The only prime factors of* Δ *are* $3, 5$ *and* 7, *and* L *is real, so the right hand side of the above congruence is* $3 \times 5 \times 7$. *The left hand side is* $\frac{1+5+21+105}{4}$. *Hence both sides are congruent to* $1 \pmod 4$ *and so* $\mathfrak{O}_L$ *is free over* $\mathbb{Z}[G]$.

Example 2.1.28. *Let* $\alpha = \sqrt{5}$, $\beta = \sqrt{41}$, $\gamma^2 = \frac{5+\sqrt{5}}{2}\frac{41+\sqrt{5\cdot 41}}{2}$ *and* $L = K(\gamma)$. *It is verifiable that* L *is a tame quaternionic extension of* $\mathbb{Q}$. *The only prime factors of* Δ *are* 5 *and* 41, *and* L *is real, so the right hand side of the above congruence is* 5×41. *The left hand side is* $\frac{1+5+41+205}{4}$. *Hence the two sides are not congruent to each other modulo* 4 *and so* $\mathfrak{O}_L$ *is not free over* $\mathbb{Z}[G]$.

This result highlights the advantages of looking here for an example of an extension that is not free classically but may be free when we consider alternative rings in place of $\mathbb{Z}[G]$.

2.2 Hopf-Galois theory

In this section we present the notion of a Hopf-Galois structure as an alternative method of studying the structure of algebraic integers in extensions of local or global fields.

2.2.1 Hopf algebras

Let R be a commutative ring with unity. We start this section by defining a Hopf algebra and how this defines a Hopf-Galois structure on an extension.

Definition 2.2.1. *An* R*-module,* A, *is called an* R-algebra *if it is adorned with a multiplication map* $\mu : A \otimes_R A \to A$ *and a unit map* $\iota : R \to A$ *such that* μ *is associative, the map* $\mu \circ (1 \otimes \iota) : A \otimes_R R \to A \otimes_R A \to A$ *is the same as the* R*-module multiplication map* $A \otimes_R R \to A$, *and finally that* $\mu \circ (\iota \otimes 1)$

is the same as scalar multiplication $R \otimes_R A \to A$. That is the diagrams

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

$$\begin{array}{ccc} A \otimes_R R & \xrightarrow{1\otimes\iota} & A \otimes_R A \\ \| & & \downarrow{\scriptstyle \mu} \\ A \otimes_R R & \xrightarrow{\textit{scalar mult.}} & A \end{array}$$

and

$$\begin{array}{ccc} R \otimes_R A & \xrightarrow{\iota\otimes 1} & A \otimes_R A \\ \| & & \downarrow{\scriptstyle \mu} \\ R \otimes_R A & \xrightarrow{\textit{scalar mult.}} & A \end{array}$$

commute.

Definition 2.2.2. *An R-module, A, is called an R-*coalgebra *if it is adorned with a map $\Delta : A \to A \otimes_R A$, called* comultiplication*, and a map $\varepsilon : A \to R$, called* counit*, that are R-module homomorphisms and that satisfy the* coassociativity *property, that is the diagram*

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_R A \\ \downarrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle \Delta\otimes 1} \\ A \otimes_R A & \xrightarrow{1\otimes\delta} & A \otimes_R A \otimes_R A \end{array}$$

commutes, and the counitary *property, that is the diagrams*

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_R A \\ \| & & \downarrow{\scriptstyle 1\otimes\varepsilon} \\ A & \xleftarrow{\mu} & A \otimes_R R \end{array}$$

and

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_R A \\ \| & & \downarrow{\scriptstyle \varepsilon\otimes 1} \\ A & \xleftarrow{\mu} & R \otimes_R A \end{array}$$

both commute.

Definition 2.2.3. *An* R-bialgebra*,* H*, is an* R*-module that is both an* R*-algebra and an* R*-coalgebra. We define the* switch *map* $\tau : H \otimes H \to H \otimes H$ *by* $\tau(h_1 \otimes h_2) = h_2 \otimes h_1$*. Then an* R*-bialgebra is called an* R-Hopf algebra *if there is an* R*-module homomorphism*

$$\lambda : H \to H$$

called the antipode *which is both an* R*-algebra and an* R*-coalgebra antihomomorphism, that is*

$$\lambda(h \otimes h') = \lambda(h') \otimes \lambda(h)$$

and

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

and further satisfies the antipode property*:*

$$\mu(1 \otimes \lambda)\Delta = \iota\varepsilon \text{ and } \mu(\lambda \otimes 1)\Delta = \iota\varepsilon.$$

Now that we have the notion of a Hopf algebra we wish to understand how such an object can define a new structure on an extension of fields. We start by defining a property of a Hopf algebra and giving a motivational example.

Definition 2.2.4. *An* R*-Hopf algebra,* H*, is* cocommutative *if* $\tau\Delta = \Delta$*, and* commutative *if* H *is commutative as an algebra. Further,* H *is* abelian *if* H *is both commutative and cocommutative.* H *is said to be* finite *if it is finitely generated and projective as an* R*-module.*

Example 2.2.5. *For a finite group* G*, a group ring,* $R[G]$*, defined in Definition 2.1.13, is the classical example of an* R*-Hopf algebra. Since* Δ, ε *and* λ *are* R*-linear homomorphisms, they are uniquely determined by their actions on elements of* G*:*

$$\Delta(\sigma) = \sigma \otimes \sigma,$$

$$\varepsilon(\sigma) = 1$$

and

$$\lambda(\sigma) = \sigma^{-1}$$

for any $\sigma \in G$. *The group ring* $R[G]$ *is finite and cocommutative as an* R*-Hopf algebra.*

The following notation is useful for describing the comultiplication on a Hopf algebra:

Definition 2.2.6. ***Sweedler Notation.*** *Let* R *be a commutative ring with unity and* H *an* R*-Hopf algebra. For* $h \in H$ *we may write*

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)} \in H \otimes_R H.$$

Example 2.2.7. *Using Sweedler notation we may recognise that cocommutativity becomes the condition*

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

Definition 2.2.8. *Let* H *be an* R*-Hopf algebra and* S *an* R*-algebra which is also an* H*-module. Then* S *is said to be an* H*-module algebra if, for all* $h \in H$ *and* $s, t \in S$*, we have*

$$h(st) = \sum_{(h)} h_{(1)}(s) h_{(2)}(t)$$

and

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

We finally define the notion of a Hopf-Galois structure and give a known example recognisable from the discussion in the previous section.

Definition 2.2.9. *Let* H *be a finite cocommutative* R*-Hopf algebra and let* S *be a finite commutative* R*-algebra. We say* S *is an* H-Galois extension *of*

R, or the extension S/R is H-Galois, or H gives a Hopf-Galois structure on S/R, if S is a left H-module algebra, and the R-module homomorphism

$$j : S \otimes_R H \to End_R(S)$$

$$j(s \otimes h)(t) = sh(t), \text{ for } s, t \in S, h \in H,$$

is an isomorphism.

Example 2.2.10. *Let L/K be a finite Galois extension of fields with group G. Then the K-Hopf algebra $K[G]$ gives a Hopf-Galois structure on the extension. This example is called the* classical *structure and any other Hopf-Galois structure admitted by such an extension is said to be* nonclassical.

2.2.2 Greither and Pareigis theory

Greither and Pareigis proved a theorem, in [GP87] (see also [Chi00, Theorem 6.8]), that classifies Hopf-Galois structures on separable field extensions in group theoretic terms. We state it here in a weakened form specifically for Galois extensions. We start by presenting some group theoretic properties that are necessary for understanding the theorem.

Definition 2.2.11. *For some set X, let $Perm(X)$ be the group of permutations on the letters of the set X. A subgroup $N \subset Perm(X)$ is said to be regular if any two (and therefore all three) of the following conditions are satisfied:*

1. *N and X have the same cardinality,*

2. *N acts transitively on X (i.e. for all $x, y \in X$ there exists $n \in N$ such that $nx = y$),*

3. *the stabiliser $Stab_N(x) = \{n \in N \mid nx = n\}$ is trivial for all $x \in X$.*

Definition 2.2.12. *Let L/K be a Galois extension of fields with group G. We denote and define the* left regular representation map *by*

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

$$\lambda(\tau)(\sigma) = \tau\sigma$$

for all $\sigma, \tau \in G$. Similarly, we denote and define the right regular representation map *by*

$$\rho : G \to Perm(G)$$

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

for all $\sigma, \tau \in G$.

Remark 2.2.13. *In $Perm(G)$ the subgroups $\rho(G)$ and $\lambda(G)$ commute with each other.*

We define an action of G on $Perm(G)$ by ${}^{g}x = \lambda(g)x\lambda(g^{-1})$ for all $x \in Perm(G)$. Any subgroup N of $Perm(G)$ that is normalized by $\lambda(G)$ is acted on by G under the same action. This allows us to define the fixed group ring $L[N]^G$ as the set of elements of $L[N]$ that are fixed under the above action of G.

Now we may state the theorem of Greither and Pareigis.

Theorem 2.2.14. ***Greither and Pareigis.*** *Let L/K be a Galois extension of fields with group G. Then we have the following;*

1. *There is a bijection between regular subgroups N of $Perm(G)$ that are normalised by $\lambda(G)$ and Hopf-Galois structures on L/K.*

2. *The bijection may be explicitly described by $N \leftrightarrow L[N]^G$ where $L[N]^G$ is the K-Hopf algebra that gives a Hopf-Galois structure onto L/K. Such a group N is said to be the* underlying subgroup *of the Hopf-Galois structure it corresponds to.*

3. $L[N]^G$ *acts on* L *by the following*

$$\left(\sum_{n\in N} c_n n\right)\cdot x = \sum_{n\in N} c_n n^{-1}(1_G)[x] \tag{2.2}$$

where $c_n \in L$, $x \in L$.

Proof. See [Chi00, Theorem 6.8]. □

Remark 2.2.15. *Let* H *be a Hopf algebra giving a Hopf-Galois structure on an extension with underlying subgroup* N. N *is abelian if and only if* H *is commutative.*

Example 2.2.16. *Let* L/K *be a finite Galois extension with group* G. *It is easy to see that* $\lambda(G)$ *and* $\rho(G)$ *commute with one another regardless of whether or not* G *is abelian and that* $\rho(G)$ *is a regular subgroup of* $Perm(G)$. *Then, since* λ *and* ρ *commute, it is normalised by* $\lambda(G)$. *Thus* $L[\rho(G)]^G$ *is a* K*-Hopf algebra adorning a Hopf-Galois structure onto* L/K. *In fact, the action of* G *on* $\rho(G)$ *is trivial and so* $L[\rho(G)]^G = K[\rho(G)] = K[G]$ *and so this is the classical structure found in Example 2.2.10.*

Moreover $\lambda(G) = \rho(G)$ *if and only if* G *is abelian. If* G *is not abelian then it is also easy to see that* $\lambda(G)$ *is a regular subgroup of* $Perm(G)$ *and is trivially normalised by* $\lambda(G)$. *Thus* $L[\lambda(G)]^G$ *is a* K*-Hopf algebra admitting a Hopf-Galois structure on* L/K *and this is called the* canonical nonclassical *structure.*

We will lean heavily on this theorem as we can now present every Hopf algebra giving a Hopf-Galois structure on a Galois extension in this form as a "twisted" form of a group ring. It also gives us ways of relating two structures to each other. One example of such a relationship is given here.

Definition 2.2.17. *Let* L/K *be an extension which is* H*-Galois for some Hopf algebra* H*, with underlying subgroup* N. *Define the centraliser of* N *in*

Perm(G) *by*

$$N' = \mathrm{Cent}_{Perm(G)}(N) = \{\eta' \in Perm(G) \,|\, \eta\eta' = \eta'\eta \text{ for all } \eta \in N\}.$$

Then N' *is a regular* G*-stable subgroup of* $Perm(G)$ *and thus is the underlying subgroup of some other Hopf algebra* H' *adorning* L/K *with a Hopf-Galois structure. We define the structure given by* H' *to be the* opposite *structure to that given by* H*.*

Example 2.2.18. *For nonabelian extensions, the classical and canonical nonclassical structures are opposites.*

2.2.3 Hopf Algebra isomorphisms

Two Hopf-Galois structures can have the same Hopf algebra that acts in two different ways. The results in this subsection are presented so that we may understand when Hopf-Galois structures have different Hopf algebras or the same Hopf algebra only with different actions.

Definition 2.2.19. *Let* G *be a group and* N *be a set. Then* N *is a* G-set *if there is a* G*-action on the set* N*, i.e for all* $n \in N$ *and* $g, h \in G$ *we have* $g(hn) = (gh)n$*. Two* G*-sets,* N_1, N_2 *are said to be isomorphic as* G*-sets if there is a* G*-equivariant bijection* $f : N_1 \to N_2$*, i.e.* $f(gn) = gf(n)$ *for all* $g \in G$ *and* $n \in N_1$*.*

Definition 2.2.20. *Let* G *be a group and* N *be a* G*-set. Then* N *is said to be a* G-group *if it is a group on which* G *acts via automorphisms. We say that two* G*-groups* N_1, N_2 *are isomorphic as* G*-groups if there is a* G*-equivariant isomorphism* $f : N_1 \to N_2$*.*

Example 2.2.21. *An underlying subgroup,* N*, of a Hopf-Galois structure on a field extension* L/K*, that has Galois group* G*, is a* G*-group.*

We may finally present the result of Koch, Kohl, Truman and Underwood that isolates when two Hopf algebras are isomorphic based upon the relationship between their underlying subgroups.

Theorem 2.2.22. *Let L/K be a Galois extension of fields with group G. Let N_1 and N_2 be underlying subgroups of Hopf-Galois structures on L/K. Then $L[N_1]^G \cong L[N_2]^G$ as K-Hopf algebras if and only if $N_1 \cong N_2$ as G-groups.*

Proof. See [KKTU19a, Theorem 2.2] □

Example 2.2.23. *Let L/K be a finite Galois extension of number fields with Galois group G. Then $K[G]$, the Hopf algebra with underlying subgroup $\rho(G)$ is not isomorphic to $L[\lambda(G)]^G$ as K-Hopf algebras, unless G is abelian when the Hopf algebras are actually equal. This is because the action of G on $\rho(G)$ is trivial but the action of G on $\lambda(G)$ is conjugation so is not trivial when G is not abelian.*

2.2.4 Separable algebras and orders

Now we present some general results that will allow us to find decompositions of Hopf algebras. We have discussed how two Hopf algebras can be isomorphic but act on an extension in different ways to give different Hopf-Galois structures. Even when two Hopf algebras are not isomorphic as Hopf algebras, they can be isomorphic as K-algebras. The following results allow us to understand when this is the case.

Definition 2.2.24. *Let K be a field and A a K-algebra. A is* semisimple *if it is the direct sum of a finite number of minimal left ideals. A is* separable *if for every extension field L of K, including K itself, $L \otimes_K A$ is a semisimple L-algebra.*

In particular, if an algebra is separable then it is semisimple.

Theorem 2.2.25. ***Artin-Wedderburn.*** *Let A be a semisimple ring. Then*

$$A \cong \bigoplus_{i=1}^{r} D_i^{n_i \times n_i}$$

for some division rings D_i where r is the number of simple A-modules and the n_i and D_i are determined up to isomorphism for each i.

This is only useful to us if our Hopf algebra is separable, however in many cases a Hopf algebra that gives a Hopf-Galois structure to an extension is separable.

Lemma 2.2.26. *Let L/K be any Galois extension with a Hopf algebra H giving a Hopf-Galois structure on the extension. Suppose the characteristic of K does not divide the degree of the extension. Then H is a separable K-algebra.*

Proof. See [Tru18, Lemma 4.2]. □

Thus every Hopf algebra has a decomposition of the form described in Theorem 2.2.25. We can understand such a decomposition of certain subrings. To study this we need to find the notion of an order.

Definition 2.2.27. *Let K be a number field with ring of integers $\mathfrak{O}_K$, and let A be a finite dimensional K-algebra. An $\mathfrak{O}_K$-order in A is a subring Λ of A satisfying the following conditions:*

- *the centre of Λ contains $\mathfrak{O}_K$,*
- *Λ is finitely generated as an $\mathfrak{O}_K$-module,*
- *$\Lambda \otimes_{\mathfrak{O}_K} K = A$.*

An $\mathfrak{O}_K$-order in A is called maximal *if it is not properly contained in any larger $\mathfrak{O}_K$-order in A.*

Example 2.2.28. *Let L/K be a finite Galois extension of number fields with group G. with rings of integers $\mathfrak{O}_L$ and $\mathfrak{O}_K$ respectively. Then the group ring $\mathfrak{O}_K[G]$ is an $\mathfrak{O}_K$-order in $K[G]$. Moreover, the Hopf algebra $L[N]^G$ has the $\mathfrak{O}_K$-order $\mathfrak{O}_L[N]^G$.*

We find that a Hopf algebra giving a Hopf-Galois structure on an extension will contain a unique maximal order, under certain hypotheses.

Proposition 2.2.29. *Let A be a commutative separable K-algebra. Then there exists a unique maximal $\mathfrak{O}_K$-order in A.*

Proof. See [CR81, 26.10]. □

2.2.5 Bases of Hopf algebras

We now present results that give us a technique to find the algebra decompositions of our Hopf algebras, along with explicit bases that respect the decompositions. We first present a result that gives an $\mathfrak{O}_K$-basis of $\mathfrak{O}_L[N]^G$.

Lemma 2.2.30. *Let L/K be a Galois extension of fields with K^{alg} the algebraic closure of K. Let G be the Galois group of L/K and N be the underlying subgroup of some Hopf-Galois structure on L/K. Further, let $\mathfrak{O}_L$ and $\mathfrak{O}_K$ be the rings of integers of L and K respectively. Let $n_1, \ldots, n_r$ be the representatives of the G-orbits of N. For each $i \in \{1, \ldots, r\}$ let L_i be the fixed field of $S_i = Stab_G(n_i) \leq G$, and let $x_{i,1}, \ldots, x_{i,r_i}$ be a K-basis of L_i. Finally, for $1 \leq i \leq r$ and $1 \leq j \leq r_i$, set*

$$a_{i,j} := \sum_{g \in G/S_i} g(x_{i,j})\, {}^g n_i.$$

Then

1. *The elements $a_{i,j}$, $1 \leq i \leq r$, $1 \leq j \leq r_i$, form a K-basis of $L[N]^G$.*

2. *If, for each* $i \in \{1, \ldots, r\}$ *the elements* $x_{i,1}, \ldots, x_{i,r_i}$ *form an* $\mathfrak{O}_K$*-basis of* $\mathfrak{O}_{L_i}$ *then the elements* $a_{i,j}$, $1 \leq i \leq r$, $1 \leq j \leq r_i$, *form an* $\mathfrak{O}_K$*-basis of* $\mathfrak{O}_L[N]^G$.

Proof. See [BB99, Lemma 2.1]. □

We now wish to present a result that gives an $\mathfrak{O}_K$-basis of the maximal $\mathfrak{O}_K$-order in $L[N]^G$, for N abelian, which is only sometimes equal to $\mathfrak{O}_L[N]^G$. In order to do this we first present some useful information regarding the dual group.

Definition 2.2.31. *Let* $\hat{N}$ *denote the* dual group *of the group* N*, defined as the group of* K^{alg}*-characters* χ *of* N*. We note that a group* G *with an action on* N *acts on* $\hat{N}$ *by*

$$({}^{g}\chi)(n) := g(\chi({}^{g^{-1}}n))$$

for $\chi \in \hat{N}$, $g \in G$ *and* $n \in N$.

The *primitive idempotent* in $\prod_{\chi \in \hat{N}} K^{\text{alg}}$ has entry 1 in the component of χ and 0 elsewhere. Then we denote the corresponding element of $K^{\text{alg}}[N]$ by e_χ. Then

$$e_\chi = \frac{1}{|N|} \sum_{n \in N} \chi(n^{-1})n.$$

Finally, note that ${}^{g}(e_\chi) = e_{({}^{g}\chi)}$ for each $g \in G$ and $\chi \in \hat{N}$.

The following result applies only to abelian underlying subgroups N, though the techniques presented here naturally extend to nonabelian N by replacing the orbit representatives of the dual group by the characters of N.

Lemma 2.2.32. *Let* L/K *be a finite Galois extension of fields with group* G *and a Hopf-Galois structure that has abelian underlying subgroup* N*. Suppose* $\text{char}(K) \nmid |N|$*. Let* $\chi_1, \ldots, \chi_s \in \hat{N}$ *be a set of representatives for the* G*-orbits of* $\hat{N}$*. For each* $k \in \{1, \ldots, s\}$*, let* $\hat{L}_k$ *denote the fixed field of*

$S_k = Stab_G(\chi_k) \leq G$, and let $y_{k,1}, \ldots, y_{k,s_k}$ be a K-basis of $\hat{L}_k$. For $1 \leq k \leq s$ and $1 \leq l \leq s_k$, set

$$\hat{a}_{k,l} := \sum_{g \in G/S_k} g(y_{k,l})\, {}^g e_{\chi_k}.$$

Then

1. *The elements $\hat{a}_{k,l}$, $1 \leq k \leq s$, $1 \leq l \leq s_k$, form a K-basis of $L[N]^G$ and*

$$H = \prod_{k=1}^{s} \hat{L}_k.$$

2. *If, for each $k \in \{1, \ldots, s\}$, the elements $y_{k,1}, \ldots, y_{k,s_k}$ form an $\mathfrak{O}_K$-basis of $\mathfrak{O}_{\hat{L}_k}$ then the elements $\hat{a}_{k,l}$, $1 \leq k \leq s$, $1 \leq l \leq s_k$, form an $\mathfrak{O}_K$-basis of the maximal $\mathfrak{O}_K$-order in $L[N]^G$.*

Proof. See [BB99, Lemma 2.2]. □

Remark 2.2.33. *It is possible that the images of the characters of N do not necessarily lie in the extension L. In this case fix an algebraic closure of K, K^{alg}, and let $\Omega = Gal(K^{alg}/K)$. Then the group algebra $K^{alg}[N]$ has a basis of mutually orthogonal idempotents, each corresponding to an element of $\hat{N}$. The action of Ω on $K^{alg}[N]$ permutes these idempotents and so one can form Ω-invariant linear combinations of them. Then, since $L[N]^G = K^{alg}[N]^\Omega$, such linear combinations must be a K-basis of $L[N]^G$, that corresponds to the Artin-Wedderburn decomposition found in Lemma 2.2.32.*

2.2.6 Quotient structures

We now take a small detour to consider "quotient structures" as a manner of relating structures on an extension to structures on a subextension.

Let L/K be a Galois extension of fields. Let $H = L[N]^G$ be a Hopf algebra giving a Hopf-Galois structure on the extension. If P is a G-stable

subgroup of N then $L[P]^G$ is a Hopf subalgebra of $L[N]^G$, and we define its *fixed field* to be

$$L^P := \{x \in L \,|\, z \cdot x = \varepsilon(z)x \text{ for all } z \in L[P]^G\}.$$

Now suppose P is normal in N. Since P is normalized by $\lambda(G)$ it corresponds to a subgroup of G under an injection Ψ, mapping from subgroups of N normalized by $\lambda(G)$ to subgroups of G defined by $\Psi(P) = \mathrm{Orb}_P(1_G) = J$ (see [KKTU19b, Lemma 2.6]). J can be described in two further natural forms: $J = \mathrm{Gal}(L/L^P)$ and $J = \{q^{-1}(1_G) | q \in P\}$ (see [KKTU19b, Theorem 2.4]). If J is normal in G it makes sense to consider G/J and we find that $\lambda(G)/\lambda(J)$ and N/P act regularly on the cosets $\{g_1J, ..., g_mJ\}$ as permutation groups (see [KKTU19b, Lemma 2.7]).

We wish to recognise N/P as an underlying subgroup of a Hopf-Galois structure on L/K. It is therefore helpful to find the following

Lemma 2.2.34. *$\lambda(G)/\lambda(J)$ normalizes N/P as a subgroup of $Perm(\{g_iJ\})$.*

Proof. See [KKTU19b, Lemma 2.8]. □

With this we may find that the Hopf algebra $L^P[N/P]^{G/J}$ gives a Hopf-Galois structure on the extension L^P/K (see [KKTU19b, Theorem 2.9]). We may remove the assumption that J be normal in G, but still impose the condition that P be normal in N. Doing this, we find that the obvious generalisation of Lemma 2.2.34 does hold, that is:

Theorem 2.2.35. *The Hopf algebra $L[N/P]^G$ gives a Hopf-Galois structure on L^P/K.*

Proof. See [KKTU19b, Theorem 2.10]. □

So, if P is a normal subgroup of N then the Hopf algebra $L[N/P]^G$ gives a Hopf-Galois structure on the extension L^P/K, which itself may not be

Galois. In fact, it is shown that G acts on N/P by ${}^g(\eta P) = ({}^g\eta)P$ for all $g \in G$ and $\eta \in N$, and that the Hopf algebra $L[N/P]^G$ acts on L^P by

$$\left(\sum_{\bar{\eta}\in N/P} c_{\bar{\eta}}\bar{\eta}\right)\cdot x = \sum_{\bar{\eta}\in N/P} c_{\bar{\eta}}\eta^{-1}(1_G)[x] \tag{2.3}$$

for all $x \in L^P$ where $\bar{\eta} = \eta P$.

2.2.7 Quaternion algebras

The final part of the section presents some more specific results regarding quaternion algebras, that will later appear in some of the Artin-Wedderburn decompositions of Hopf algebras. For this subsection let K be a field of characteristic zero.

Definition 2.2.36. *Let $U, V \in K^\times$. We define the* quaternion algebra $(U,V)_K$ *to be the K-algebra on two generators u, v whose relations are defined by*

$$u^2 = U, \quad v^2 = V, \quad uv = -vu.$$

From here we present some useful results about quaternion algebras.

Proposition 2.2.37. *$\{1, u, v, uv\}$ is a K-basis for $(U,V)_K$.*

Proof. See [Lam05, Chapter III, Proposition 1.0]. □

Proposition 2.2.38. *We have the following useful properties.*

1. *$(U,V)_K \cong (Ux^2, Vy^2)_K$ for any $U, V, x, y \in K^\times$.*

2. *$(-1,1)_K \cong M_2(K)$.*

3. *The centre of $(U,V)_K$ is K.*

4. $(U,V)_K$ *is a simple algebra, that is it has no nontrivial ideals.*

Proof. See [Lam05, Chapter III, Proposition 1.1]. □

Proposition 2.2.39. *Algebras with the properties (3) and (4) above are called* central simple algebras *over* K*. If two* K*-algebras are central simple algebras over* K *then so is their tensor product.*

Proof. See [Lam05, Chapter IV, Theorem 1.2(3)]. □

We now lay out some definitions in order to finally define the norm on a quaternion algebra.

Definition 2.2.40. *A* quaternion *is an element of a quaternion algebra. A quaternion* $x = c_0 + c_1u + c_2v + c_3uv \in (U,V)_K$ *is called a* pure quaternion *if* $c_0 = 0$*.*

Definition 2.2.41. *We denote and define the* conjugate *of a quaternion* $x = c_0 + c_1u + c_2v + c_3uv$ *by* $\bar{x} = c_0 - c_1u - c_2v - c_3uv$*.*

Definition 2.2.42. *We define the norm of a quaternion* x *to be* $N(x) = x\bar{x}$*. For* $x = c_0 + c_1u + c_2v + c_3uv$ *the norm of* x *is given explicitly as*

$$N(x) = c_0^2 - c_1^2U - c_2^2V + c_3^2UV.$$

Having defined the norm we now state some useful properties of the map.

Proposition 2.2.43. *We have the following properties of the norm.*

1. For $x, y \in (U,V)_K$*,* $N(xy) = N(x)N(y)$*.*

2. $x \in (U,V)_K$ *is invertible if and only if* $N(x) \neq 0$*.*

Proof. See [Lam05, Chapter III, Proposition 2.4]. □

We can now state a theorem that describes when two quaternion algebras are isomorphic.

Theorem 2.2.44. *The following statements are equivalent:*

1. $(U, V)_K$ *and* $(U', V')_K$ *are isomorphic as* K*-algebras.*

2. *The norms on* $(U, V)_K$ *and* $(U', V')_K$ *are equivalent as quadratic forms.*

3. *The norms on the pure quaternions of* $(U, V)_K$ *and* $(U', V')_K$ *are equivalent as quadratic forms.*

Proof. See [Lam05, Chapter III, Theorem 2.5]. □

We now define a group of equivalence classes of quaternion algebras so that we can rephrase previous results in a more useful manner.

Definition 2.2.45. *We may adorn the set of isomorphism classes of central simple division algebras over* F *with a multiplication such that*

$$[A][B] = [C]$$

where C *is the component of* $A \otimes_K B$ *that is a division algebra. This yields a group called the* Brauer group *of* K*, denoted by* $\mathrm{Br}(K)$*.*

Remark 2.2.46. *The Brauer group is often defined by setting up an equivalence relation between central simple algebras over* K *and proving the set of equivalence classes has a group structure. One finds that these two formulations are equivalent (see [Lam05, Chapter IV, Proposition 1.4]).*

In particular, two quaternion algebras $(U, V)_K$ *and* $(U', V')_K$ *are isomorphic as* K*-algebras if and only if* $[U, V] = [U', V']$ *in* $\mathrm{Br}(K)$*, where* $[U, V]$ *in* $\mathrm{Br}(K)$ *is the isomorphism class of* $(U, V)_K$*. Moreover the identity class* $[1, 1]$ *corresponds to* $M_2(K)$*.*

Finally we state a useful property of the classes in the Brauer group.

Theorem 2.2.47. *For $U, V, W \in K^{alg}$, we have*

$$(U, V)_K \otimes (U, W)_K \cong (U, VW)_K \otimes_K M_2(K).$$

This is equivalent to

$$[U, V][U, W] = [U, VW]$$

in the Brauer group.

Proof. See [Lam05, Chapter III, Theorem 2.11]. □

2.3 Hopf-Galois module theory

In this section we investigate Hopf-Galois module theory, starting with the general definition of an associated order as a generalisation of the classical group ring $K[G]$. We will present the theory of Childs and Hurley, the Hopf-Galois module structure of opposite structures, and finally some general results under the assumption the extension is tame.

2.3.1 Associated order and Hopf orders

We first recall the definition of an order in general from Definition 2.2.27, and what it means for an order to be maximal. We recall from Proposition 2.2.29 that a Hopf-Galois structure with abelian underlying subgroup, of extensions we will be concerned with in this thesis, will contain a unique maximal order.

In Hopf-Galois theory we can define a specific type of order that will give us a strong general result later.

Definition 2.3.1. *Let R be a Dedekind domain with field of fractions K of characteristic zero. Let H be a finite K-Hopf algebra. An R-order in H is called a* Hopf order *if it is an R-Hopf algebra with operations inherited from those on H.*

Now we define the most important type of $\mathfrak{O}_K$ order that is our replacement for $\mathfrak{O}_K[G]$ in the classical structure.

Definition 2.3.2. *Suppose H is a finite K-Hopf algebra and L/K is an H-Hopf-Galois extension of local or global fields. Let $\mathfrak{O}_L$ and $\mathfrak{O}_K$ be the rings of integers of K and L respectively. The* associated order *of $\mathfrak{O}_L$ in H is*

$$\mathfrak{A}_H = \{h \in H \mid h(\mathfrak{O}_L) = \mathfrak{O}_L\}.$$

The associated order is an $\mathfrak{O}_K$-order in H but need not be a Hopf order. For instance, if L is a wild abelian Galois extension of $\mathbb{Q}$ then $\mathfrak{A}_H$ is not necessarily a Hopf order. Still, the associated order is the best $\mathfrak{O}_K$-order to consider in place of $\mathfrak{O}_K[G]$ due to the following.

Proposition 2.3.3. *Let L/K be an H-Hopf-Galois extension, $\mathfrak{H} \subset \mathfrak{A}_H$ an order over $\mathfrak{O}_K$ in H, and suppose $\mathfrak{O}_L$ is $\mathfrak{H}$-free of rank one. Then $\mathfrak{H} = \mathfrak{A}_H$.*

Proof. See [Chi00, Propostion 12.5]. □

By considering the associated order we can obtain results for extensions we previously couldn't. For instance Leopoldt found that if L is any abelian extension of $\mathbb{Q}$, then the ring of integers $\mathfrak{O}_L$ of L is a free module of rank one over its associated order in $\mathbb{Q}[G]$ (see [Tho10, pp 165]). However, when the associated order is a Hopf order we have a strong claim due to Childs:

Theorem 2.3.4. *Suppose L/K is a finite H-Hopf-Galois extension of local (resp. global) fields. If $\mathfrak{A}_H$ is a Hopf order in H, then $\mathfrak{O}_L$ is free (resp. locally free) of rank one over $\mathfrak{A}_H$.*

Proof. See [Chi00, Theorem 12.7]. □

2.3.2 Childs-Hurley theory

Here we present some theory of Childs and Hurley that concerns the structure of $\mathfrak{O}_L$ in certain extensions of local fields.

Theorem 2.3.4 says that if L/K is a finite H-Hopf-Galois extension of local fields with the associated order a Hopf order then $\mathfrak{O}_L$ is free over the associated order. Under certain additional hypotheses we can determine an explicit generator of $\mathfrak{O}_L$ over $\mathfrak{A}_H$.

Definition 2.3.5. *A ring is said to be a* local ring *if it contains a unique maximal (left) ideal.*

Definition 2.3.6. *Let R be a commutative ring with unity and H an R-Hopf algbera. An element $\theta \in H$ is a* left integral *if for all $x \in H$ we have $x\theta = \varepsilon(x)\theta$. An element $\theta \in H$ is a* right integral *if for all $x \in H$, $\theta x = \varepsilon(x)\theta$.*

If R is a principal ideal domain then the module of left integrals of H is a free R-module of rank one. That is, if I is the set of all integrals in R then $I = R\theta$ for some integral θ. This leads to a result that determines an explicit generator when the associated order is a local Hopf order.

Theorem 2.3.7. ***(Childs and Hurley).*** *Let L/K be an H-Hopf-Galois extension of local fields and suppose $\mathfrak{A}_H$ is a local Hopf order in H. Let θ generate the module of integrals of $\mathfrak{A}_H$. If $t \in \mathfrak{O}_L$ is such that $\theta \cdot t = 1$ then $\mathfrak{O}_L = \mathfrak{A}_H \cdot t$.*

Proof. See [Chi00, Proposition 14.7]. □

Finally, we present an alternative characterisation of a local ring.

Theorem 2.3.8. *A ring R is local if and only if for all x in R, either x or $1 - x$ is a unit of R.*

Proof. See [Lam13, §19, Theorem 19.5, part 5″]. □

2.3.3 Opposite structures

Here we briefly recall the notion of opposite structures and find how this relates to the Hopf-Galois module structure of finite Galois extensions. Recall the definition of opposite structures from Definition 2.2.17.

Theorem 2.3.9. *Let L/K be a finite Galois extension of number fields or $\mathfrak{p}$-adic fields and let H and H' be Hopf algebras giving Hopf-Galois structures on L/K whose actions commute. Let $\mathfrak{A}$ and $\mathfrak{A}'$ be the associated orders of $\mathfrak{O}_L$ in H and H' respectively. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module if and only if it is a free $\mathfrak{A}'$-module.*

Proof. See [Tru18, Theorem 1.2]. □

In particular we have the following:

Corollary 2.3.10. *If L/K is an extension of number fields then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module if and only if it is a locally free $\mathfrak{A}'$-module.*

Proof. See [Tru18, Corollary 1.3]. □

2.3.4 Tame extensions

In the final part of this section we will present some theory of Hopf-Galois module theory useful for tame extensions in particular. We first present results that enable us to understand the relationship between $\mathfrak{O}_L[N]^G$ and $\mathfrak{A}_H$ where H is the Hopf algebra $L[N]^G$.

Proposition 2.3.11. *Let L/K be a Galois extension of number fields and suppose that L/K is H-Galois for some Hopf algebra $H = L[N]^G$ with underlying subgroup N of $Perm(G)$. We have that $\mathfrak{O}_L[N]^G \subseteq \mathfrak{A}_H$.*

Proof. See [Tru11, Proposition 2.5]. □

We now present results that state in some circumstances that the completion of the associated order is the completion of $\mathfrak{O}_L[N]^G$.

Proposition 2.3.12. *Let L/K be a finite extension of number fields and let H be a commutative Hopf algebra giving a Hopf-Galois structure on the extension. For any prime $\mathfrak{p}$ lying above a prime number p that does not divide the order of the extension we have that $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is the unique maximal order in H and so is equal to $\mathfrak{A}_{H,\mathfrak{p}}$. Moreover, $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. See [Tru11, Theorem 4.3, Theorem 4.4]. □

Theorem 2.3.13. *Let L/K be a finite Galois extension of number fields with group G, and suppose that L/K is H-Galois for the Hopf algebra $H = L[N]^G$. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which is unramified in $\mathfrak{O}_L$. Then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.*

Proof. See [Tru11, Theorem 5.4]. □

We define a type of extension that allows us to present a result which will then apply to a case useful for this thesis.

Definition 2.3.14. *Let L/K be a Galois extension of number fields. We say the extension is* domestic *if no prime of $\mathfrak{O}_K$ lying above a prime number dividing $[L : K]$ ramifies in $\mathfrak{O}_L$.*

Theorem 2.3.15. *Let L/K be a finite domestic Galois extension of number fields. Suppose that L/K is H-Galois for some commutative Hopf algebra H. Then $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.*

Proof. See [Tru11, Theorem 5.9]. □

In particular, we get the following corollary.

Corollary 2.3.16. *Let L/K be a finite Galois extension of number fields of prime power degree which is at most tamely ramified. Suppose that L/K is H-Galois for some commutative Hopf algebra H. Then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.*

Proof. Since L/K has prime power degree, the assumption that the extension is tamely ramified is equivalent to the assumption that the extension is domestic. See [Tru11, Corollary 5.10]. □

2.4 Locally free class groups

In the final section of this chapter we present the theory of locally free class groups that provides us with machinery to understand the global module structure of $\mathfrak{O}_L$ from the local module structure. The discussion that follows is valid for number fields in general, however, we specialise to the base field $K = \mathbb{Q}$.

Let A be a $\mathbb{Q}$-algebra and let Λ be a $\mathbb{Z}$-order in A. A Λ-*lattice* is a finitely generated free $\mathbb{Z}$-module which is also a Λ-module. If X is a Λ-lattice then for each prime number p we write $X_p = \mathbb{Z}_p \otimes_{\mathbb{Z}} X$ and $\Lambda_p = \mathbb{Z}_p \otimes_{\mathbb{Z}} \Lambda$, and then X_p is a Λ_p-lattice.

Definition 2.4.1. *We say that X is a* locally free Λ*-lattice of rank 1 if X_p is a free Λ_p-module of rank 1 for each p - a generalisation of Definition 2.1.17. If X and Y are locally free Λ-lattices of rank 1, then we say that X and Y are* stably isomorphic *if*

$$X \oplus \Lambda^k \cong Y \oplus \Lambda^k$$

for some $k \geq 0$. In particular we say that X is stably free *over Λ if $X \oplus \Lambda^k = \Lambda^k$ for some $k \geq 0$.*

In general being stably free is weaker than being free but we have the following:

Proposition 2.4.2. ***The Eichler Condition.*** *Suppose that no Artin-Wedderburn component of A that is a quaternion algebra $(x, y)_{\mathbb{Q}}$ is a totally definite quaternion algebra over $\mathbb{Q}$, that is, $(x, y)_{\mathbb{R}} \cong (-1, -1)_{\mathbb{R}}$. Then stably free Λ-modules are free.*

Proof. See [CR81, page 718]. □

Definition 2.4.3. *The set of stable isomorphism classes of locally free* Λ*-lattices forms an abelian group with operation*

$$[X] + [Y] = [X \oplus Y],$$

called the locally free class group *of* Λ*, denoted* $\mathrm{Cl}(\Lambda)$*.*

Remark 2.4.4. *A* Λ*-lattice,* X*, is stably free if and only if it has trivial class in* $\mathrm{Cl}(\Lambda)$*.*

Definition 2.4.5. *We denote and define the* idèle group *of* A *by*

$$\mathbb{J}(A) = \Big\{ (a_p)_p \in \prod_p A_p^\times \;\Big|\; a_p \in \Lambda_p^\times \text{ for almost all } p \Big\}.$$

This can be shown to be independent of the choice of the order Λ*. We further define two subgroups of* $\mathbb{J}(A)$*. We denote and define the subgroup of* unit idèles *of* Λ *by*

$$\mathbb{U}(\Lambda) = \prod_p \Lambda_p^\times = \{ (a_p)_p \,|\, a_p \in \Lambda_p^\times \text{ for all } p \}.$$

and the subgroup of principal idèles $\{(a)_p \,|\, a \in A^\times\}$ *which we denote* $A^\times$ *when the context is clear.*

We now define a map from A to its centre to be able to give a useful description of the locally free class group.

Let A be a $\mathbb{Q}$-algebra with centre C. Write $A = A_1 \times A_2 \times \cdots \times A_t$ for its decomposition into simple algebras. Denote by C_i the centre of the simple algebra A_i and note that C_i is isomorphic to some extension of $\mathbb{Q}$. Let B be one of the A_i, a simple algebra of square dimension, say m^2 over its centre. There exists some finite extension, E say, of $\mathbb{Q}$ such that $E \otimes_{\mathbb{Q}} B \cong M_m(E)$ and denote the image of $1 \otimes b$ by T_b.

Definition 2.4.6. ***(Reduced Norm.)*** *We define the* reduced characteristic polynomial *of b to be the characteristic polynomial of T_b. We then define the* reduced norm *of b to be the constant term of the reduced characteristic polynomial, denoted* $\mathrm{nr}(b)$. *Finally, we define the* reduced norm on A *to be the map* $\mathrm{nr} : A \to C$ *for which we apply the reduced norm component-wise on each of the A_i, that is*

$$\mathrm{nr}((a_1, a_2, \ldots, a_t)) = (\mathrm{nr}(a_1), \mathrm{nr}(a_2), \ldots, \mathrm{nr}(a_t)).$$

Example 2.4.7. *Let $(U, V)_{\mathbb{Q}}$ be a quaternion algebra which has centre $\mathbb{Q}$, and note that it is a simple algebra over $\mathbb{Q}$. Let $z \in (U, V)_{\mathbb{Q}}$. There is a finite extension E of $\mathbb{Q}$ such that $E \otimes (U, V)_{\mathbb{Q}} \cong M_2(E)$ so the reduced characteristic polynomial of z is monic with coefficients in $\mathbb{Q}$ and of degree 2, with z as a root. Such a polynomial is unique and we can write a polynomial down that fits these properties: let $\bar{z}$ be the quaternion conjugate of z and consider the polynomial*

$$(x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z}.$$

This is the reduced characteristic polynomial of z and the reduced norm of z is the constant term $z\bar{z}$ which is the same as the quaternion norm of z defined in Definition 2.2.42.

The reduced norm map $\mathrm{nr} : A \to C$, where C is the centre of A, induces a reduced norm map $\mathrm{nr} : \mathbb{J}(A) \to \mathbb{J}(C)$, and we let $\mathbb{J}_0(A)$ be the kernel of this map. That is

$$\mathbb{J}_0(A) = \{(a_p)_p \in \mathbb{J}(A) \mid \mathrm{nr}(a_p)_p = 1\}.$$

Theorem 2.4.8. *In the notation established above we have*

$$\mathrm{Cl}(\Lambda) \cong \frac{\mathbb{J}(A)}{\mathbb{J}_0(A)A^{\times}\mathbb{U}(\Lambda)}.$$

Proof. See [CR87, Theorem 49.22]. □

We wish to describe the class of a locally free Λ-lattice in $\mathrm{Cl}(\Lambda)$ and in order to do so we require an additional assumption. Since X is a Λ-module, $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is a module over $\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$, which is equal to A. We assume that $\mathbb{Q} \otimes_{\mathbb{Z}} X$ is actually a free A-module of rank 1. Then let x be a free generator of $\mathbb{Q} \otimes_{\mathbb{Z}} X$ as an A-module, and for each p, let x_p be a free generator of X_p as a Λ_p-module. Then for each p, there exists a unique element $a_p \in A_p$ such that $a_p \cdot x = x_p$.

Proposition 2.4.9. *The class of X in $\mathrm{Cl}(\Lambda)$ corresponds to the class of the idèle $(a_p)_p$ in the quotient group*

$$\frac{\mathbb{J}(A)}{\mathbb{J}_0(A)A^\times \mathbb{U}(\Lambda)}.$$

Proof. See [CR87, Proposition 49.22]. □

We can obtain a simpler description by applying reduced norms to the idèle group $\mathbb{J}(A)$ and the subgroups studied so far. We have $\mathrm{nr}(\mathbb{J}(A)) = \mathbb{J}(C)$ and $\mathrm{nr}(\mathbb{U}(\Lambda)) = \prod_p \mathrm{nr}(\Lambda_p^\times)$. In general $\mathrm{nr}(A^\times)$ is a (possibly proper) subgroup C^+ of $C^\times$ (see [CR87, §45A]). Putting these together and applying the third isomorphism theorem we obtain the following.

Theorem 2.4.10. *We have*

$$\mathrm{Cl}(\Lambda) \cong \frac{\mathbb{J}(C)}{C^+ \prod_p \mathrm{nr}(\Lambda_p^\times)}.$$

Proof. See [CR87, Theorem 49.17]. □

Proposition 2.4.11. *The class of X in $\mathrm{Cl}(\Lambda)$ corresponds to the class of the reduced norm of the idèle $(a_p)_p$ in the quotient group*

$$\frac{\mathbb{J}(C)}{C^+ \prod_p \mathrm{nr}(\Lambda_p^\times)}.$$

Chapter 3

Hopf-Galois structures

In this chapter we determine the Hopf-Galois structures admitted by a quaternionic extension, and study properties of the corresponding Hopf algebras.

We shall reserve K for a certain intermediate field so we change notation: let L/F be a finite Galois extension of fields with group G. Furthermore, let H be a finite dimensional F-Hopf algebra, such that H gives a Hopf-Galois structure on L/F.

Since a Hopf-Galois structure on an extension L/F consists of a Hopf algebra H and an action of H on L, it is possible for distinct Hopf-Galois structures on L/F to involve Hopf algebras that are isomorphic, either as F-Hopf algebras or as F-algebras. These phenomena have recently been studied in papers such as [KKTU19b] and [KKTU19a]. In particular, [KKTU19a] studies in detail the Hopf-Galois structures admitted by a dihedral extension of fields of degree $2p$, where p is an odd prime. In this chapter we similarly analyse the Hopf-Galois structures admitted by a Galois extension of fields with Galois group isomorphic to Q_8, the quaternion group of order 8.

The results of this chapter have appeared in [TT19].

Recall Theorem 2.2.14, which classifies all of the Hopf-Galois structures admitted by a finite Galois extension of fields. Every Hopf algebra giving a Hopf-Galois structure onto the extension L/K has the form $H = L[N]^G$ for

some N described in the theorem that is called the underlying subgroup of the structure.

3.1 Structures on the extension

Let L/F be a quaternionic extension and let its Galois group G have generators σ and τ, that is

$$G = \langle \sigma, \tau \,|\, \sigma^4 = \tau^4 = 1, \sigma^2 = \tau^2, \sigma\tau = \tau\sigma^{-1} \rangle.$$

First, we recall Proposition 2.1.21 that states L/F has a unique biquadratic subextension which we label K.

The underlying subgroup of a structure must have order 8, the same as the Galois group. There are 5 isomorphism types of groups of order 8: the elementary abelian group $C_2 \times C_2 \times C_2$, $C_4 \times C_2$, the cyclic group C_8, the dihedral group D_4 and the quaternion group Q_8. A count of the Hopf-Galois structures admitted by L/F appears in [SV18, Table A.1], which we reproduce in Table 3.1 below. The same count appears in work of Crespo and Salguero [CS20, Table 3], as an application of an algorithm written in the computational algebra system Magma which gives all Hopf-Galois structures on separable field extensions of a given degree.

We now determine the regular subgroups of $\mathrm{Perm}(G)$ corresponding to these Hopf-Galois structures. We start with the subgroups corresponding to the Hopf-Galois structures of type $C_2 \times C_2 \times C_2$.

Lemma 3.1.1. *Let $s, t \in \{\sigma, \tau\}$ with $s \neq t$ and let $E_{s,t}$ be generated by $\lambda(s)\rho(t), \lambda(s^2)$, and $\lambda(t)\rho(st)$. Then $E_{s,t}$ is a regular subgroup of Perm(G) that is normalized by $\lambda(G)$ and isomorphic to $C_2 \times C_2 \times C_2$. The groups $E_{\sigma,\tau}$ and $E_{\tau,\sigma}$ are distinct, and are the underlying subgroups of the 2 Hopf-Galois structures of type $C_2 \times C_2 \times C_2$ on L/F.*

Type	Number of structures
$C_2 \times C_2 \times C_2$	2
$C_4 \times C_2$	6
C_8	6
Q_8	2
D_4	6

Table 3.1: The number of Hopf-Galois structures on a Quaternionic extension

Proof. The elements of $E_{s,t}$ are

$$1, \qquad \lambda(s)\rho(t), \qquad \lambda(t)\rho(st), \qquad \lambda(st)\rho(s),$$

$$\lambda(s^2), \quad \lambda(s^{-1})\rho(t), \quad \lambda(t^{-1})\rho(st), \quad \lambda((st)^{-1})\rho(s).$$

All of the non-identity elements above have order 2 in $\mathrm{Perm}(G)$, so $E_{s,t}$ is isomorphic to $C_2 \times C_2 \times C_2$. It is straightforward to verify that $E_{s,t} \subset \mathrm{Perm}(G)$. It is also straightforward to verify that $E_{s,t} \cdot 1_G = G$ since one need only list the obvious actions of each element on 1_G:

$$1, \quad st^{-1}, \quad s^{-1}, \quad t^{-1},$$

$$s^2, \quad st, \quad s, \quad t$$

respectively; hence $E_{s,t}$ is a regular subgroup of $\mathrm{Perm}(G)$. To show that $E_{s,t}$ is normalized by $\lambda(G)$, it is sufficient to show that it is normalized by $\lambda(s)$ and $\lambda(t)$. Using the fact that $\lambda(G)$ and $\rho(G)$ commute inside $\mathrm{Perm}(G)$, as stated in Remark 2.2.13, we have, for example

$$^{s}\lambda(s)\rho(t) = \lambda(sss^{-1})\rho(t) = \lambda(s)\rho(t)$$
$$^{t}\lambda(s)\rho(t) = \lambda(tst^{-1})\rho(t) = \lambda(s^{-1})\rho(t).$$

Similar calculations apply to the other elements, and so $E_{s,t}$ is normalized by $\lambda(G)$. Finally, we have $E_{s,t} \neq E_{t,s}$ since $\lambda(t)\rho(s)$ lies in $E_{t,s}$ but not in $E_{s,t}$. Referring to Table 3.1 we see that $E_{\sigma,\tau}$ and $E_{\tau,\sigma}$ are the underlying subgroups of the two Hopf-Galois structures of type $C_2 \times C_2 \times C_2$ on L/F. □

We now find the subgroups corresponding to the Hopf-Galois structures of type $C_4 \times C_2$ using a similar technique.

Lemma 3.1.2. *Let $s, t \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$ and let $A_{s,t}$ be generated by the permutations $\lambda(s)$ and $\rho(t)$. Then $A_{s,t}$ is a regular subgroup of Perm(G) that is normalized by $\lambda(G)$ and isomorphic to $C_4 \times C_2$. The 6 choices of the pair s, t yield distinct groups, and these are the underlying subgroups of the 6 structures of type $C_4 \times C_2$ on L/F.*

Proof. We have $\langle \rho(t), \lambda(s) \rangle \cong C_4 \times C_2$ since $\rho(t)$ and $\lambda(s)$ are both of order 4, commute with each other, and share the same square. It is straightforward to verify that $A_{s,t} \subset \mathrm{Perm}(G)$ and that for $g, h \in G$ we have $\lambda(g)\rho(h) \cdot 1_G = gh^{-1}$; hence $A_{s,t}$ is a regular subgroup of Perm(G). The verification that it is normalized by $\lambda(G)$ is very similar to the verification in Lemma 3.1.1, using the fact that $\rho(G)$ and $\lambda(G)$ commute inside Perm(G). To show that the six choices of the pair s, t yield distinct groups, note that for each such pair the group $A_{s,t}$ is the only one that contains $\lambda(s)$ and $\rho(t)$. Hence, by Table 3.1, the groups $A_{s,t}$ are the underlying subgroups of the 6 Hopf-Galois structures of type $C_4 \times C_2$. □

The subgroups corresponding to the Hopf-Galois structures of type C_8 cannot be described in terms of combinations of elements from $\lambda(G)$ and $\rho(G)$, since the order of any such element is at most 4.

Lemma 3.1.3. *Let $s, t \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$ and let $C_{s,t}$ be generated by the permutation $\eta_{s,t}$ defined in cycle notation by*

$$\eta_{s,t} = (1 \ s \ t \ (st)^{-1} \ \sigma^2 \ s^{-1} \ t^{-1} \ (st)).$$

Then $C_{s,t}$ is a regular subgroup of Perm(G) that is normalized by $\lambda(G)$ and isomorphic to C_8. The 6 choices of the pair s, t yield distinct groups, and these are the underlying subgroups of the 6 structures of type C_8 on L/F.

Proof. It is clear that $C_{s,t}$ is a subgroup of Perm(G) isomorphic to C_8. Moreover, we have $C_{s,t} \cdot 1_G = G$ since $\eta_{s,t}^k \cdot 1_G = 1_G$ if and only if $k \equiv 0 \pmod 8$. Thus $C_{s,t}$ is a regular subgroup of Perm(G). To show that $C_{s,t}$ is normalized by $\lambda(G)$, it is sufficient to show that it is normalized by $\lambda(s)$ and $\lambda(t)$. We have

$$\begin{aligned}
&\lambda(s)\eta_{s,t}\lambda(s^{-1}) \\
&\quad = (1\ s\ s^2\ s^{-1})(t\ st\ t^{-1}\ (st)^{-1})\eta_{s,t}(1\ s^{-1}\ s^2\ s)(t\ (st)^{-1}\ t^{-1}\ st) \\
&\quad = (1\ (st)^{-1}\ t^{-1}\ s\ s^2\ st\ t\ s^{-1}) \\
&\quad = \eta_{s,t}^3,
\end{aligned}$$

and similarly, $\lambda(t)\eta_{s,t}\lambda(t^{-1}) = \eta_{s,t}$. Therefore $C_{s,t}$ is normalized by $\lambda(G)$. It may be verified that each of the 6 choices of the pair s, t gives a permutation that differs from all powers of those of the other choices. Hence, by Table 3.1, the groups $C_{s,t}$ are the underlying subgroups of the 6 Hopf-Galois structures of type C_8. □

Having found the abelian underlying subgroups of the corresponding Hopf-Galois structures on our extension L/F we now find the structures of quaternionic type. To this end, recall $\lambda(G)$ and $\rho(G)$ from Example 2.2.16.

Lemma 3.1.4. *$\rho(G)$ and $\lambda(G)$ are the underlying subgroups of the two Hopf-Galois structures of type Q_8.*

Proof. As stated in Example 2.2.16, since G is non-abelian, $\rho(G)$ and $\lambda(G)$ are distinct regular subgroups of Perm(G) normalized by $\lambda(G)$. By Table 3.1, they are the underlying subgroups of the 2 Hopf-Galois structures of type Q_8. □

Finally, the subgroups corresponding to the Hopf-Galois structures of type D_4, the dihedral group of order 8, have a similar description to the groups $E_{s,t}$ and $A_{s,t}$.

Lemma 3.1.5. *Let $s, t \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$. Let $D_{s,\lambda}$ be generated by $\lambda(s)$ and $\lambda(t)\rho(s)$, and let $D_{s,\rho}$ be generated by $\rho(s)$ and $\lambda(s)\rho(t)$. Then $D_{s,\lambda}$ and $D_{s,\rho}$ do not depend upon the choice of t, and are regular subgroups of Perm(G) that are normalized by $\lambda(G)$ and isomorphic to D_4. The 3 choices of s yield 6 distinct groups, and these are the underlying subgroups of the Hopf-Galois structures of type D_4 on L/F.*

Proof. For a fixed choice of t the elements of $D_{s,\lambda}$ are

$$1,\ \lambda(s),\ \lambda(s^2),\ \lambda(s^{-1}),\ \lambda(t)\rho(s),\ \lambda(st)\rho(s),\ \lambda(t^{-1})\rho(s),\ \lambda((st)^{-1})\rho(s).$$

We see immediately that using st in place of t yields the same group, that $\lambda(s)$ has order 4, $\lambda(t)\rho(s)$ has order 2, and that these elements anticommute. Therefore $D_{s,\lambda} \cong D_4$. It is straightforward to verify that $D_{s,\lambda} \subset \mathrm{Perm}(G)$ and that $D_{s,\lambda} \cdot 1_G = G$; hence $D_{s,\lambda}$ is a regular subgroup of Perm(G). The verification that it is normalized by $\lambda(G)$ is very similar to the verifications in Lemma 3.1.1 and Lemma 3.1.2, using the fact that $\rho(G)$ and $\lambda(G)$ commute inside Perm(G). Similarly, $D_{s,\rho}$ is a regular subgroup of Perm(G) that is isomorphic to D_4 and normalized by $\lambda(G)$. To show that the 3 choices of s yield 6 distinct groups, note that for each s the group $D_{s,\lambda}$ is the only one that contains $\lambda(s)$ and that $D_{s,\rho}$ is the only one that contains $\rho(s)$. Hence, by Table 3.1, the groups $D_{s,\lambda}$ and $D_{s,\rho}$ are the underlying subgroups of the 6 Hopf-Galois structures of type D_4. □

Remark 3.1.6. *For every regular subgroup N of Perm(G) corresponding to a Hopf-Galois structure on L/F we have $\rho(\sigma^2) \in N$, and so $Z(\rho(G)) \subseteq \rho(G) \cap N$. Clearly this is the case for $N = \rho(G)$ and $N = \lambda(G)$, and it is easy to verify that it holds for $N = E_{s,t}, A_{s,t}, D_{s,\lambda}$, and $D_{s,\rho}$ (for all valid*

choices of s, t) from the definitions of these groups. Finally, we can verify that it holds for the groups $C_{s,t}$ (for all valid choices of s, t) by computing $\eta_{s,t}^4 = \rho(\sigma^2)$ in these cases.

3.2 Hopf algebra isomorphisms

In this section we determine which of the Hopf algebras giving Hopf-Galois structures on L/F are isomorphic as F-Hopf algebras. Recall that in Theorem 2.2.22, Koch, Kohl, Underwood and Truman outline the following criterion for two Hopf algebras arising from the Greither-Pareigis correspondence to be isomorphic as Hopf algebras: let N_1 and N_2 be underlying subgroups of two Hopf-Galois structures on L/F. Then $L[N_1]^G \cong L[N_2]^G$ as F-Hopf algebras if and only if there exists a G-equivariant isomorphism $f : N_1 \xrightarrow{\sim} N_2$. In particular, no two Hopf algebras of different types may be isomorphic as F-Hopf algebras.

We now determine which of our Hopf Algebras are isomorphic. We consider the isomorphism classes of the underlying subgroups individually. We start with the elementary abelian groups.

Lemma 3.2.1. *The Hopf algebras giving the two Hopf-Galois structures of type $C_2 \times C_2 \times C_2$ are isomorphic to each other as Hopf algebras. That is, $L[E_{\sigma,\tau}]^G \cong L[E_{\tau,\sigma}]^G$ as Hopf algebras.*

Proof. Recall the definition of $E_{s,t}$ from Lemma 3.1.1 with non-trivial G-orbits

$$\{\lambda(s)\rho(t), \lambda(s^{-1})\rho(t)\},$$

$$\{\lambda(t)\rho(st), \lambda(t^{-1})\rho(st)\}$$

and

$$\{\lambda(st)\rho(s), \lambda((st)^{-1})\rho(s)\}$$

with stabilisers $\langle s\rangle$, $\langle t\rangle$ and $\langle st\rangle$ respectively. Let the map $f : E_{s,t} \to E_{t,s}$ be defined by

$$f : \begin{cases} \lambda(s)\rho(t) & \mapsto & \lambda(s)\rho((st)^{-1}) \\ \lambda(s^2) & \mapsto & \lambda(s^2) \\ \lambda(t)\rho(st) & \mapsto & \lambda(t)\rho(s). \end{cases}$$

The map is an isomorphism by construction and is G-equivariant since it maps a representative of the orbit with stabiliser s, t and st in $E_{s,t}$ to a representative of s, t and st, respectively, in $E_{t,s}$. □

Now we find that for the Hopf-Galois structures of type $C_4 \times C_2$ the Hopf algebra isomorphism classes are determined by the choice of s and so there are 3 isomorphically distinct pairs of isomorphic Hopf algebras.

Lemma 3.2.2. *Let $s, s', t, t' \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$ and $s' \neq t'$. We have $L[A_{s,t}]^G \cong L[A_{s',t'}]^G$ if and only if $s = s'$.*

Proof. Recall the definition of $A_{s,t}$ from Lemma 3.1.2. The non-trivial G-orbits of $A_{s,t}$ are $\{\lambda(s), \lambda(s^{-1})\}$ and $\{\lambda(s)\rho(t), \lambda(s^{-1})\rho(t)\}$ both with stabiliser $\langle s\rangle$. Therefore if $s \neq s'$ then there cannot be a G-equivariant isomorphism between $A_{s,t}$ and $A_{s',t'}$ for any choices of t, t'. For fixed s, t and t' satisfying $s \neq t$ and $s \neq t'$, let the map $f : A_{s,t} \to A_{s,t'}$ be defined by

$$f : \begin{cases} \lambda(s) & \mapsto & \lambda(s) \\ \rho(t) & \mapsto & \rho(t'). \end{cases}$$

Then f is a G-equivariant isomorphism by construction following the same reasoning as in the proof of Lemma 3.2.1. □

With a nearly identical argument we now give the result for Hopf-Galois structures of type C_8.

Lemma 3.2.3. *Let $s, s', t, t' \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$ and $s' \neq t'$. We have $L[C_{s,t}]^G \cong L[C_{s',t'}]^G$ as Hopf algebras if and only if $t = t'$.*

Proof. Recall the definition of $C_{s,t}$ from Lemma 3.1.1. The nontrivial G-orbits of $C_{s,t}$ are $\{\eta_{s,t}, \eta_{s,t}^3\}$, $\{\eta_{s,t}^2, \eta_{s,t}^6\}$ and $\{\eta_{s,t}^5, \eta_{s,t}^7\}$, all with stabiliser $\langle t \rangle$. Therefore if $t \neq t'$ then there cannot be a G-equivariant isomorphism between $C_{s,t}$ and $C_{s',t'}$ for any choices of s, s'. For fixed t and s, s' satisfying $s \neq t$ and $s' \neq t$ let $\eta_{s,t}$ and $\eta_{s',t}$ be generators of $C_{s,t}$ and $C_{s',t}$ respectively; then the map $f : C_{s,t} \to C_{s',t}$ defined by

$$f : \eta_{s,t} \mapsto \eta_{s',t}.$$

is a G-equivariant isomorphism. □

The result for the Hopf-Galois structures of type Q_8 is an instance of a well known result (see [KKTU19b, Example 2.4], for example).

Lemma 3.2.4. *The Hopf algebras $L[\lambda(G)]^G$ and $L[\rho(G)]^G$ are not isomorphic as Hopf algebras.*

Proof. The G-action on $\rho(G)$ is trivial since $\lambda(G)$ and $\rho(G)$ commute. However, the G-action on $\lambda(G)$ is conjugation so that the G-orbits are the conjugacy classes. Therefore no G-equivariant isomorphism can exist. □

Finally, we can give the result for the Hopf-Galois structures of type D_4.

Lemma 3.2.5. *The Hopf algebras $L[D_{s,\lambda}]^G$ and $L[D_{s,\rho}]^G$ are all pairwise nonisomorphic as Hopf algebras.*

Proof. Recall the definitions of $D_{s,\lambda}$ and $D_{s,\rho}$ from Lemma 3.1.5. The nontrivial G-orbits of $D_{s,\lambda}$ are

$$\{\lambda(s), \lambda(s^{-1})\}, \{\lambda(t)\rho(s), \lambda(t^{-1})\rho(s)\}, \text{ and } \{\lambda(st)\rho(s), \lambda((st)^{-1})\rho(s)\},$$

with stabilisers $\langle s \rangle$, $\langle t \rangle$, and $\langle st \rangle$ respectively. If $s \neq s'$ and $f : D_{s,\lambda} \to D_{s',\lambda}$ is a G-equivariant bijection then by considering stabilisers we see that

$f(\lambda(s)) = \lambda(t')\rho(s')$ for some t'. But $\lambda(s)$ has order 4, whereas $\lambda(t')\rho(s')$ has order 2. Therefore f cannot be an isomorphism.

The non-trivial G-orbits of $D_{s,\rho}$ are

$$\{\lambda(s)\rho(t), \lambda(s^{-1})\rho(t)\} \text{ and } \{\lambda(s)\rho(st), \lambda(s^{-1})\rho(st)\}$$

both with stabiliser $\langle s \rangle$. Therefore if $s \neq s'$ then there cannot be a G-equivariant isomorphism between $D_{s,\rho}$ and $D_{s',\rho}$.

Finally, there cannot be a G-equivariant isomorphism between $D_{s,\lambda}$ and $D_{s',\rho}$ for any s, s', since these groups have different numbers of G-orbits. □

3.3 F-algebra isomorphisms

In this section we investigate the F-algebra structure of the Hopf algebras giving Hopf-Galois structures on L/F. We now impose the assumption that the characteristic of F is not 2; thus ensuring the Hopf algebras are separable by Lemma 2.2.26, hence semisimple, so that each has an Artin-Wedderburn decomposition by Theorem 2.2.25.

Recall that, since L/F is a quaternionic extension it has a unique bi-quadratic subextension K/F corresponding to the unique order 2 subgroup $\langle \sigma^2 \rangle$ of G, so that $\mathrm{Gal}(K/F) = G/\langle \sigma^2 \rangle$. Let $s, t \in \{\sigma, \tau, \sigma\tau\}$ with $s \neq t$, and let ω, ν be elements of K such that $\omega^2, \nu^2 \in F$, $s(\omega) = \omega, t(\omega) = -\omega$, $s(\nu) = -\nu$ and $t(\nu) = \nu$; note that $K = F(\omega, \nu)$.

Recall Lemma 2.2.32, a result of Bley and Boltje, that shows how one may construct an F-basis of H corresponding to the Artin-Wedderburn decomposition. Recall further, from Remark 2.2.33, that when the values of the characters of N do not necessarily lie in L we may extend to the algebraic closure of F and act through $\mathrm{Gal}(F^{\mathrm{alg}}/F)$ in order to find G-invariant linear combinations of mutually orthogonal idempotents of $F^{\mathrm{alg}}[N]$ that form an F-basis of $L[N]^G$.

If H is a Hopf algebra whose underlying subgroup N is isomorphic to $C_2 \times C_2 \times C_2$ then the values of the characters of N lie in F, so in this case no such extension is required. Using this observation we have:

Lemma 3.3.1. *Let $E_{s,t}$ be defined as in Lemma 3.1.1. Then we have*

$$L[E_{s,t}]^G \cong F^4 \times K \text{ as } F\text{-algebras.}$$

Proof. The dual group $\widehat{E}_{s,t}$ is generated by three characters:

$$\chi_1 : \begin{cases} \lambda(s)\rho(t) & \mapsto & -1 \\ \lambda(s^2) & \mapsto & 1 \\ \lambda(t)\rho(st) & \mapsto & 1 \end{cases}$$

$$\chi_2 : \begin{cases} \lambda(s)\rho(t) & \mapsto & 1 \\ \lambda(s^2) & \mapsto & -1 \\ \lambda(t)\rho(st) & \mapsto & 1 \end{cases},$$

$$\chi_3 : \begin{cases} \lambda(s)\rho(t) & \mapsto & 1 \\ \lambda(s^2) & \mapsto & 1 \\ \lambda(t)\rho(st) & \mapsto & -1 \end{cases}.$$

Let χ_0 denote the identity in $\widehat{E}_{s,t}$, and recall the G-orbit structure of $E_{s,t}$ in Lemma 3.2.1. It is easily verified that ${}^s\chi_2 = \chi_2\chi_3$, ${}^t\chi_2 = \chi_1\chi_2$ and ${}^{st}\chi_2 = \chi_1\chi_2\chi_3$ and that s and t act trivially on χ_0, χ_1, χ_3 and $\chi_1\chi_3$. Hence the orbits of G in $\widehat{E}_{s,t}$ are

$$\{\chi_0\}, \quad \{\chi_1\}, \quad \{\chi_3\}, \quad \{\chi_1\chi_3\}, \text{ and } \{\chi_2, \chi_1\chi_2, \chi_2\chi_3, \chi_1\chi_2\chi_3\}.$$

The orbit representatives $\chi_0,\ \chi_1,\ \chi_3,\ \chi_1\chi_3$ all have stabilizer G, and the orbit representative χ_2 has stabiliser $\langle\sigma^2\rangle$. Therefore we have $L[E_{s,t}]^G \cong F^4 \times K$, as claimed. □

For the remaining structures whose underlying subgroup N is abelian there may exist characters of N whose values do not lie in the field F. In these cases the action of $\Omega = \mathrm{Gal}(F^{\mathrm{alg}}/F)$ on $\widehat{N}$ depends upon the intersection of L with certain cyclotomic extensions of F, and can be difficult to follow in detail. To overcome this problem we study the action of Ω on the group algebra $F^{\mathrm{alg}}[N]$, as in Remark 2.2.33. As discussed above, we have $L[N]^G = F^{\mathrm{alg}}[N]^\Omega$, and the action of Ω factors through $\mathrm{Gal}(L'/F)$ for some cyclotomic extension L' of L. Thus, writing $G' = \mathrm{Gal}(L'/L)$, we have

$$L[N]^G = \left(L'[N]^{G'}\right)^G,$$

where the action of G' on $L'[N]$ is only on the coefficients. In the following lemma we follow this process by choosing a subfield E of F^{alg} that contains L and the values of the characters of N, and consider the action of $G' = \mathrm{Gal}(E/L)$ in place of Ω. This allows us to find an L-basis of $L[N]$ by acting on idempotents of $E[N]$ by G', before considering the action of G. By forming G-invariant linear combinations of these basis elements we obtain a basis of $L[N]^G$ corresponding to its Artin-Wedderburn decomposition. Although working with bases in this way is rather cumbersome, it has the advantage of applying uniformly, whereas studying the orbits of Ω in $\widehat{N}$ can split into many cases, depending upon the roots of unity contained in L.

We continue with the Hopf algebras giving the structures of type $C_4 \times C_2$ where here we find an explicit basis. We will find a certain idempotent plays an important role in all of the coming bases so we introduce the notation:

$$f_0 = \frac{1}{2}\big(1 - \lambda(\sigma^2)\big)$$

where σ is chosen arbitrarily from the subset $\{\sigma, \tau, \sigma\tau\}$ of elements of G since $\sigma^2 = \tau^2 = (\sigma\tau)^2$.

Lemma 3.3.2. *Let $A_{s,t}$ be defined as in Lemma 3.1.2. Then we have*

$$L[A_{s,t}]^G \cong F^4 \times F(\omega, \iota)^d \text{ as } F\text{-algebras,}$$

where $\iota \in F^{alg}$ is such that $\iota^2 = -1$ and $d = 2/[F(\omega, \iota) : F(\omega)]$.

Proof. We may write $A_{s,t} = \langle \lambda(s), \lambda(s)\rho(t) \rangle$. Following the discussion above we define a subgroup of F^{alg} by $E = L(i)$ and let $G' = \text{Gal}(E/L) = \langle g \rangle$ where $g : i \mapsto -i$. Then $E[N] \cong E^8$ and $L[N] = E[N]^{G'}$ as G' has no effect on N when it acts. Let $\text{Gal}(E/F) = G''$. Then

$$E[N]^{G''} = L[N]^G.$$

Thus a basis of $E[N]$ can be found by considering the idempotents formed using each generator of $A_{s,t}$. That is the idempotents $\{E_i e_j\}_{i \in \{0,1\}, j \in \{0,1,2,3\}}$ where

$$e_0 = \frac{1 + \lambda(s) + \lambda(s^2) + \lambda(s^3)}{4},$$
$$e_1 = \frac{1 + i\lambda(s) - \lambda(s^2) - i\lambda(s^3)}{4},$$
$$e_2 = \frac{1 - \lambda(s) + \lambda(s^2) - \lambda(s^3)}{4},$$
$$e_3 = \frac{1 - i\lambda(s) - \lambda(s^2) + i\lambda(s^3)}{4},$$
$$E_0 = \frac{1 + \lambda(s)\rho(t)}{2},$$

and

$$E_1 = \frac{1 - \lambda(s)\rho(t)}{2}.$$

We next descend to L by considering the action of G' and constructing elements that remained fixed under this action. We clearly need only consider the action of $g \in G'$ and it is easy to see that e_0, e_2, E_0 and E_1 are fixed and that ${}^g e_1 = e_3$ and vice versa. Therefore g fixes

$$e_1 + e_3 = \frac{1 - \lambda(s^2)}{2} := f_0$$

and

$$i(e_1 - e_3) = -f_0\lambda(s).$$

So our current candidate basis elements are

$$e_0E_0,\ e_2E_0,\ e_0E_1,\ e_2E_1,\ f_0E_0,\ -f_0\lambda(s)E_0,\ f_0E_1,\ -f_0\lambda(s)E_1.$$

These are the following elements:

$$b_0 = \frac{1}{8}\big(1 + \lambda(s) + \lambda(s^2) + \lambda(s^{-1}) + \rho(t)^{-1} + \lambda(s)^{-1}\rho(t) + \rho(t) + \lambda(s)\rho(t)\big),$$

$$b_1 = \frac{1}{8}\big(1 - \lambda(s) + \lambda(s^2) - \lambda(s^{-1}) - \rho(t)^{-1} + \lambda(s)^{-1}\rho(t) - \rho(t) + \lambda(s)\rho(t)\big),$$

$$b_2 = \frac{1}{8}\big(1 + \lambda(s) + \lambda(s^2) + \lambda(s^{-1}) - \rho(t)^{-1} - \lambda(s)^{-1}\rho(t) - \rho(t) - \lambda(s)\rho(t)\big),$$

$$b_3 = \frac{1}{8}\big(1 - \lambda(s) + \lambda(s^2) - \lambda(s^{-1}) + \rho(t)^{-1} - \lambda(s)^{-1}\rho(t) + \rho(t) - \lambda(s)\rho(t)\big),$$

$$b_4 = \frac{1}{4}\big(1 - \lambda(s^2) + \lambda(s)^{-1}\rho(t) - \lambda(s)\rho(t)\big),$$

$$b_5 = \frac{1}{4}\big(1 - \lambda(s^2) - \lambda(s)^{-1}\rho(t) + \lambda(s)\rho(t)\big),$$

$$b_6 = \frac{1}{4}\big(-\lambda(s) + \lambda(s^{-1}) + \rho(t)^{-1} - \rho(t)\big),$$

$$b_7 = \frac{1}{4}\big(-\lambda(s) + \lambda(s^{-1}) - \rho(t)^{-1} + \rho(t)\big),$$

which are an L-basis of $L[A_{s,t}]$. Recall from Lemma 3.2.2 that the non-trivial G-orbits of $A_{s,t}$, are $\{\lambda(s), \lambda(s^{-1})\}$, $\{\lambda(s)\rho(t), \lambda(s^{-1})\rho(t)\}$, both with stabiliser $\langle s\rangle$. From this we see that b_0, b_1, b_2 and b_3 are fixed by G, that ${}^tb_4 = b_5$, and that ${}^tb_6 = b_7$. Therefore the following linear combinations of the above elements are all fixed by G, and in fact form a basis of $L[A_{s,t}]^G$ over F:

$$a_0 = b_0,$$

$$a_1 = b_1,$$

$$a_2 = b_2,$$

$$a_3 = b_3,$$
$$a_{4,0} = b_4 + b_5 = \frac{1}{2}\big(1 - \lambda(s^2)\big) = f_0,$$
$$a_{4,1} = \omega(b_4 - b_5) = -\omega f_0 \lambda(s)\rho(t),$$
$$a_{4,2} = -b_6 + b_7 = f_0\rho(t),$$
$$a_{4,3} = -\omega(b_6 + b_7) = \omega f_0 \lambda(s).$$

We have $a_i a_j = \delta_{i,j} a_i$ for $i, j = 0, 1, 2, 3$ and $a_i a_{4,k} = 0$ for all $i = 0, 1, 2, 3$ and $k = 0, 1, 2, 3$. Finally, we consider the multiplication table of the $a_{4,k}$.

	$a_{4,0}$	$a_{4,1}$	$a_{4,2}$	$a_{4,3}$
$a_{4,0}$	$a_{4,0}$	$a_{4,1}$	$a_{4,2}$	$a_{4,3}$
$a_{4,1}$	$a_{4,1}$	$\omega^2 a_{4,0}$	$a_{4,3}$	$\omega^2 a_{4,2}$
$a_{4,2}$	$a_{4,2}$	$a_{4,3}$	$-a_{4,0}$	$-a_{4,1}$
$a_{4,3}$	$a_{4,3}$	$\omega^2 a_{4,2}$	$-a_{4,1}$	$-\omega^2 a_{4,0}$

From the table it is clear that we have the claimed decomposition. □

We use a similar process for the Hopf algebras giving the Hopf-Galois structures of type C_8, but we suppress the details of the descent and instead give candidate L-basis elements of $L[N]$.

Lemma 3.3.3. *Let $C_{s,t}$ be defined as in Lemma 3.1.3. Then we have*

$$L[C_{s,t}]^G \cong F^2 \times F(\nu\iota)^{d_1} \times F(r\iota, \nu\iota)^{d_1 d_2} \text{ as } F\text{-algebras,}$$

where $r, \iota \in F^{alg}$ such that $r^2 = 2$, $\iota^2 = -1$ and where $d_1 = 2/[F(\nu\iota) : F]$ and $d_2 = 2/[F(r\iota, \nu\iota) : F(\nu\iota)]$.

Proof. Let $\eta = \eta_{s,t}$ as defined in Lemma 3.1.3, so that $C_{s,t} = \langle\eta\rangle$, and let

$$b_0 = \frac{1}{8}\big(1 + \eta + \eta^2 + \eta^3 + \eta^4 + \eta^5 + \eta^6 + \eta^7\big),$$

$$b_1 = \frac{1}{8}\big(1 - \eta + \eta^2 - \eta^3 + \eta^4 - \eta^5 + \eta^6 - \eta^7\big),$$

$$b_2 = \frac{1}{4}\big(1 - \eta^2 + \eta^4 - \eta^6\big),$$

$$b_3 = \frac{1}{4}\big(\eta - \eta^3 + \eta^5 - \eta^7\big),$$

$$b_4 = \frac{1}{2}\big(1 - \eta^4\big),$$

$$b_5 = \frac{1}{2}\big(\eta^3 - \eta^7\big),$$

$$b_6 = \frac{1}{2}\big(\eta^2 - \eta^6\big),$$

$$b_7 = \frac{1}{2}\big(\eta - \eta^5\big).$$

It is easily verified that these 8 elements of $L[C_{s,t}]$ are linearly independent over L and so form an L-basis of $L[C_{s,t}]$. Recall from Lemma 3.2.3 that the nontrivial G-orbits of $C_{s,t}$ are $\{\eta, \eta^3\}$, $\{\eta^2, \eta^6\}$ and $\{\eta^5, \eta^7\}$, all with stabiliser $\langle t \rangle$. From this we see that b_0, b_1, b_2 and b_4 are fixed by G, that ${}^s b_3 = -b_3$, ${}^s b_6 = -b_6$, and that ${}^s b_5 = b_7$. Therefore the following linear combinations of the above elements are all fixed by G, and in fact form a basis of $L[C_{s,t}]$ over L:

$$a_0 = b_0,$$

$$a_1 = b_1,$$

$$a_{2,0} = b_2,$$

$$a_{2,1} = \nu b_3 = \nu b_2 \eta,$$

$$a_{3,0} = b_4 = f_0,$$

$$a_{3,1} = \nu b_6 = \nu f_0 \eta^2,$$

$$a_{3,2} = (b_5 + b_7) = f_0(\eta^3 + \eta),$$

$$a_{3,3} = \nu(b_5 - b_7) = \nu f_0(\eta^3 - \eta).$$

We have $a_i a_j = \delta_{i,j} a_i$ for $i, j = 0, 1$, $a_i a_{2,k} = 0$ for all $i = 0, 1, 3$ and $k = 0, 1$, and $a_i a_{3,k} = 0$ for all $i = 0, 1, 2$ and $k = 0, 1, 2, 3$. Finally, we consider the multiplication tables of of the $a_{2,k}$ and the $a_{3,k}$:

	$a_{2,0}$	$a_{2,1}$
$a_{2,0}$	$a_{2,0}$	$a_{2,1}$
$a_{2,1}$	$a_{2,1}$	$-\nu^2 a_{2,0}$

	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$
$a_{3,0}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$
$a_{3,1}$	$a_{3,1}$	$-\nu^2 a_{3,0}$	$a_{3,3}$	$-\nu^2 a_{3,2}$
$a_{3,2}$	$a_{3,2}$	$a_{3,3}$	$-2a_{3,0}$	$-2a_{3,1}$
$a_{3,3}$	$a_{3,3}$	$-\nu^2 a_{3,2}$	$-2a_{3,1}$	$2\nu^2 a_{3,0}$

From these tables it is clear that we have the claimed decomposition. □

The remaining structures are of nonabelian type, and so we cannot employ the methods of [BB99, Lemma 2.2]. We emulate the same process using the character table in place of the dual group of our underlying subgroup. We write down a convenient L-basis of $L[N]$ and form G-invariant linear combinations of these basis elements. We find that certain quaternion algebras appear in the decompositions, and so we recall our notation for these from Definition 2.2.36: let $(U, V)_F$ denote the quaternion algebra with F-basis $1, u, v, w$ satisfying the relations $u^2 = U \in F^\times$, $v^2 = V \in F^\times$, and $uv = w = -vu$.

We begin with the Hopf Algebras giving the classical and canonical nonclassical structures of type Q_8.

Lemma 3.3.4. *We have*

$$L[\rho(G)]^G \cong K[G] \cong F^4 \times (-1,-1)_F \text{ as } F\text{-algebras}$$

and

$$L[\lambda(G)]^G \cong F^4 \times (-\omega^2,-\nu^2)_F \text{ as } F\text{-algebras.}$$

Proof. Let $\mu \in \{\rho, \lambda\}$. The character table for $\mu(G)$ is

	1	$\{\mu(\sigma^2)\}$	$\{\mu(s), \mu(s^{-1})\}$	$\{\mu(t), \mu(t^{-1})\}$	$\{\mu(st), \mu((st)^{-1})\}$
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	-1	1	-1
χ_3	1	1	-1	-1	1
ψ	2	-2	0	0	0

First we consider the case $\mu = \rho$, corresponding to the classical Hopf-Galois structure on L/F. For $k = 0, 1, 2, 3$, let e_k be the orthogonal idempotent corresponding to the character χ_k. The idempotent corresponding to the 2-dimensional representation is

$$e_\psi = \frac{1}{2}\Big(1 - \rho(\sigma^2)\Big) = f_0.$$

The following is a set of 8 linearly independent elements of $L[\rho(G)]$, and each element is fixed by G since the action of G on $\rho(G)$ is trivial. It is therefore a basis of $L[\rho(G)]^G = F[\rho(G)]$ over F:

$$\{e_0, e_1, e_2, e_3, f_0, f_0\rho(s), f_0\rho(t), f_0\rho(st)\}.$$

The e_k are orthogonal idempotents, and each is also orthogonal to every element of the set $\{f_0, f_0\rho(s), f_0\rho(t), f_0\rho(st)\}$. This set spans a 4-dimensional

F-algebra, which is isomorphic to the quaternion algebra $(-1,-1)_F$ via the F-algebra isomorphism defined by $f_0\rho(s) \mapsto u$, $f_0\rho(t) \mapsto v$. Therefore we have the claimed decomposition.

Now we consider the case $\mu = \lambda$, corresponding to the canonical non-classical Hopf-Galois structure on L/F. As discussed in Lemma 3.2.4 the G-orbits of $\lambda(G)$ are the conjugacy classes. As above, for $k = 0, 1, 2, 3$ let e_k be the orthogonal idempotent corresponding to the character χ_k, and note that these are fixed by G. The idempotent f_0, corresponding to the 2-dimensional representation of $\lambda(G)$, is also fixed by G. Now consider the L-linearly independent set $\{f_0, f_0\lambda(s), f_0\lambda(t), f_0\lambda(st)\}$. An element of the sub-algebra generated by this set is of the form

$$x = a_0 f_0 + a_1 f_0\lambda(s) + a_2 f_0\lambda(t) + a_3 f_0\lambda(st) \text{ with } a_k \in L \text{ for } k = 0, 1, 2, 3.$$

The element x is fixed by G if and only if $a_1 = a_1'\omega$, $a_2 = a_2'\nu$ and $a_3 = a_3'\omega\nu$ for some $a_0, a_1', a_2', a_3' \in F$. Thus the following set is an F-basis of $L[\lambda(G)]^G$:

$$\{e_0, e_1, e_2, e_3, f_0, \omega f_0\lambda(s), \nu f_0\lambda(t), \omega\nu f_0\lambda(st)\}.$$

As above, the e_k are orthogonal to each other and to every element of the set $\{f_0, \omega f_0\lambda(s), \nu f_0\lambda(t), \omega\nu f_0\lambda(st)\}$. This set spans a 4-dimensional F-algebra, which is isomorphic to the quaternion algebra $(-\omega^2, -\nu^2)_F$ via the F-algebra isomorphism from $(U, V)_F$ defined by $u \mapsto \omega f_0\lambda(s), v \mapsto \nu f_0\lambda(t)$. Therefore we have the claimed decomposition. □

It may appear that the Hopf algebras giving the classical and canonical non-classical structures are not isomorphic as F-algebras. However, we recall Theorem 2.1.22 which gives us the following:

Lemma 3.3.5. *We have $(-\omega^2, -\nu^2)_F \cong (-1,-1)_F$ as F-algebras.*

Proof. By Witt's result (Theorem 2.1.22), the fact that $K = F(\omega, \nu)$ embeds into a quaternionic extension of F implies that the quadratic form $\omega^2 x_1^2 +$

$\nu^2x_2^2 + \omega^2\nu^2x_3^2$ is equivalent to the quadratic form $x_1^2 + x_2^2 + x_3^2$. These are the norm forms of the subspaces of pure quaternions of $(-\omega^2, -\nu^2)_F$ and $(-1,-1)_F$, respectively. Therefore the norms are equivalent as quadratic forms, and so, by Theorem 2.2.44, $(-\omega^2, -\nu^2)_F \cong (-1,-1)_F$ as F-algebras. □

Corollary 3.3.6. *We have $L[\rho(G)]^G \cong L[\lambda(G)]^G \cong F^4 \times (-1,-1)_F$ as F-algebras.*

In fact, this result follows from an unpublished theorem of Greither which states that if L/F is *any* Galois extension of fields then $F[G] \cong L[\lambda(G)]^G$ as F-algebras. See [KKTU19a, Theorem 5.2] for more details.

Finally, we have the Hopf Algebras giving the structures of type D_4.

Lemma 3.3.7. *Let $D_{s,\lambda}$ and $D_{s,\rho}$ be defined as in Lemma 3.1.5. Then we have*

$$L[D_{s,\lambda}]^G \cong F^4 \times (-\omega^2, \nu^2)_F \text{ as } F\text{-algebras}$$

and

$$L[D_{s,\rho}]^G \cong F^4 \times (-1, \omega^2)_F \text{ as } F\text{-algebras.}$$

Proof. For ease, let $X = \{1, \lambda(s^2)\}$ so the character table for $D_{s,\lambda}$ is the following:

	1	$\{\lambda(s^2)\}$	$\lambda(s)X$	$\lambda(t)\rho(s)X$	$\lambda(st)\rho(s)X$
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	-1	1	-1
χ_3	1	1	-1	-1	1
ψ	2	-2	0	0	0.

As in the proof of Lemma 3.3.4, for $k = 0, 1, 2, 3$ let e_k be the orthogonal idempotent corresponding to the character χ_k, and note that the idempotent corresponding to the 2-dimensional representation is f_0. Recall from Lemma 3.2.5 that the non-trivial G-orbits of $D_{s,\lambda}$ are

$$\{\lambda(s), \lambda(s^{-1})\}, \{\lambda(t)\rho(s), \lambda(t^{-1})\rho(s)\}, \text{ and } \{\lambda(st)\rho(s), \lambda((st)^{-1})\rho(s)\},$$

with stabilisers $\langle s \rangle$, $\langle t \rangle$, and $\langle st \rangle$ respectively. Hence each e_k is fixed by G. Now consider the L-linearly independent set

$$\{f_0, f_0\lambda(s), f_0\lambda(t)\rho(s), f_0\lambda(st)\rho(s)\}.$$

An element of the sub-algebra generated by these elements is of the form

$$x = a_0 e + a_1 e\lambda(s) + a_2 e\lambda(t)\rho(s) + a_3 e\lambda(st)\rho(s) \text{ with } a_k \in L \text{ for } k = 0, 1, 2, 3.$$

The element x is fixed by G if and only if $a_1 = a_1'\omega$, $a_2 = a_2'\nu$ and $a_3 = a_3'\omega\nu$ for some $a_0, a_1', a_2', a_3' \in F$. Let $f_\omega = \omega f_0\lambda(s)$, $f_\nu = \nu f_0\lambda(t)\rho(s)$ and $f_{\omega\nu} = \omega\nu f_0\lambda(st)\rho(s)$, and consider the set

$$\{e_0, e_1, e_2, e_3, f_0, f_\omega, f_\nu, f_{\omega\nu}\}.$$

This set is L-linearly independent and each element is fixed by G. It is therefore an F-basis of $L[D_{s,\lambda}]^G$. The e_k are orthogonal to each other and to every element of the set $\{f_0, f_\omega, f_\nu, f_{\omega\nu}\}$. This set spans a 4-dimensional F-algebra with the following multiplication table:

	f_0	f_ω	f_ν	$f_{\omega\nu}$
f_0	f_0	f_ω	f_ν	$f_{\omega\nu}$
f_ω	f_ω	$-\omega^2 f_0$	$f_{\omega\nu}$	$-\omega^2 f_\nu$
f_ν	f_ν	$-f_{\omega\nu}$	$\nu^2 f_0$	$-\nu^2 f_\omega$
$f_{\omega\nu}$	$f_{\omega\nu}$	$\omega^2 f_\nu$	$\nu^2 f_\omega$	$(\omega\nu)^2 f_0$

From this table we see that $L[D_{s,\lambda}]^G \cong F^4 \times (-\omega^2, \nu^2)_F$ as F-algebras.

We determine the structure of $L[D_{s,\rho}]^G$ by essentially the same method, and so we omit some of the details. In notation analogous to that employed above, we find that the set

$$\{e_0, e_1, e_2, e_3, f_0, f_1, f_2, f_3\},$$

where f_0, $f_1 = f_0\rho(s)$, $f_2 = \omega f_0\lambda(s)\rho(t)$ and $f_3 = \omega f_0\lambda(s)\rho(st)$, is an F-basis of $L[D_{s,\lambda}]^G$. The final four elements span a 4-dimensional F-algebra with the following multiplication table:

	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	$-f_0$	f_3	$-f_2$
f_2	f_2	$-f_3$	$\omega^2 f_0$	$-\omega^2 f_1$
f_3	f_3	f_2	$\omega^2 f_1$	$\omega^2 f_0$

From this table we see that $L[D_{s,\rho}]^G \cong F^4 \times (-1, \omega)_F$ as F-algebras. □

As in the case of the Hopf algebras giving the Hopf-Galois structures of Q_8 type, some of the quaternion algebras appearing in the decompositions above are isomorphic:

Lemma 3.3.8. *We have $(-\omega^2, \nu^2)_F \cong (-1, \omega^2)_F$ as F-algebras.*

Proof. Write $[-\omega^2, \nu^2], [-1, \omega^2]$ for the classes of $(-\omega^2, \nu^2)_F, (-1, \omega^2)_F$ in the Brauer group $\mathrm{Br}(F)$. It is sufficient to show that $[-\omega^2, \nu^2] = [-1, \omega^2]$. We refer to Theorem 2.2.47 for the multiplicative property, and to Proposition 2.2.38 for further properties, of the classes of quaternion algebras in $\mathrm{Br}(F)$. Using the result of Lemma 3.3.5 we have $[-\omega^2, -\nu^2] = [-1, -1]$, and

so in $\mathrm{Br}(F)$ we have

$$\begin{aligned}
[-\omega^2,\nu^2][-\omega^2,-\nu^2] &= [-\omega^2,-\nu^4] \\
&= [-\omega^2,-1] \\
&= [-1,-\omega^2] \\
&= [-1,\omega^2][-1,-1] \\
&= [-1,\omega^2][-\omega^2,-\nu^2].
\end{aligned}$$

Cancelling $[-\omega^2,-\nu^2]$, we obtain $[-\omega^2,\nu^2]=[-1,\omega^2]$, as claimed. Therefore $(-\omega^2,\nu^2)_F \cong (-1,\omega^2)_F$ as F-algebras. □

Corollary 3.3.9. *We have*

$$L[D_{s,\rho}]^G \cong L[D_{s,\lambda}]^G \cong F^4 \times (-1,\omega^2)_F \text{ as } F\text{-algebras.}$$

In order to better understand the F-algebra structure of the Hopf algebras $L[D_{s,\rho}]^G$, we investigate the relationships between $(-1,\omega^2)_F, (-1,\nu^2)_F$ and $(-1,\omega^2\nu^2)_F$.

Lemma 3.3.10. *Let $x,y \in \{\omega^2,\nu^2,\omega^2\nu^2\}$ with $x \neq y$. Then we have $(-1,x)_F \cong (-1,xy)_F$ as F-algebras if and only if $(-1,y)_F \cong M_2(F)$ as F-algebras.*

Proof. In $\mathrm{Br}(F)$ we have $[-1,xy]=[-1,x][-1,y]$, so $[-1,x]=[-1,xy]$ if and only if $[-1,y]=[-1,1]$. That is, $(-1,x)_F \cong (-1,xy)_F$ as F-algebras if and only if $(-1,y)_F \cong (-1,1)_F \cong M_2(F)$ as F-algebras. □

Lemma 3.3.10 suggests three scenarios for the quaternion algebras $(-1,\omega^2)_F$, $(-1,\nu^2)_F$ and $(-1,\omega^2\nu^2)_F$; all three are isomorphic to matrix rings; exactly one is isomorphic to a matrix ring and the other two are isomorphic to the same division algebra; or each is isomorphic to a distinct division algebra. The following examples illustrate that each of these three cases does occur.

Example 3.3.11. *Suppose that -1 is a square in F. Then for $x \in \{\omega^2, \nu^2, \omega^2\nu^2\}$ we have that -1 occurs as the norm of an element of the field $F(x)$, and so $(-1,x)_F \cong (-1,1)_F \cong M_2(F)$ [JY88, Proposition I.1.6]. Therefore in this case we have*

$$L[D_{s,\rho}]^G \cong L[D_{t,\rho}]^G \cong L[D_{st,\rho}]^G \cong F^4 \times M_2(F)$$

as F-algebras.

Example 3.3.12. *Let $F = \mathbb{Q}$, $\omega = \sqrt{11}$, $\nu = \sqrt{2}$. Then, by [Fuj90a], $K = \mathbb{Q}(\omega, \nu)$ can be embedded in a quaternionic extension L of $\mathbb{Q}$. In this case we have $(-1,\nu^2)_{\mathbb{Q}} \cong (-1,1)_{\mathbb{Q}} \cong M_2(\mathbb{Q})$ a $\mathbb{Q}$-algebras since 2 is the norm of the element $1+i \in \mathbb{Q}(i)$, and so by Lemma 3.3.10 we have $(-1,\omega^2)_{\mathbb{Q}} \cong (-1,\omega^2\nu^2)_{\mathbb{Q}}$ as $\mathbb{Q}$-algebras. However, $(-1,\omega^2)_{\mathbb{Q}} \ncong M_2(\mathbb{Q})$, since no element of $\mathbb{Q}(i)$ has norm 11. Therefore in this case we have $L[D_{t,\rho}]^G \cong \mathbb{Q}^4 \times M_2(\mathbb{Q})$ and*

$$L[D_{s,\rho}]^G \cong L[D_{st,\rho}]^G \cong F^4 \times (-1,\omega^2) \ncong F^4 \times M_2(\mathbb{Q})$$

as $\mathbb{Q}$-algebras.

Example 3.3.13. *Let $F = \mathbb{Q}$, $\omega = \sqrt{11}$, $\nu = \sqrt{6}$. Then, by [Vau92, Example 4.4], $K = \mathbb{Q}(\omega, \nu)$ can be embedded in a quaternionic extension L of $\mathbb{Q}$. In this case none of $(-1,\omega^2)_{\mathbb{Q}}, (-1,\nu^2)_{\mathbb{Q}}, (-1,\omega^2\nu^2)_{\mathbb{Q}}$ is isomorphic to $M_2(\mathbb{Q})$ as a $\mathbb{Q}$-algebra, since none of $6, 11, 66$ occurs as the norm of an element of $\mathbb{Q}(i)$. Therefore by Lemma 3.3.10 these quaternion algebras are all nonisomorphic as $\mathbb{Q}$-algebras, and so we have*

$$L[D_{s,\rho}]^G \ncong L[D_{t,\rho}]^G \ncong L[D_{st,\rho}]^G$$

as $\mathbb{Q}$-algebras.

3.4 Opposite Hopf-Galois structures

The final section of this chapter highlights the relationship between some of these Hopf algebras. Recall Definition 2.2.17 that defines the opposite

Hopf-Galois structure to that with Hopf algebra $H = L[N]^G$, is that with Hopf algebra $H' = L[N']^G$ where N' is the centraliser of N in $\mathrm{Perm}(G)$. Further note from Definition 2.2.17 that the structures of abelian type are opposite only to themselves. Finally, recall Example 2.2.18, that states that the classical and canonical nonclassical structures are opposite to each other. This raises the question of which of the dihedral structures are opposite to each other.

Proposition 3.4.1. *Recall the definitions of $D_{s,\lambda}$ and $D_{s,\rho}$ from Lemma 3.1.5. For each choice of $s \in \{\sigma, \tau, \sigma\tau\}$ we have $L[D_{s,\lambda}]^G = (L[D_{s,\rho}]^G)'$.*

Proof. It is sufficient to show that each generator of $D_{s,\lambda}$ commutes with each generator of $D_{s,\rho}$ since this implies $D_{s,\rho} \subseteq D'_{s,\lambda}$ and since $|D'_{s,\lambda}| = |D_{s,\lambda}|$ this means $D_{s,\rho} = \mathrm{Cent}_{\mathrm{Perm}(G)}(D_{s,\lambda})$ as required. We make finitely many calculations:

$$\rho(s)\lambda(s) = \lambda(s)\rho(s),$$

$$\rho(s)\big(\lambda(t)\rho(s)\big) = \lambda(t)\rho(s)^2 = \big(\lambda(t)\rho(s)\big)\rho(s),$$

$$\big(\lambda(s)\rho(t)\big)\lambda(s) = \lambda(s)^2\rho(t) = \lambda(s)\big(\lambda(s)\rho(t)\big),$$

and finally, noting that $\rho(s^2) \in Z(\mathrm{Perm}(G))$,

$$\begin{aligned}
\big(\lambda(s)\rho(t)\big)\big(\lambda(t)\rho(s)\big) &= \lambda(s)\lambda(t)\rho(t)\rho(s) \\
&= \lambda(st)\rho(ts) \\
&= \lambda(ts)\lambda(s^2)\rho(st)\rho(s^2) \\
&= \lambda(t)\lambda(s)\lambda(s^2)\rho(s^2)\rho(s)\rho(t), \\
&= \big(\lambda(t)\rho(s)\big)\big(\lambda(s)\rho(t)\big).
\end{aligned}$$

□

Chapter 4

Some general results

In this chapter we turn to questions of integral module structure in Hopf-Galois extensions. In the first section, we prove a general "descent" lemma relating the integral Hopf-Galois module structure of a Galois extension to that of a subextension (Lemma 4.1.2). In the second section we apply this result to Hopf-Galois structures of cyclic type on a tame quaternionic extension of $\mathbb{Q}$.

4.1 Quotient structures

Let L/F be a Galois extension of number fields or p-adic fields. Let $H = L[N]^G$ be a Hopf algebra giving a Hopf-Galois structure on the extension, and let P be a G-stable normal subgroup of N. Recall Theorem 2.2.35 that states that the Hopf algebra $L[N/P]^G$ gives a Hopf-Galois structure on L^P/F and recall from Equation (2.3) that the action of the Hopf algebra on the extension is given by

$$\left(\sum_{\bar{\eta}\in N/P} c_{\bar{\eta}}\bar{\eta}\right)\cdot x = \sum_{\bar{\eta}\in N/P} c_{\bar{\eta}}\eta^{-1}(1_G)[x]$$

for all $x \in L^P$ and $\bar{\eta} = \eta P$.

There is a natural homomorphism $\nu : N \to N/P$ which clearly extends to an L-algebra homomorphism $\nu : L[N] \to L[N/P]$. We first aim to understand the interaction of ν with the G-actions in order to restrict ν to H.

Lemma 4.1.1. *We have $\nu({}^g z) = {}^g\nu(z)$ for all $z \in L[N]$, and so ν restricts to a K-algebra homomorphism $\nu : L[N]^G \to L[N/P]^G$.*

Proof. First, it is sufficient to consider the case where $z = c\eta$ with $c \in L$ and $\eta \in N$. In this case, for each $g \in G$ we have

$$\nu({}^g c\eta) = \nu(g(c)\,{}^g\eta) = g(c)({}^g\eta)P,$$

and

$${}^g\nu(c\eta) = {}^g(c\eta P) = g(c)({}^g\eta)P,$$

due to the description of the action of G on $L[N/P]$ given in Equation (2.3), repeated above. Hence, ν is G-equivariant, and so ν maps any element fixed under G to another element fixed under G. □

We now state the main lemma of this section, before specialising to the case where G is isomorphic to the quaternion group of order 8.

Lemma 4.1.2. *Let $K = L^P$, let $\mathfrak{A}_{L/F}$ denote the associated order of $\mathfrak{O}_L$ in $L[N]^G$, and let $\mathfrak{A}_{K/F}$ denote the associated order of $\mathfrak{O}_K$ in $L[N/P]^G$. Suppose that $\mathfrak{O}_L$ is a free $\mathfrak{A}_{L/F}$-module and that L/K is at most tamely ramified. Then $\mathfrak{A}_{K/F} = \nu(\mathfrak{A}_{L/F})$ and $\mathfrak{O}_K$ is a free $\mathfrak{A}_{K/F}$-module.*

Proof. Let $\alpha \in \mathfrak{O}_L$ be a free generator of $\mathfrak{O}_L$ as an $\mathfrak{A}_{L/F}$-module, so that $\mathfrak{O}_L = \mathfrak{A}_{L/F} \cdot \alpha$. Since L/K is at most tamely ramified, we have $\mathfrak{O}_K = \mathrm{Tr}_{L/K}(\mathfrak{O}_L)$. Let $\theta = \sum_{\pi \in P} \pi \in L[N]$; then ${}^g\theta = \theta$ for all $g \in G$, since P is a G-stable subgroup of N, and so $\theta \in L[N]^G$. In [KKTU19b, Theorem 2.4] it is shown that $P \cdot 1_G = \mathrm{Gal}(L/K)$. Hence,

$$\theta \cdot x = \sum_{\pi \in P} \pi^{-1}(1_G)[x] = \sum_{g \in \mathrm{Gal}(L/K)} g(x) = \mathrm{Tr}_{L/K}(x)$$

for all $x \in L$.

Since P is normal in N we have $\theta\eta = \eta\theta$ for all $\eta \in N$ and, in particular, $\theta\pi = \theta$ for all $\pi \in P$. So, let $\eta_1, \eta_2, \ldots, \eta_r$ be a set of coset representatives for P in N. Then, each $z \in L[N]^G$ can be uniquely expressed in the form

$$z = \sum_{i=1}^{r} \sum_{\pi \in P} c_{i,\pi} \eta_i \pi$$

where $c_{i,\pi} \in L$. Now for $x \in L$ we have

$$\begin{aligned}
(\theta z) \cdot x &= \left(\theta \sum_{i=1}^{r} \sum_{\pi \in P} c_{i,\pi} \eta_i \pi \right) \cdot x \\
&= \left(\sum_{i=1}^{r} \sum_{\pi \in P} c_{i,\pi} \theta \eta_i \pi \right) \cdot x \\
&= \left(\sum_{i=1}^{r} \sum_{\pi \in P} c_{i,\pi} \eta_i \pi \theta \right) \cdot x \\
&= \left(\sum_{i=1}^{r} \sum_{\pi \in P} c_{i,\pi} \eta_i \pi \right) \cdot (\theta \cdot x) \\
&= \left(\sum_{i=1}^{r} \sum_{\pi \in P} c_{i,\pi} \eta_i P \right) \cdot (\theta \cdot x) \text{ by Equation (2.3)} \\
&= \nu(z) \cdot \mathrm{Tr}_{L/K}(x).
\end{aligned}$$

From this we now have

$$\begin{aligned}
\mathfrak{O}_K &= \mathrm{Tr}_{L/K}(\mathfrak{O}_L) \\
&= \mathrm{Tr}_{L/K}(\mathfrak{A}_{L/F} \cdot \alpha) \\
&= \theta \cdot (\mathfrak{A}_{L/F} \cdot \alpha) \\
&= (\theta \mathfrak{A}_{L/F}) \cdot \alpha \\
&= \nu(\mathfrak{A}_{L/F}) \cdot \mathrm{Tr}_{L/K}(\alpha).
\end{aligned}$$

Therefore $\mathfrak{O}_F$ is a free module of rank one over $\nu(\mathfrak{A}_{L/F})$, which is an order in $L[N/P]^G$. Since the only order in $L[N/P]^G$ over which $\mathfrak{O}_K$ can possibly

be free is its associated order $\mathfrak{A}_{K/F}$ by Proposition 2.3.3, we have $\mathfrak{A}_{K/F} = \nu(\mathfrak{A}_{L/F})$ and $\mathfrak{O}_K$ is a free $\mathfrak{A}_{K/F}$-module. □

We now have enough information to be able to consider the consequences of the previous section in our case.

4.2 Quaternionic extensions

First recall Proposition 2.1.21 that states L/F has a unique biquadratic subextension K/F. Now we may use Corollary 2.1.23 to find a useful property of the unique biquadratic subfield K of the quaternionic extension $L/\mathbb{Q}$.

Proposition 4.2.1. *If the biquadratic field $K = \mathbb{Q}(\alpha, \beta)$ can be embedded into a quaternionic field then $a, b > 0$ and so $K \subset \mathbb{R}$.*

Proof. If K can be embedded into a quaternionic extension $L/\mathbb{Q}$ then so can the quadratic extensions $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$. Then a and b are positive values in $\mathbb{Q}$ as they can be written as the sum of three squares by Corollary 2.1.23. □

Now, our focus of study shall be on tame quaternionic extensions and so it is important to understand necessary conditions for our extension to be tame.

Proposition 4.2.2. *Let $L/\mathbb{Q}$ be a quaternionic field with unique biquadratic subfield K. Then $L/\mathbb{Q}$ is tamely ramified if and only if L/K is tamely ramified and $K/\mathbb{Q}$ is tamely ramified.*

Proof. In general, a tower of number fields is tamely ramified if and only if each layer is tamely ramified. This follows from the fact that ramification indices in towers are multiplicative (see [FT93, Chapter 3, Section 1]). □

4.3 Hopf-Galois structures of cyclic type

For this section let $L/\mathbb{Q}$ be a tame quaternionic extension. We apply Lemma 4.1.2 and argue that $\mathfrak{O}_L$ may not be free over its associated order in any structure of cyclic type.

Proposition 4.3.1. *Let $L/\mathbb{Q}$ be a tame quaternionic extension. Let $L[N]^G$ be a Hopf algebra giving a Hopf-Galois structure of cyclic type on $L/\mathbb{Q}$, and let $\mathfrak{A}$ denote the associated order of $\mathfrak{O}_L$ in $L[N]^G$. Then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module, but not a globally free $\mathfrak{A}$-module.*

Proof. Since $L/\mathbb{Q}$ is a tamely ramified extension of prime power degree and $L[N]^G$ is commutative, we have $\mathfrak{A} = \mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module by Corollary 2.3.16. Since N is cyclic of order 8 it contains a unique subgroup P of order 2, and P is G-stable since G acts on N by automorphisms. Therefore $L^P = K$ is the unique subfield of order 4 over $\mathbb{Q}$. If $\mathfrak{O}_L$ is free over its associated order in $L[N]^G$ then by Lemma 4.1.2 $\mathfrak{O}_K$ is free over its associated order in $L[N/P]^G$. We proceed to show this is impossible.

The field K is a tame biquadratic extension of $\mathbb{Q}$, and is real since it embeds into a quaternionic extension of $\mathbb{Q}$ by Proposition 4.2.1. Since $L/\mathbb{Q}$ is tame, we must have that $K/\mathbb{Q}$ is tame by Proposition 4.2.2. Hence, we may write $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ for some positive squarefree integers a and b that are both congruent to 1 modulo 4 by Proposition 2.1.25. The extension $K/\mathbb{Q}$ admits precisely four Hopf-Galois structures: the classical structure of elementary abelian type and three non-classical structures each of cyclic type (see [Byo02, Theorem 2.5]). Since the quotient group N/P is cyclic of order 4, the Hopf-Galois structure on $K/\mathbb{Q}$ corresponding to N/P must be non-classical. Each of these corresponds to a quadratic subfield $\mathbb{Q}(\sqrt{v})/\mathbb{Q}$ with $v \in \{a, b, ab\}$. Moreover, in [Tru12, Proposition 6.1] it is shown that a necessary condition for $\mathfrak{O}_K$ to be free over its associated order in the Hopf-Galois structure corresponding to the choice v is that there is an integer

solution the equation

$$x^2 + vy^2 = \pm 2d. \tag{4.1}$$

where $d = \gcd(u, v)$ such that $u \in \{a, b, av\} - \{v\}$. If x_0, y_0 are an integer solution to Equation (4.1) then we have $d|x_0^2$ and so, since d is squarefree, $d|x_0$. Therefore we obtain an integer solution to the equation

$$dx^2 + (v/d)y^2 = 2,$$

which is impossible since d and v/d cannot both be 1 because $v > 1$. Therefore $\mathfrak{O}_K$ is not free over its associated order in the Hopf-Galois structure $L[N/P]^G$ on $K/\mathbb{Q}$, and so $\mathfrak{O}_L$ is not free over its associated order in $L[N]^G$. □

Chapter 5

A Class of tame quaternionic fields

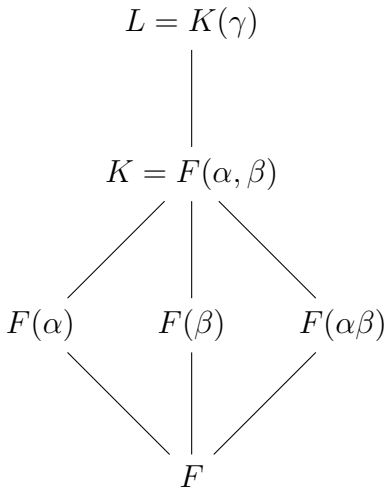
5.1 Constructing quaternionic extensions

Now we have found all of the Hopf-Galois structures on any quaternionic extension, we focus on tame quaternionic extensions $L/\mathbb{Q}$. In order to determine the structure of $\mathfrak{O}_L$ as a module over the associated order of each of the Hopf-Galois structures on $L/\mathbb{Q}$ we will find local generators, for which we need some explicit information about the extensions. To this end, from now on L/F is a quaternionic extension with F a field of characteristic zero. Recall from Proposition 2.1.21 that any quaternionic extension L/F must have a unique biquadratic subextension K/F. We can deduce equivalent conditions for when a biquadratic extension can be embedded into a quaternionic extension.

To understand the properties of a quaternionic extension we need to understand its Galois group. To begin with, it is helpful to understand the Galois group of the unique biquadratic subextension K/F, and how the elements of this group act on the elements of L/K. In doing so we find the

actions of the Galois group of K/F also give sufficient conditions for an extension to be quaternionic.

Lemma 5.1.1. *Let $a, b \in F$ be such that $a, b, ab \notin F^2$, let $\alpha, \beta \in F^{alg}$ satisfy $\alpha^2 = a$, $\beta^2 = b$. Let $K = F(\alpha, \beta)$ and let $s, t \in Gal(K/F)$ be defined by $s(\alpha) = \alpha$, $s(\beta) = -\beta$, $t(\alpha) = -\alpha$ and $t(\beta) = \beta$. Let $c \in K - K^2$ and let $\gamma \in F^{alg}$ be such that $\gamma^2 = c$.*



Then $L = K(\gamma)$ is a quaternionic extension of F if and only if the following conditions are satisfied:

- $\gamma^2 s(\gamma^2) = bx_1^2$ *for some* $x_1 \in F(\alpha)$;
- $\gamma^2 t(\gamma^2) = abx_2^2$ *for some* $x_2 \in F(\beta)$;
- $\gamma^2 st(\gamma^2) = ax_3^2$ *for some* $x_3 \in F(\alpha\beta)$.

Proof. Following the proof of [Fuj90b, Lemma 1] we suppose L/F is a quaternionic extension. Then $K(\gamma) = K(\sqrt{s(\gamma^2)})$ and so $\gamma^2 s(\gamma^2) = \lambda^2$ for some $\lambda \in K$. Since $\gamma^2 s(\gamma^2) = N_{K/F(\alpha)}(\gamma^2) \in F(\alpha)$, λ must have the form x_1 or $x_1\beta$

for some $x_1 \in F(\alpha)$. If $\lambda = x_1 \in F(\alpha)$, then $L = K(\gamma)/F(\alpha)$ is an abelian extension but is not cyclic. We know that $L/F(\alpha)$ is a cyclic extension so λ must have the form $x_1\beta$. That is, $\gamma^2 s(\gamma^2) = bx_1^2$ for some $x_1 \in F(\alpha)$. Similarly, we have $\gamma^2 t(\gamma^2) = abx_2^2$, $\gamma^2 st(\gamma^2) = ax_3^2$ for some $x_2 \in F(\beta)$ and $x_3 \in F(\alpha\beta)$. Conversely, if the conditions hold, then L/F is a Galois extension of degree 8 and the subextensions $L/F(\mu)$ for $\mu \in \{\alpha, \beta, \alpha\beta\}$ are all cyclic of degree 4. Any finite group of order 8 which contains three cyclic subgroups of degree 4 is the quaternion group and so L/F is a quaternionic extension. □

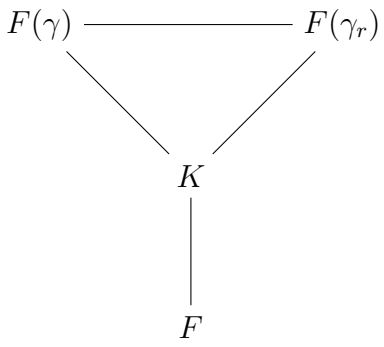
This result does not practically help construct quaternionic extensions, but does provide valuable information about such extensions. Once one has found one such extension, with the biquadratic subextension K/F, it is straightforward to construct infinitely many more and, in fact, all of those quaternionic extensions with biquadratic subextension K/F. The following proposition explains this construction.

Proposition 5.1.2. *Let K be a biquadratic extension of F, let $c \in K - K^2$ and let $\gamma \in F^{alg}$ be such that $\gamma^2 = c$. Suppose that $F(\gamma)$ is a quaternionic extension of F that contains K. For $r \in F^\times$, let $\gamma_r \in F^{alg}$ be such that $\gamma_r^2 = r\gamma^2 = rc$. Then:*

1. *the field $F(\gamma_r)$ is a quaternionic extension of F containing K;*

2. *every quaternionic extension of F containing K is of the form $F(\gamma_r)$ for some $r \in F^\times$;*

3. *$F(\gamma_r) = F(\gamma_{r'})$ if and only if $r/r' \in K^2$.*



Proof. We follow the proof of [Fuj90b, Proposition]. If $L = F(\gamma) = K(\gamma)$ is a quaternionic extension of F, then by Lemma 5.1.1, $F(\gamma_r) = K(\gamma_r)$ is a quaternionic extension of F containing K. Conversely, let L' be any quaternionic extension of F containing K. Then $L' = K(\zeta)$ for some $\zeta^2 \in K$ and, as in the results of Lemma 5.1.1, $K(\zeta/\gamma)$ is a Galois extension of F and the three extensions $K(\zeta/\gamma)/F(\mu)$ with $\mu \in \{\alpha, \beta, \alpha\beta\}$ are all bicyclic. Since a finite group of order 8 which contains three abelian subgroups of type $C_2 \times C_2$ is an abelian group of type $C_2 \times C_2 \times C_2$ we have that $K(\zeta/\gamma)/F$ is an abelian extension of type $C_2 \times C_2 \times C_2$. Hence, $K(\zeta/\gamma)$ has the form $K(\sqrt{r})$ for some $r \in F^\times$, and hence $K(\zeta) = K(\gamma_r)$. Therefore, $L' = K(\zeta) = F(\gamma_r)$.

Finally, as $F(\gamma_r) = K(\gamma_r)$ for $r \in F^\times$, $F(\gamma_{r_1}) = F(\gamma_{r_2})$ for $r_1, r_2 \in F^\times$ if and only if $r_1/r_2 \in K^2$. □

We now only need an explicit construction for finding a quaternionic extension with a given biquadratic subextension. The following theorem is a modified version of a theorem due to Fujisaki ([Fuj90a, Theorem 1]) that gives a straightforward construction. Though it may not account for all quaternionic extensions of a given field, with the previous result we certainly capture infinitely many.

Theorem 5.1.3. *Let $k, m, n, r \in F^\times$, and let $a = k^2 + m^2 + n^2$, $b = m^2 + n^2$. Suppose that $a, b, ab \notin F^2$ and let $\alpha, \beta \in F^{alg}$ satisfy $\alpha^2 = a, \beta^2 = b$. Let*

$\gamma_r \in F^{alg}$ satisfy

$$\gamma_r^2 = r\frac{(a+\alpha\beta)(b+m\beta)}{4}.$$

Then $F(\gamma_r)$ is a quaternionic extension of F with biquadratic subfield $K = F(\alpha,\beta)$. The group $Gal(F(\gamma_r)/F)$ is generated by the automorphisms σ,τ defined by

$$\begin{aligned}
&\sigma(\alpha)=\alpha, && \sigma(\beta)=-\beta, && \sigma(\gamma_r)=\frac{\alpha-\beta}{k}\frac{\beta-m}{n}\gamma_r,\\
&\tau(\alpha)=-\alpha, && \tau(\beta)=\beta, && \tau(\gamma_r)=\frac{\alpha-\beta}{k}\gamma_r,\\
&\sigma\tau(\alpha)=-\alpha, && \sigma\tau(\beta)=-\beta, && \sigma\tau(\gamma_r)=\frac{\beta-m}{n}\gamma_r.
\end{aligned}$$

Proof. Let $K = F(\alpha,\beta)$ be a bicyclic biquadratic extension of F and let $\mathrm{Gal}(K/F) = \{\sigma_0,\sigma_1,\sigma_2,\sigma_3\}$ where $\sigma_0 = 1_K$ is the identity and

$$\begin{aligned}
\sigma_1 &:(\alpha,\beta)\mapsto(\alpha,-\beta),\\
\sigma_2 &:(\alpha,\beta)\mapsto(-\alpha,\beta),\\
\sigma_3 &:(\alpha,\beta)\mapsto(-\alpha,-\beta).
\end{aligned}$$

Let $L = K(\gamma_r)$ with $\gamma_r^2 \in K$ and let $\mu_i : K \to F^{\mathrm{alg}}$ for $i = 0,1,2,3$ denote any fixed embeddings of K into F^{alg} which extend σ_i for $i = 0,1,2,3$ respectively.

Now, as an example, consider μ_2.

$$\begin{aligned}
\mu_2(\gamma_r)^2 &= \sigma_2(\frac{r}{4}(a+\alpha\beta)(b+m\beta))\\
&= \frac{r}{4}(a-\alpha\beta)(b+m\beta)\\
&= \frac{(\alpha-\beta)^2}{k^2}\frac{r}{4}(a+\alpha\beta)(b+m\beta)\\
&= \left(\pm\left(\frac{\alpha-\beta}{k}\right)\gamma_r\right)^2
\end{aligned}$$

so

$$\mu_2(\gamma_r) = e_2\frac{\alpha-\beta}{k}\gamma_r$$

where $e_2 = \pm 1$ is dependent on the choice of μ_2. Similarly,

$$\mu_o(\gamma_r) = e_0\gamma_r,$$

$$\mu_1(\gamma_r) = e_1\frac{\alpha-\beta}{k}\frac{\beta-m}{n}\gamma_r,$$

$$\mu_3(\gamma_r) = e_3\frac{\beta-m}{n}\gamma_r,$$

where $e_0, e_1, e_3 = \pm 1$ is dependent on our choice of μ_i for $i = 0, 1, 3$.

Remark 5.1.4. *If one multiplies each of the above by γ_r and then squares the result one can verify the conditions found in Lemma 5.1.1 hold and so the extension is quaternionic. What follows is an alternative, more direct, route to the same conclusion.*

As one can see, $\mu_i(\gamma_r)$ $(i = 0, 1, 2, 3)$ are all in L for any extension $\mu_i : L \to F^{\text{alg}}$ of σ_i $(i = 0, 1, 2, 3)$ and so it follows that $L = K(\gamma_r)$ is a Galois extension of F and μ_i $(i = 0, 1, 2, 3)$ are automorphisms of L over F.

It is clear, then, that the restriction of μ_i^2 to K is σ_i^2 which is the identity on K due to the isomorphism type of $\text{Gal}(K/F)$. Furthermore $\mu_i^2(\gamma_r) = -\gamma_r$ $(i = 0, 1, 2, 3)$. It follows that $\gamma_r \notin K$ so that $[L : F] = 8$. Hence L/F is a Galois extension of degree 8. Now, it is clear that μ_0^4 maps γ to itself and so is the identity on L. Similarly, μ_i^2 is certainly not the identity on L nor is μ_i^3 which, when restricted to K, also acts like σ_i for each $i = 1, 2, 3$. Choose $e_0 = -1$ so that $\mu_0(\gamma_r) = -\gamma_r$. Then we have

$$id, \mu_0, \mu_1, \mu_1^3, \mu_2, \mu_2^3, \mu_3, \mu_3^3$$

are different automorphisms of L over F and so form the Galois group of L/F. One may assume that each $e_i = 1$ $(i = 1, 2, 3)$ since if any are -1, one can simply replace μ_i with μ_i^3. Under this assumption it is verifiable that the

following relations hold:

$$\mu_i^4 = id \quad (\mu_i^2 \neq id) \quad (i = 1, 2, 3)$$
$$\mu_i^2 = \mu_0 \quad (i = 1, 2, 3)$$
$$\mu_2\mu_1 = \mu_3, \quad \mu_1\mu_3 = \mu_2, \quad \mu_3\mu_2 = \mu_1$$
$$\mu_1^{-1}\mu_2\mu_1 = \mu_2^3 = \mu_2^{-1},$$

where $\mu_i\mu_j$ is defined by $\mu_i\mu_j(x) = \mu_i(\mu_j(x))$ for any $x \in L$. These relations determine that the Galois group $\mathrm{Gal}(L/F)$ is isomorphic to the quaternion group of order 8.

Finally, since it is verifiable that $\mu(\gamma_r) \neq \nu(\gamma_r)$ for any $\mu, \nu \in \mathrm{Gal}(L/F)$ such that $\mu \neq \nu$, it is true that $L = F(\gamma_r)$. To reconcile this notation with that of the statement we note now that $\mu_1 \equiv \sigma$, $\mu_2 \equiv \tau$ and $\mu_3 \equiv \sigma\tau$. □

Using this construction, one can construct infinitely many quaternionic extensions. The construction is always closely linked to the unique biquadratic subfield, a theme that continues to appear throughout this work.

5.2 Tamely ramified quaternionic fields

We wish to study tamely ramified quaternionic extensions of $\mathbb{Q}$. We can find equivalent conditions for when a quaternionic extension of the form described in Theorem 5.1.3 is tame.

First, it is useful to recall that any biquadratic subfield of a quaternionic extension must be totally real, by Proposition 4.2.1. Recall further that it is necessary that $K/\mathbb{Q}$ be tamely ramified in order that $L/\mathbb{Q}$ be tamely ramified, by Proposition 4.2.2. As such we now find a sufficient condition for when $L/\mathbb{Q}$ is tamely ramified under the assumption that $K/\mathbb{Q}$ is.

Proposition 5.2.1. *Let $L/\mathbb{Q}$ be a quaternionic extension with unique biquadratic subfield K, and suppose that $K/\mathbb{Q}$ is tamely ramified. Write*

$L = K(\gamma)$ with $\gamma^2 \in \mathfrak{O}_K$, and suppose that there exists $\lambda \in \mathfrak{O}_K$ such that $\gamma^2 \equiv \lambda^2 \pmod{4\mathfrak{O}_K}$ and $Tr_{K/\mathbb{Q}}(\lambda) = 1$. Then $L/\mathbb{Q}$ is tamely ramified.

Proof. Let $\delta = \frac{\lambda-\gamma}{2} \in L$. Then $(2\delta+\gamma)^2 = \lambda^2$, so δ is a root of $x^2 + \lambda x + \frac{\gamma^2-\lambda^2}{4} = 0$. Since $\gamma, \lambda \in \mathfrak{O}_L$ and $\gamma^2 \equiv \lambda^2 \pmod{4\mathfrak{O}_K}$, the coefficients of this polynomial are algebraic integers, and so $\delta \in \mathfrak{O}_L$. Now we have

$$\begin{aligned}\mathrm{Tr}_{L/\mathbb{Q}}(\delta) &= \mathrm{Tr}_{K/\mathbb{Q}}\Big(\mathrm{Tr}_{L/K}\Big(\frac{\lambda-\gamma}{2}\Big)\Big)\\ &= \mathrm{Tr}_{K/\mathbb{Q}}(\lambda)\\ &= 1.\end{aligned}$$

Therefore $\delta \in \mathfrak{O}_L$ satisfies $\mathrm{Tr}_{L/\mathbb{Q}}(\delta) = 1$, and so $L/\mathbb{Q}$ is tamely ramified. □

Due to our construction in Proposition 5.1.2 we now give an equivalent condition for when $K(\gamma_r)/\mathbb{Q}$ is tamely ramified given that $K(\gamma_1)/\mathbb{Q}$ is.

Proposition 5.2.2. *Let $L/\mathbb{Q}$ be a tamely ramified quaternionic extension with unique biquadratic subfield K. Write $L = K(\gamma)$ with $\gamma^2 \in \mathfrak{O}_K$. Then the tamely ramified quaternionic fields containing K are precisely the fields $K(\gamma_r)$ where $\gamma_r^2 = r\gamma^2$ and r is a squarefree integer congruent to $1 \pmod{4\mathbb{Z}}$.*

Proof. From Proposition 5.1.2 it is clear that the quaternionic fields containing K are precisely the fields $K(\gamma_r)$ where r is a squarefree integer. Since $L/\mathbb{Q}$ is tamely ramified we have that $K/\mathbb{Q}$ is tamely ramified, and so $K(\gamma_r)/\mathbb{Q}$ is tamely ramified if and only if $K(\gamma_r)/K$ is tamely ramified.

Let $\rho \in \mathbb{R}$ be such that $\rho^2 = r$ and suppose $r \equiv 1 \pmod{4\mathbb{Z}}$. Then $L(\rho)/L$ is tame since we have that $(1+\rho)/2$ is an algebraic integer of trace 1 in the extension. Thus $L(\rho)/\mathbb{Q}$ is tame (as it can be formed as a tower of extensions known to be tame). Now $K(\gamma_r)$ is contained in the field $L(\rho) = K(\gamma, \rho)$ and so $K(\gamma_r)/\mathbb{Q}$ is tame as it is a subextension of the tame extension $L(\rho)/\mathbb{Q}$.

Conversely, if $K(\gamma_r)/\mathbb{Q}$ is tame then the composition $K(\gamma, \gamma_r)$ is tame. However, $\gamma_r^2/\gamma^2 = r$ and so $\rho \in K(\gamma, \gamma_r)$. Thus $\mathbb{Q}(\rho) \subseteq K(\gamma, \gamma_r)$, so $\mathbb{Q}(\rho)$ is tame and so $r \equiv 1 \pmod{4\mathbb{Z}}$. □

To understand the reliance of our construction of tamely ramified quaternionic extensions on the construction of the biquadratic subfield and, more specifically, on the principal remainders of a and b modulo 16, we state the possible congruences of a and b.

Lemma 5.2.3. *Let $k, m, n \in \mathbb{Z} - \{0\}$ with m odd and k, n even. Let $a = k^2 + m^2 + n^2$, $b = m^2 + n^2$. The possible principal remainders of a, b modulo 16 are shown in the following table*

b \ a	*1*	*5*	*9*	*13*
1	✓	✓	✗	✗
5	✗	✓	✓	✗
9	✗	✗	✓	✓
13	✓	✗	✗	✓

We now compile these results to give us the conclusions we have been working towards. We find that $L/\mathbb{Q}$ is a tamely ramified quaternionic extension of the type described in Theorem 5.1.3 if and only if conditions, involving those elements constructing K and the number r that is intrinsic in generating our quaternionic extensions, hold, and that such a result is sufficient to describe when any quaternionic extension of the form constructed in Theorem 5.1.3 is tame.

Theorem 5.2.4. *Let $k, m, n \in \mathbb{Z} - \{0\}$ with m odd and k, n even, and let $a = k^2 + m^2 + n^2$, $b = m^2 + n^2$. Suppose that $a, b, ab \notin \mathbb{Z}^2$ and let $\alpha, \beta \in \mathbb{Q}^{alg}$ satisfy $\alpha^2 = a, \beta^2 = b$. Let $r \in \mathbb{Z}$ and let $\gamma_r \in \mathbb{Q}^{alg}$ satisfy*

$$\gamma_r^2 = \frac{r}{4}(a + \alpha\beta)(b + m\beta).$$

Then

1. *γ_r is an algebraic integer;*

2. *$\mathbb{Q}(\gamma_r)$ is a quaternionic extension of $\mathbb{Q}$ with biquadratic subfield $K = \mathbb{Q}(\alpha, \beta)$;*

3. *every quaternionic field with biquadratic subfield $\mathbb{Q}(\alpha, \beta)$ has the form $\mathbb{Q}(\gamma_r)$ for some squarefree $r \in \mathbb{Z}$;*

4. *if $k \equiv n \pmod 4$ then $\mathbb{Q}(\gamma_r)/\mathbb{Q}$ is tamely ramified if and only if $r \equiv 1 \pmod 4$;*

5. *if $k \not\equiv n \pmod 4$ than $\mathbb{Q}(\gamma_r)/\mathbb{Q}$ is tamely ramified if and only if $r \equiv -1 \pmod 4$.*

Proof. We prove each part separately.

1. Since $a \equiv b \equiv 1 \pmod{4\mathbb{Z}}$ the numbers $\frac{1+\alpha\beta}{2}$ and $\frac{1+\beta}{2}$ are algebraic integers, and so (since m is odd) the numbers $\frac{a+\alpha\beta}{2}$ and $\frac{b+m\beta}{2}$ are algebraic integers. Therefore γ_r is an algebraic integer.

2. This is immediate from Theorem 5.1.3.

3. This is immediate from parts 2 and 3 of Proposition 5.1.2.

4. Suppose that $k \equiv n \pmod 4$. By Proposition 5.2.2, it is sufficient to show that $\mathbb{Q}(\gamma_1)/\mathbb{Q}$ is tamely ramified. We show that there exists some $\lambda \in \mathfrak{O}_K$ such that $\gamma_1^2 \equiv \lambda^2 \pmod{4\mathfrak{O}_K}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = 1$. By Proposition 5.2.1 this implies $\mathbb{Q}(\gamma_1)/\mathbb{Q}$ is tamely ramified. We have $k^2 \equiv n^2 \pmod{16}$, and $m^2 \equiv 1, 9 \pmod{16}$. First, if $k \equiv n \equiv 0$

(mod 4) then $k^2 \equiv n^2 \equiv 0 \pmod{16}$. We have

$$\begin{aligned}\left(\frac{1+m\beta}{2}\right)^2 &= \frac{1+(m^2-2)b}{4} + \frac{b+m\beta}{2} \\ &= \frac{1+(m^2-2)(m^2+n^2)}{4} + \frac{b+m\beta}{2} \\ &\equiv \frac{1+m^2(m^2-2)}{4} + \frac{b+m\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\beta)}} \\ &= \frac{b+m\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\beta)}},\end{aligned}$$

since $m^2(m^2-2) \equiv -1 \pmod{16}$ for all odd m. Similarly, we have

$$\left(\frac{1+\alpha\beta}{2}\right)^2 = \frac{1+a(b-2)}{4} + \frac{a+\alpha\beta}{2} \equiv \frac{a+\alpha\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\alpha\beta)}},$$

since $a(b-2) \equiv b(b-2) \equiv -1 \pmod{16}$. Therefore we have $\gamma_1^2 \equiv \lambda^2 \pmod{4\mathfrak{O}_K}$ with

$$\lambda = \frac{1+\alpha\beta}{2}\frac{1+m\beta}{2},$$

which satisfies $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = 1$, and so by Proposition 5.2.1, $\mathbb{Q}(\gamma_1)/\mathbb{Q}$ is tamely ramified.

Now, if $k \equiv n \equiv 2 \pmod 4$ then $k^2 \equiv n^2 \equiv 4 \pmod{16}$. We have

$$\begin{aligned}\left(\frac{1-m\beta}{2}\right)^2 &= \frac{1+(m^2+2)b}{4} - \frac{b+m\beta}{2} \\ &= \frac{1+(m^2+2)(m^2+n^2)}{4} - \frac{b+m\beta}{2} \\ &\equiv \frac{1+(m^2+2)(m^2+4)}{4} - \frac{b+m\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\beta)}} \\ &\equiv -\frac{b+m\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\beta)}},\end{aligned}$$

since $(m^2+2)(m^2+4) \equiv -1 \pmod{16}$ for all odd m. Similarly, we

have

$$\left(\frac{1-\alpha\beta}{2}\right)^2 = \frac{1+a(b+2)}{4} - \frac{a+\alpha\beta}{2}$$
$$\equiv -\frac{a+\alpha\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\alpha\beta)}},$$

since $a(b+2) \equiv a(a-2) \equiv -1 \pmod{16}$. Therefore we have $\gamma_1^2 \equiv \lambda^2 \pmod{4\mathfrak{O}_K}$ with

$$\lambda = \frac{1-\alpha\beta}{2}\frac{1-m\beta}{2},$$

which satisfies $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = 1$, and so by Proposition 5.2.1, $\mathbb{Q}(\gamma_1)/\mathbb{Q}$ is tamely ramified.

5. Suppose that $k \not\equiv n \pmod 4$. By Proposition 5.2.2, it is sufficient to show that $\mathbb{Q}(\gamma_{-1})/\mathbb{Q}$ is tamely ramified as we can identify all extensions $\mathbb{Q}(\gamma_r)/\mathbb{Q}$ where $r \equiv -1 \pmod 4$ with the extensions $\mathbb{Q}(\gamma_{-s})/\mathbb{Q}$ where $s \equiv 1 \pmod 4$. We show that there exists some $\lambda \in \mathfrak{O}_K$ such that $\gamma_1^2 \equiv -\lambda^2 \pmod{4\mathfrak{O}_K}$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = 1$. Since this is equivalent to $\gamma_{-1}^2 \equiv \lambda^2 \pmod{4\mathfrak{O}_K}$, by Proposition 5.2.1 this implies $\mathbb{Q}(\gamma_{-1})/\mathbb{Q}$ is tamely ramified. We have that $m^2 \equiv 1, 9 \pmod{16}$. First, if $k \equiv 2 \pmod 4$, $n \equiv 0 \pmod 4$ then we have

$$\left(\frac{1+m\beta}{2}\right)^2 \equiv \frac{b+m\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\beta)}}$$

as in part 4, since we have $n \equiv 0 \pmod 4$. Moreover

$$\left(\frac{1-\alpha\beta}{2}\right)^2 \equiv -\frac{a+\alpha\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\alpha\beta)}}$$

as in part 4, since we have $k \equiv 2 \pmod 4$ as above. This satisfies $-\gamma_1^2 \equiv \lambda^2 \pmod{4\mathfrak{O}_K}$ and

$$\lambda = \frac{1+m\beta}{2}\frac{1-\alpha\beta}{2}$$

which clearly satisfies $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = 1$.

Now, if $k \equiv 0 \pmod 4$ and $n \equiv 2 \pmod 4$ then we have

$$\left(\frac{1-m\beta}{2}\right)^2 \equiv -\frac{b+m\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\beta)}}$$

as in part 4, since we have $n \equiv 2 \pmod 4$. Moreover

$$\left(\frac{1+\alpha\beta}{2}\right)^2 \equiv \frac{a+\alpha\beta}{2} \pmod{4\mathfrak{O}_{\mathbb{Q}(\alpha\beta)}}$$

as in part 4, since we have $k \equiv 0 \pmod 4$. This satisfises $-\gamma_1^2 = \lambda^2 \pmod{4\mathfrak{O}_K}$ and

$$\lambda = \frac{1-m\beta}{2}\frac{1+\alpha\beta}{2}$$

which clearly satisfies $\mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = 1$. So, in either case, $\mathbb{Q}(\gamma_{-1})/\mathbb{Q}$ is tamely ramified by Proposition 5.2.1.

□

Remark 5.2.5. *We refer to extensions of the form described in Theorem 5.2.4 as* Fujisaki *extensions. That is a Fujisaki extension is an extension $L/\mathbb{Q}$ such that $L = \mathbb{Q}(\gamma_r)$ where $\gamma_r^2 = \frac{r}{4}(a+\alpha\beta)(b+m\beta)$ as defined above.*

5.3 Discriminants and integral bases

Suppose that $L/\mathbb{Q}$ is a tamely ramified quaternionic field with biquadratic subfield K. Write $K = \mathbb{Q}(\alpha, \beta)$ with $\alpha^2 = a$, $\beta^2 = b$ squarefree integers, necessarily congruent to 1 modulo 4. In order to find local generators we first need to ascertain a $\mathbb{Z}_p$-basis for $\mathfrak{O}_{L,p}$ for each prime p. To do this we consider the discriminant of $L/\mathbb{Q}$ and compare it to an $\mathfrak{O}_K$-module with a specified basis. First we consider the ramification of each prime p.

Lemma 5.3.1. *No prime number p is totally ramified in $L/\mathbb{Q}$.*

Proof. We show that no prime number p is totally ramified in $K/\mathbb{Q}$. For a quadratic extension $\mathbb{Q}(\delta)$ with $\delta^2 = d$ a squarefree integer, a prime number $p > 2$ splits in $\mathbb{Q}(\delta)$ if and only if $\left(\frac{d}{p}\right) = 1$. Since the Legendre symbol is totally multiplicative in the top entry, at least one of $\left(\frac{a}{p}\right)$, $\left(\frac{b}{p}\right)$, $\left(\frac{ab}{p}\right)$ is equal to 1, and so splits in at least one of the subextensions $\mathbb{Q}(\alpha)/\mathbb{Q}$, $\mathbb{Q}(\beta)/\mathbb{Q}$, $\mathbb{Q}(\alpha\beta)/\mathbb{Q}$. Also, the prime 2 is unramified as the extension is tame. Therefore p is not totally ramified in $K/\mathbb{Q}$ for any prime p. □

Any prime that does ramify, then, may still not totally ramify, but will appear in the discriminant of $L/\mathbb{Q}$. We determine the power with which ramifying primes appear.

Proposition 5.3.2. *Let p be a prime number that ramifies in $L/\mathbb{Q}$. Then*

$$\nu_p(\mathfrak{d}(L/\mathbb{Q})) = \begin{cases} 6 & \text{if } p \text{ ramifies in } K/\mathbb{Q} \\ 4 & \text{otherwise.} \end{cases}$$

Proof. Let e_p denote the ramification index of p in L. If p ramifies in $K/\mathbb{Q}$ then $e_p > 2$, but we have $e_p \neq 8$ by Lemma 5.3.1, so we must have $e_p = 4$. Since the ramification is tame, [Neu13, Chapter III, Section 2, Theorem 2.6] implies that $\nu_{\mathfrak{P}}(\mathfrak{D}(L/\mathbb{Q})) = 3$ for each prime ideal $\mathfrak{P}$ of $\mathfrak{O}_L$ lying above p, and then [Neu13, Chapter III, Section 2, Theorem 2.9] implies that $\nu_p(\mathfrak{d}(L/\mathbb{Q})) = 6$. If p does not ramify in $K/\mathbb{Q}$ then $e_p = 2$, and we have $\nu_{\mathfrak{P}}(\mathfrak{D}(L/\mathbb{Q})) = 1$ for each prime ideal $\mathfrak{P}$ of $\mathfrak{O}_L$ lying above p. Finally, [Neu13, Chapter III, Section 2, Theorem 2.10] implies that $\nu_p(\mathfrak{d}(L/\mathbb{Q})) = 4$. □

We now work with a certain $\mathfrak{O}_K$-module, Γ, defined via a specified basis, and consider its discriminant along with that of $L/\mathbb{Q}$. First, we must specialize to tame Fujisaki extensions and we begin by finding the discriminant of Γ so that we may use it as a comparison for $\mathfrak{O}_{L,p}$.

Lemma 5.3.3. *Let $L = \mathbb{Q}(\gamma_r)$ be a tame Fujisaki extension. Suppose that a and b are squarefree, that $(a, b) = 1$ and that r is a squarefree odd integer satisfying $(r, ab) = 1$. Let*

$$\Gamma = \mathbb{Z}\langle 1, \alpha, \beta, \alpha\beta, \gamma_r, \sigma(\gamma_r), \tau(\gamma_r), \sigma\tau(\gamma_r)\rangle \subset L.$$

The discriminant of Γ in the extension $L/\mathbb{Q}$ is denoted and given by

$$\mathfrak{d}(\Gamma) = 2^{16}a^6b^6r^4.$$

Proof. Taking the trace map $\mathrm{Tr} : L \to \mathbb{Q}$ we have

$$\mathrm{Tr}(1) = 8, \quad \mathrm{Tr}(\alpha) = 0, \quad \mathrm{Tr}(\beta) = 0, \quad \mathrm{Tr}(\alpha\beta) = 0, \quad \mathrm{Tr}(a\beta) = 0,$$

$$\mathrm{Tr}(b\alpha) = 0, \quad \mathrm{Tr}(a) = 8a, \quad \mathrm{Tr}(b) = 8b, \quad \mathrm{Tr}(ab) = 8ab, \quad \mathrm{Tr}(\gamma_r) = 0,$$

$$\mathrm{Tr}(\sigma(\gamma_r)) = 0, \quad \mathrm{Tr}(\tau(\gamma_r)) = 0, \quad \text{and} \quad \mathrm{Tr}(\sigma\tau(\gamma_r)) = 0.$$

Moreover,

$$\begin{aligned}\mathrm{Tr}_{L/\mathbb{Q}}(\gamma_r^2) &= 2\mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{r(a+\alpha\beta)(b+m\beta)}{4}\right)\\ &= 2\mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{abr}{4}\right) + 0\\ &= 2abr,\end{aligned}$$

and

$$\begin{aligned}\mathrm{Tr}_{L/\mathbb{Q}}(\gamma_r\tau(\gamma_r)) &= 2\mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{\alpha-\beta}{k}\gamma_r^2\right)\\ &= 2\mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{r(mba-mab)}{4k}\right) + 0\\ &= 0.\end{aligned}$$

Similarly, we can find, $\mathrm{Tr}(\gamma_r\sigma(\gamma_r)) = \mathrm{Tr}(\gamma_r\sigma\tau(\gamma_r)) = 0$ which is enough to give

$$\mathrm{Tr}(\sigma(\gamma_r)^2) = 2abr,\ \mathrm{Tr}(\tau(\gamma_r)^2) = 2abr,\ \mathrm{Tr}(\sigma\tau(\gamma_r)^2) = 2abr,\ \mathrm{Tr}(\gamma_r\sigma\tau(\gamma_r)) = 0,$$

$$\mathrm{Tr}(\sigma(\gamma_r)\tau(\gamma_r)) = 0,\ \mathrm{Tr}(\sigma(\gamma_r)\sigma\tau(\gamma_r)) = 0,\ \text{and } \mathrm{Tr}(\tau(\gamma_r)\sigma\tau(\gamma_r)) = 0.$$

Consequently, we have

$$\mathfrak{d}(\Gamma) = \det \begin{pmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 8b & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 8ab & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2abr & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2abr & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2abr & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2abr \end{pmatrix} = 2^{16}a^6b^6r^4.$$

□

Proposition 5.3.4. *Let $r = 1$ or $r = -1$ and let $L = \mathbb{Q}(\gamma_r)$ be a quaternionic field. Suppose that $L/\mathbb{Q}$ is a tame Fujisaki extension such that a and b are squarefree in $\mathbb{Z}$ and $(a, b) = 1$. Define Γ as in Lemma 5.3.3. Then*

1. *$\mathfrak{d}(L/\mathbb{Q}) = a^6b^6$,*

2. *for all odd prime numbers p we have $\mathfrak{O}_{L,p} = \Gamma_p$.*

Proof. Since $(a, b) = 1$ we have

$$\mathfrak{d}(K/\mathbb{Q}) = \mathfrak{d}(\mathbb{Q}(\alpha)/\mathbb{Q})\mathfrak{d}(\mathbb{Q}(\beta)/\mathbb{Q}) = a^2b^2,$$

and so Proposition 5.3.2 implies that $a^6b^6|\mathfrak{d}(L/\mathbb{Q})$. Now, clearly we have $\Gamma \subset \mathfrak{O}_L$, and by Lemma 5.3.3 we know that $\mathfrak{d}(\Gamma) = 2^{16}a^6b^6$.

Now, $\mathfrak{d}(\mathfrak{O}_L)|\mathfrak{d}(\Gamma)$ and we know $2 \nmid \mathfrak{d}(\mathfrak{O}_L)$ since $L/\mathbb{Q}$ is tame, thus $\mathfrak{d}(\mathfrak{O}_L) = a^6b^6$ as required for part 1.

So, for part 2, note that if p is an odd prime number then we have

$$[\mathfrak{O}_{L,p} : \Gamma_p]^2 = [\mathfrak{O}_L : \Gamma]_p^2 = \frac{\mathfrak{d}(\mathfrak{O}_L)}{\mathfrak{d}(\Gamma)} = 2^{16} \in \mathbb{Z}_p^\times,$$

and so $\mathfrak{O}_{L,p} = \Gamma_p$. □

We must now consider the same problem when $r \neq \pm 1$ and when the quaternionic field L is a tame Fujisaki extension over $\mathbb{Q}$.

Proposition 5.3.5. *Let $L = \mathbb{Q}(\gamma_r)$ be a tame Fujisaki extension. Suppose that a and b are squarefree, $(a, b) = 1$, and that r is a squarefree odd integer satisfying $(r, ab) = 1$. Let Γ be defined as in Lemma 5.3.3. Then*

1. $\mathfrak{d}(L/\mathbb{Q}) = a^6b^6r^4$,

2. *for all odd prime numbers p we have $\mathfrak{O}_{L,p} = \Gamma_p$.*

Proof. Suppose that $r \equiv 1 \pmod 4$. Here, if $r \equiv -1 \pmod 4$ then we replace γ_1 with γ_{-1} in the following. As in Proposition 5.3.4, we have $a^6b^6|\mathfrak{d}(L/\mathbb{Q})$. Now let p be a prime number dividing r and $\mathfrak{p}$ a prime ideal of $\mathfrak{O}_K$ lying above p. Using Proposition 5.3.2, we see that to prove part 1 it is sufficient to show that p is unramified in $K/\mathbb{Q}$ and $\mathfrak{p}$ is ramified in L/K. The first is easy since $(r, ab) = 1$ so any prime dividing r does not divide the discriminant of $K/\mathbb{Q}$, which is a^2b^2, and so is unramified. For the second part we note by [HGK81, Theorem 118] that $\mathfrak{p}$ is ramified in L/K if and only if $\nu_\mathfrak{p}(\gamma_r^2)$ is odd. We have $r \equiv 1 \pmod 4$ and $L/\mathbb{Q}$ is tamely ramified, so $\mathfrak{d}(K(\gamma_1)/\mathbb{Q}) = a^6b^6$ by Proposition 5.3.4, and so p is unramified in $K(\gamma_1)/\mathbb{Q}$. Therefore $\nu_\mathfrak{p}(\gamma_1^2)$ is even. Now we have

$$\nu_\mathfrak{p}(\gamma_r^2) = \nu_\mathfrak{p}(r\gamma_1^2) = \nu_\mathfrak{p}(r) + \nu_\mathfrak{p}(\gamma_1^2),$$

so $\nu_{\mathfrak{p}}(\gamma_r^2)$ is odd if and only if $\nu_{\mathfrak{p}}(r)$ is odd. Finally, since $(r, ab) = 1$, we know that p is not ramified in $K/\mathbb{Q}$, so $\nu_{\mathfrak{p}}(r) = \nu_p(r)$, which is odd since r is squarefree. Therefore $\mathfrak{p}$ is ramified in L/K, and so $\mathfrak{d}(L/\mathbb{Q}) = a^6b^6r^4$. The proof of part 2 is analogous to part 2 of Proposition 5.3.4 since $\mathfrak{d}(\Gamma) = 2^{16}a^6b^6r^4$ by Lemma 5.3.3. □

We have ascertained a basis for $\mathfrak{O}_{L,p}$ and can use this to find the local generators we seek.

5.4 Galois module structure

Before we find these local generators we first look at what we know of the module structure of $\mathfrak{O}_L$ as a $\mathbb{Z}[G]$-module. Letting $L/\mathbb{Q}$ be a Fujisaki extension defined in Remark 5.2.5 we will also suppose that a and b are squarefree, $(a, b) = 1$ and that r is an odd, squarefree integer such that $(r, ab) = 1$. We first recall Theorem 2.1.26, a result due to Martinet (1971) that gives a criterion for when $\mathfrak{O}_L$ is free over $\mathbb{Z}[G]$. Recall that this is freeness in the classical case, and we wish to further investigate freeness when our extension is adorned with Hopf-Galois structures that are not the classical one. This result allows us to ascertain the answer to this with the classical structure with a much simpler method.

We now find the possible values of ψ and ϕ from Theorem 2.1.26 for tame Fujisaki extensions.

Proposition 5.4.1. *Let $L = \mathbb{Q}(\gamma_r)$ be a tame Fujisaki extension of $\mathbb{Q}$. Suppose that a and b are squarefree and $(a, b) = 1$. Then*

$$\phi = \begin{cases} 1 \pmod 4 & \text{if } k \equiv 0 \pmod 4 \\ -1 \pmod 4 & \text{if } k \equiv 2 \pmod 4. \end{cases}$$

Proof. Since $(a, b) = 1$ the discriminants of the three quadratic subfields of $L/\mathbb{Q}$ are a, b, ab. Recalling that $a = k^2 + m^2 + n^2$ and $b = m^2 + n^2$ with m odd and k, n even we have

$$1 + a + b + ab = (1 + b)(1 + b + k^2) = (1 + b)^2 + k^2(1 + b).$$

We know that $b \equiv 1 \pmod 4$ so $b+1 \equiv 2 \pmod 4$ and $(b+1)^2 \equiv 4 \pmod{16}$. If $k \equiv 0 \pmod 4$ then $k^2 \equiv 0 \pmod{16}$ and we have $1 + a + b + ab \equiv 4 \pmod{16}$, so $\phi \equiv 1 \pmod 4$. If $k \equiv 2 \pmod 4$ then $k^2 \equiv 4 \pmod{16}$ and we have $1 + a + b + ab \equiv 4 + 8(2b' + 1) \pmod{16}$ for some integer b'. Hence $1 + a + b + ab \equiv 12 \pmod{16}$ and $\phi \equiv -1 \pmod 4$. □

Proposition 5.4.2. *Let $L = \mathbb{Q}(\gamma_r)$ be a tame Fujisaki extension of $\mathbb{Q}$. Suppose that a and b are squarefree and $(a, b) = 1$ and that $(r, ab) = 1$. Then*

$$\psi \equiv \epsilon|r| \pmod 4$$

where $\epsilon = 1$ if L is real and $\epsilon = -1$ otherwise.

Proof. Proposition 5.3.4 gives $\Delta = a^6b^6r^4$ so $p|\Delta$ if and only if $p|abr$ so

$$\prod_{p|\Delta} p = \prod_{p|abr} p = |abr| = ab|r|$$

since a, b and r are squarefree, pairwise coprime and $a, b > 0$. Since a, b are both congruent to 1 modulo 4 we have that

$$ab|r| \equiv |r| \pmod 4.$$

□

With these results we have the following useful corollary.

Corollary 5.4.3. *Let $L = \mathbb{Q}(\gamma_r)$ be a tame quaternionic extension of $\mathbb{Q}$. Suppose a and b are squarefree and $(a, b) = 1$ and that $(r, ab) = 1$. Then $\mathfrak{O}_L$ is a free $\mathbb{Z}[G]$-module if and only if $n \equiv 0 \pmod 4$.*

Proof. Let $k \equiv n \equiv 0 \pmod 4$, then $r \equiv 1 \pmod 4$ by Theorem 5.2.4. Thus $\phi \equiv 1 \pmod 4$ by Proposition 5.4.1 and $\psi \equiv 1 \pmod 4$ by Proposition 5.4.2 since either $r > 0$ so that $|r| \equiv 1 \pmod 4$ and $\epsilon = 1$ (L is real) or $r < 0$ so that $|r| \equiv -1 \pmod 4$ and $\epsilon = -1$ (L is not real).

Let $k \equiv n \equiv 2 \pmod 4$, then $r \equiv 1 \pmod 4$ by Theorem 5.2.4. Thus $\phi \equiv -1 \pmod 4$ by Proposition 5.4.1 but $\psi \equiv 1 \pmod 4$ by Proposition 5.4.2 as above.

Let $k \equiv 2 \pmod 4$, $n \equiv 0 \pmod 4$, then $r \equiv -1 \pmod 4$ by Theorem 5.2.4. Thus $\phi \equiv -1 \pmod 4$ by Proposition 5.4.1 and $\psi \equiv -1 \pmod 4$ by Proposition 5.4.2 since either $r > 0$ so that $|r| \equiv -1 \pmod 4$ and $\epsilon = 1$ or $r < 0$ so that $|r| \equiv 1 \pmod 4$ and $\epsilon = -1$.

Let $k \equiv 0 \pmod 4$, $n \equiv 2 \pmod 4$, then $r \equiv -1 \pmod 4$ by Theorem 5.2.4. Thus $\phi \equiv 1 \pmod 4$ by Proposition 5.4.1 but $\psi \equiv -1 \pmod 4$ by Proposition 5.4.2 as above. □

Remark 5.4.4. *It is worth noting that it is obvious the choice of r cannot affect whether or not $\mathfrak{O}_L$ is a free $\mathbb{Z}[G]$-module.*

Example 5.4.5. *Recall Example 2.1.28. We have $L = \mathbb{Q}(\gamma)$ with $\gamma^2 = \frac{5+\sqrt{5}}{2}\frac{41+\sqrt{5\cdot 41}}{2}$. This is a tame Fujisaki extension for which $\mathfrak{O}_L$ is not free over $\mathbb{Z}[G]$.*

Example 5.4.6. *Construct a Fujisaki extension with $m = 5$, $n = 6$ and $k = 2$. Let $L = \mathbb{Q}(\gamma_5)$ so that $L/\mathbb{Q}$ is tame by Theorem 5.2.4. Then we find $\phi \equiv -1 \pmod 4$ and $\psi \equiv 1 \pmod 4$ so that $\mathfrak{O}_L$ is not free over $\mathbb{Z}[G]$. However, letting $m = 5$, $n = 4$ and $k = 6$ gives a quaternionic extension $\mathbb{Q}(\gamma_{-1})/\mathbb{Q}$ that is tame. Moreover $\phi \equiv -1 \pmod 4$ and $\psi \equiv -1 \pmod 4$ (so $n \equiv 0 \pmod 4$) so that $\mathfrak{O}_L$ is free over $\mathbb{Z}[G]$.*

Chapter 6

Local freeness and generators

In this chapter we assume that $L/\mathbb{Q}$ is a tame Fujisaki extension with Galois group G, and that $H = L[N]^G$ is a Hopf algebra giving a Hopf-Galois structure on the extension. Note that from now on we denote by γ the element γ_r such that $\mathbb{Q}(\gamma_r) = L$. We will prove the following theorem.

Theorem 6.0.1. *If $L/\mathbb{Q}$ is a tame Fujisaki extension then $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$ for all H.*

Due to Proposition 2.3.12 we know that this is true for H commutative and so we start by proving the result for the structures of dihedral type, and find the result for the classical and nonclassical structures is straightforward.

In addition, for each Hopf algebra H giving a Hopf-Galois structure on $L/\mathbb{Q}$ and each prime number p, we obtain an explicit local generator, denoted by x_p, of $\mathfrak{O}_{L,p}$ as an $\mathfrak{A}_{H,p}$-module, for all but the cyclic structures. In fact, we largely omit the cyclic structures from now on as we have found that $\mathfrak{O}_L$ is not globally free over $\mathfrak{A}_H$ for any H of cyclic type by Proposition 4.3.1 and so we cannot hope to do better than local freeness, a result we already have, thus explicit generators will not serve any purpose for our investigations.

6.1 Local generators for $p = 2$

First, we may find a local generator for the prime $p = 2$. Note here that we make no assumptions of the type of the Hopf-Galois structure as the following argument holds for all H. We start by proving that the associated orders at the prime 2 have certain necessary properties, that leads to the second proposition that the associated orders at 2 are local rings.

Proposition 6.1.1. *We have $\mathfrak{A}_{H,2} = \mathfrak{O}_{L,2}[N]^G$, that $\mathfrak{A}_{H,2}$ is a Hopf order in H_2, and $\mathfrak{O}_{L,2}$ is a free $\mathfrak{A}_{H,2}$-module.*

Proof. Since $L/\mathbb{Q}$ is tamely ramified and has 2-power degree, the prime number 2 must be unramified in $L/\mathbb{Q}$. Thus the result follows from [Tru11, Theorem 5.4]. □

Proposition 6.1.2. *The Hopf order $\mathfrak{A}_{H,2}$ is a local ring.*

Proof. By Proposition 6.1.1 we have $\mathfrak{A}_{H,2} = \mathfrak{O}_{L,2}[N]^G$. By Theorem 2.3.8, it is sufficient to show that if $z \in \mathfrak{O}_{L,2}[N]^G$ then either z or $1 - z$ is a unit of $\mathfrak{O}_{L,2}[N]^G$. Suppose that $z \notin (\mathfrak{O}_{L,2}[N]^G)^\times$, then $z \notin (\mathfrak{O}_{L,2}[N])^\times$ as otherwise there would exist $w \in \mathfrak{O}_{L,2}[N]$ such that $wz = zw = 1$, and the fact that z and 1 lie in $\mathfrak{O}_{L,2}[N]^G$ would force $w \in \mathfrak{O}_{L,2}[N]^G$ as well. Now recall the isomorphism

$$\mathfrak{O}_{L,2} \cong \prod_{\mathfrak{P}|2} \mathfrak{O}_{L,\mathfrak{P}}$$

from [FT93, Chapter III, §1, equation 1.8]. This induces an isomorphism

$$\mathfrak{O}_{L,2}[N] \cong \prod_{\mathfrak{P}|2} \mathfrak{O}_{L,\mathfrak{P}}[N],$$

and since each $\mathfrak{O}_{L,\mathfrak{P}}$ has residue characteristic 2, and N is a 2-group, each factor on the right hand side is a local ring by [CR81, §5.25]. Write $(z_\mathfrak{P})_\mathfrak{P}$ for the image of z on the right hand side, and write $\mathfrak{m}_\mathfrak{P}$ for the maximal ideal of $\mathfrak{O}_{L,\mathfrak{P}}[N]$. Since $z \notin (\mathfrak{O}_{L,2}[N])^\times$ we have $z_\mathfrak{P} \in \mathfrak{m}_\mathfrak{P}$ for some $\mathfrak{P}$. But

G acts transitively on the prime ideals of $\mathfrak{O}_L$ lying above 2 due to [Neu13, Proposition 9.1], and z is fixed by G, so in fact we have $z_{\mathfrak{P}} \in \mathfrak{m}_{\mathfrak{P}}$ for all $\mathfrak{P}$. Therefore $1 - z_{\mathfrak{P}} \notin \mathfrak{m}_{\mathfrak{P}}$ for each $\mathfrak{P}$, so $1 - z_{\mathfrak{P}} \in (\mathfrak{O}_{L,\mathfrak{P}}[N])^\times$ for each $\mathfrak{P}$ and so $1 - z$ is a unit of $\mathfrak{O}_{L,2}[N]$. Since $1 - z$ is fixed by G, this implies that $1 - z$ is a unit of $\mathfrak{O}_{L,2}[N]^G$. Therefore $\mathfrak{O}_{L,2}[N]^G$ is a local ring. □

The above result is necessary to use a result of Childs and Hurley that gives us a sufficient condition for an element to be a free generator as required. We finally give an explicit generator of $\mathfrak{O}_{L,2}$ as an $\mathfrak{A}_{H,2}$-module.

Proposition 6.1.3. *An explicit generator of $\mathfrak{O}_{L,2}$ as an $\mathfrak{A}_{H,2}$-module is*

$$x_2 := \frac{\gamma + \lambda}{2}$$

where

$$\lambda = \frac{1}{4}\Big(1 + (-1)^{k/2}\alpha\beta\Big)\Big(1 + (-1)^{n/2}m\beta\Big).$$

This value of λ is a general form of the values of λ found in the proof of Theorem 5.2.4.

Proof. By Proposition 6.1.2 and Proposition 6.1.1, $\mathfrak{A}_{H,2} = \mathfrak{O}_{L,2}[N]^G$ is a local Hopf order in H_2. The element $\theta = \sum_{\eta \in N} \eta$ is a generator of the module of left integrals of $\mathfrak{A}_{H,2}$, and so following the proof of Theorem 2.3.7 (see [Chi00, Proposition 14.7]) a sufficient condition for an element $x \in \mathfrak{O}_{L,2}$ to be a free generator of $\mathfrak{O}_{L,2}$ as an $\mathfrak{A}_{H,2}$-module is that $\theta \cdot x = 1$. We have $\theta \cdot x = \mathrm{Tr}_{L/\mathbb{Q}}(x)$ for all $x \in \mathfrak{O}_{L,2}$, so we verify that the trace of the element $\frac{1}{2}(\gamma + \lambda) \in \mathfrak{O}_{L,2}$ is 1. We have

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = 0, \quad \mathrm{Tr}_{L/\mathbb{Q}}(\beta) = 0, \quad \mathrm{Tr}_{L/\mathbb{Q}}(\alpha\beta) = 0 \text{ and } \mathrm{Tr}_{L/\mathbb{Q}}(\gamma) = 0.$$

Hence

$$\mathrm{Tr}_{L/\mathbb{Q}}\Big(\frac{\gamma + \lambda}{2}\Big) = \frac{1}{2}\mathrm{Tr}_{L/\mathbb{Q}}(\gamma) + \frac{1}{2}\mathrm{Tr}_{L/\mathbb{Q}}(\lambda) = \mathrm{Tr}_{K/\mathbb{Q}}(\lambda) = 1.$$

Therefore x_2 is a free generator of $\mathfrak{O}_{L,2}$ as an $\mathfrak{A}_{H,2}$-module. □

6.2 Properties of $\mathfrak{A}_{H,p}$ for odd p

Now, for all odd primes p recall from Proposition 5.3.5 that

$$\mathfrak{O}_{L,p} = \Gamma_p = \mathbb{Z}_p\langle 1, \alpha, \beta, \alpha\beta, \gamma, \sigma(\gamma), \tau(\gamma), \sigma\tau(\gamma)\rangle. \tag{6.1}$$

Let x_p denote a candidate generator of $\mathfrak{O}_{L,p}$ as an $\mathfrak{A}_{H,p}$-module. To find local generators at odd primes we need to study the change of basis matrices between bases of $\mathfrak{A}_{H,p} \cdot x_p$ and $\mathfrak{O}_{L,p}$. To simplify this work we first consider a helpful trait of the Artin-Wedderburn decomposition.

Lemma 6.2.1. *For all Hopf algebras, H, of any type that is not cyclic, the generators of $\mathfrak{O}_{L,p}$ over $\mathfrak{A}_{H,p}$ can be written*

$$x_p = 1 + \alpha + \beta + \alpha\beta + f_0 x_p$$

where $f_0 = \big(1 - \lambda(\sigma^2)\big)/2$.

Proof. Recall from chapter 3 that for Hopf algebras H of any type that is not cyclic, the Artin-Wedderburn decomposition has 4 one-dimensional components. Recall every underlying subgroup N contains $\rho(\sigma^2)$ so, in each case, let the elements of the underlying subgroup be 1, η_1, η_2, η_3, $\rho(\sigma^2)$, $\rho(\sigma^2)\eta_1$, $\rho(\sigma^2)\eta_2$, $\rho(\sigma^2)\eta_3$. Then the four one-dimensional components are generated by the four idempotents

$$\begin{aligned}
e_1 &= \frac{1}{8}(1 + \lambda(\sigma^2))\big(1 + \eta_1 + \eta_2 + \eta_3\big),\\
e_2 &= \frac{1}{8}(1 + \lambda(\sigma^2))\big(1 + \eta_1 - \eta_2 - \eta_3\big),\\
e_3 &= \frac{1}{8}(1 + \lambda(\sigma^2))\big(1 - \eta_1 - \eta_2 + \eta_3\big),\\
e_4 &= \frac{1}{8}(1 + \lambda(\sigma^2))\big(1 - \eta_1 + \eta_2 - \eta_3\big).
\end{aligned}$$

Since $p \neq 2$ we have that $e_1, e_2, e_3, e_4 \in \mathfrak{A}_{H,p}$ by Lemma 2.2.32, part 2. In fact, $e_1, e_2, e_3, e_4 \in \mathfrak{O}_{L,p}[N]^G$ since, as can be easily verified, they are all

fixed under the action of G. Note here that these idempotents all have a factor of $(1+\lambda(\sigma^2))/2$ and that this annihilates γ. Whereas, the other four idempotents in each case will have a factor of $(1-\lambda(\sigma^2))/2$ which fixes γ. For any $C \in K$ we have

$$(1+\lambda(\sigma^2)) \cdot C\gamma = [(1+\lambda(\sigma^2)) \cdot C](\gamma - \gamma) = 0$$

and so the basis elements of the one-dimensional components have trivial action on the other components. In fact, up to ordering, it is easily verifiable that

$$\begin{aligned} e_1 x_p &= 1, \\ e_2 x_p &= \alpha, \\ e_3 x_p &= \beta \text{ and} \\ e_4 x_p &= \alpha\beta. \end{aligned}$$

As previously noted, the idempotents corresponding to the components of the Artin-Wedderburn decomposition that are not of dimension one all have the factor $(1-\lambda(\sigma^2))/2$ which clearly acts on any element of K by sending it to 0. As such, when one finds the change of basis matrices, for any labelling order of e_1, e_2, e_3, e_4, we will always find the form

$$\begin{pmatrix} I_4 & \mathbf{0} \\ \mathbf{0} & M \end{pmatrix}$$

where I_4 is the 4x4 identity matrix, $\mathbf{0}$ is the 4x4 zero matrix, and M is an indetermined 4x4 matrix.

Hence, a basis of $\mathfrak{A}_{H,p}$ is of the form

$$\{e_1, e_2, e_3, e_4, f_0E_1, f_0E_2, f_0E_3, f_0E_4\}$$

and due to the action of e_i described above this means a generator of $\mathfrak{A}_{H,p}$ can be written in the form claimed in the lemma. □

Remark 6.2.2. *The cyclic structures can be handled in a similar way since the basis has the same form whereby f_0 appears as a factor in exactly 4 of the elements that together define the 4-dimensional component of the Artin-Wedderburn decomposition, so this component can be considered in isolation as with all of the other types. The difference is that the other four elements with a factor of $(1+\lambda(\sigma^2))/2$ do not act in the uniform manner that they do for the other types so cannot be dealt with as quickly.*

From now on, then, we consider only the matrix M by studying $f_0\mathfrak{O}_{L,p}$ as a module over $f_0\mathfrak{A}_{H,p}$ and so we shall work only with $f_0x_p = c_0\gamma + c_1\sigma(\gamma) + c_2\tau(\gamma) + c_3\sigma\tau(\gamma)$ where f_0 is the identity element corresponding to the component of dimension 4, that is:

$$f_0 := \frac{1}{2}\big(1 - \lambda(\sigma^2)\big).$$

Lemma 6.2.3. *For $u \in \{\alpha, \beta, \alpha\beta\}$ and $\mu \in \{id, \sigma, \tau, \sigma\tau\}$ the value of $u\mu(\gamma)$ can be written in terms of the basis of Γ_p as follows.*

	α	β	$\alpha\beta$
id	$m + k\tau + n\sigma\tau$	$m + n\sigma\tau$	$b + nk\sigma + mk\tau$
σ	$m\sigma - n\tau + k\sigma\tau$	$-m\sigma + n\tau$	$nk - b\sigma - mk\sigma\tau$
τ	$k - n\sigma - m\tau$	$n\sigma + m\tau$	$mk - b\tau + nk\sigma\tau$
$\sigma\tau$	$n + k\sigma - m\sigma\tau$	$n - m\sigma\tau$	$-mk\sigma + nk\tau + b\sigma\tau$

Proof. We give an example of finding such values and then an example of verifying the claimed value, and leave the remaining cases to the reader. Let $u = \alpha, \mu = id$, then

$$\begin{aligned}\alpha\gamma &= c_1\gamma + c_2\sigma(\gamma) + c_3\tau(\gamma) + c_4\sigma\tau(\gamma)\\ &= c_1\gamma + c_2\frac{(\alpha-\beta)(\beta-m)}{nk}\gamma + c_3\frac{\alpha-\beta}{k}\gamma + c_4\frac{\beta-m}{n}\gamma\end{aligned}$$

where $c_1, c_2, c_3, c_4 \in \mathbb{Q}$. Equating coefficients gives the system:

$$\begin{aligned}
\gamma\colon\ & c_1 - \frac{b}{nk}c_2 - \frac{m}{n}c_4 = 0 \\
\alpha\gamma\colon\ & -\frac{m}{nk}c_2 + \frac{1}{k}c_3 = 1 \\
\beta\gamma\colon\ & \frac{m}{nk}c_2 - \frac{1}{k}c_3 + \frac{1}{n}c_4 = 0 \\
\alpha\beta\gamma\colon\ & \frac{1}{nk}c_2 = 0
\end{aligned}$$

Hence, $c_2 = 0$ so $c_3 = k$ and so $c_4 = n$, and finally $c_1 = m$. That is

$$\alpha\gamma = m\gamma + k\tau(\gamma) + n\sigma\tau(\gamma).$$

We now verify the calculation for $u = \alpha, \mu = \sigma$. In this case the lemma claims

$$\alpha\sigma(\gamma) = m\sigma(\gamma) - n\tau(\gamma) + k\sigma\tau(\gamma).$$

This can be verified by comparing the two sides of the equation. The left hand side gives

$$\begin{aligned}
\text{LHS} &= \alpha\sigma(\gamma) \\
&= \alpha\frac{(\alpha-\beta)(\beta-m)}{nk}\gamma \\
&= \frac{-ma - b\alpha + a\beta + m\alpha\beta}{nk}\gamma
\end{aligned}$$

and the right hand side gives

$$\begin{aligned}
\text{RHS} &= m\sigma(\gamma) - n\tau(\gamma) + k\sigma\tau(\gamma) \\
&= \frac{m}{nk}(\alpha-\beta)(\beta-m)\gamma - \frac{n}{k}(\alpha-\beta)\gamma + \frac{k}{n}(\beta-m)\gamma \\
&= \frac{1}{nk}\Big(m(\alpha-\beta)(\beta-m) - n^2(\alpha-\beta) + k^2(\beta-m)\Big)\gamma \\
&= \frac{1}{nk}\Big(m\beta(\alpha-\beta) - m^2(\alpha-\beta) - n^2(\alpha-\beta) + k^2\beta - k^2m\Big)\gamma \\
&= \frac{1}{nk}\Big(-b(\alpha-\beta) + k^2\beta + m\alpha\beta - mb - mk^2\Big)\gamma \\
&= \frac{1}{nk}\Big(-b\alpha + \beta(b+k^2) + m\alpha\beta - m(b+k^2)\Big)\gamma \\
&= \frac{1}{nk}(-ma - b\alpha + a\beta + m\alpha\beta)\gamma,
\end{aligned}$$

as required. The remaining values can be similarly calculated and verified. □

6.3 Noncommutative structures

We can find local generators by constructing a generic generator of $f_0\mathfrak{A}_{H,p}$, for each odd prime p, of the form $d_0f_0 + d_1f_1 + d_2f_2 + d_3f_3$ where $d_i \in \mathbb{Z}_p$ and f_i are the basis elements of $f_0\mathfrak{A}_{H,p}$, the 4-dimensional component of $\mathfrak{A}_{H,p}$, where H is the Hopf algebra in each case. One then finds the change of basis matrix between $\Gamma_p = \mathfrak{O}_{L,p}$ and $\mathfrak{A}_{H,p}$, and its determinant in terms of the d_i. By first setting the values of the d_i to choices of 0 or 1, one may find the primes that divide the resulting determinant. For any prime that does not divide the determinant, this would be a local generator, for the rest we use a different choice of generator, until we have generators for each odd prime.

We first discuss the local generators for structures of type D_4. In these cases we don't even know if local generators exist as Proposition 2.3.12 only applies to structures of abelian type. Nevertheless we have $\mathfrak{O}_{L,p}[N]^G \subseteq \mathfrak{A}_{H,p}$, so we study $f_0\mathfrak{O}_{L,p}$ as a module over $f_0\mathfrak{O}_{L,p}[N]^G$.

Lemma 6.3.1. *If H is of dihedral type then $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$ and we have the following local generators, where $\phi \in \{\lambda, \rho\}$.*

1. *If $H = L[D_{\sigma,\phi}]^G$ then*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2, \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2m, \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma\tau(\gamma) & \text{if } \ p | m. \end{cases}$$

2. If $H = L[D_{\tau,\phi}]^G$ *then*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2, \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2m, \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma\tau(\gamma) & \text{if } \ p | m. \end{cases}$$

3. If $H = L[D_{\sigma\tau,\phi}]^G$ *then*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2, \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2b, \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma(\gamma) & \text{if } \ p | b. \end{cases}$$

Proof. First, the value of x_2 in every case is given from Proposition 6.1.3. Now, we recall the basis elements corresponding to the dimension 4 component of the Artin-Wedderburn decomposition of $L[D_{s,\rho}]^G$ from Lemma 3.3.7 are

$$f_0 = \frac{1}{2}\big(1 - \lambda(\sigma^2)\big),$$

$$f_1 = f_0\rho(s),$$

$$f_2 = \omega f_0 \lambda(s)\rho(t),$$

$$f_3 = \omega f_0 \lambda(s)\rho(st).$$

Note that the basis elements from Lemma 3.3.7 all lie in $\mathfrak{O}_L[N]^G$. Recall equation 2.2 that states the action of $L[N]^G$ on L is defined by

$$\Big(\sum_{n\in N} c_n n\Big) \cdot x = \sum_{n\in N} c_n n^{-1}(1_G)[x].$$

From this we deduce the actions of each of these basis elements on some element of $\mathfrak{O}_L$ of the form $\mu(\gamma)$ where $\mu \in \{id, \sigma, \tau, \sigma\tau\}$ are as follows:

$$\begin{aligned} f_0 \cdot \mu(\gamma) =& \mu(\gamma), \\ f_1 \cdot \mu(\gamma) =& s\mu(\gamma), \\ f_2 \cdot \mu(\gamma) =& -\omega st\mu(\gamma), \\ f_3 \cdot \mu(\gamma) =& \omega t\mu(\gamma). \end{aligned}$$

One may use these equations, with different choices of s for each of the three structures with underlying subgroup of the form $D_{s,\rho}$, to form the change of basis matrices between $f_0\mathfrak{O}_{L,p}$ and $f_0\mathfrak{A}_{H,p}$ for any candidate generator as discussed above, using Lemma 6.2.3 to ease the calculations.

First consider $D_{\sigma,\rho}$ where s is chosen to be σ. We first consider the candidate generator γ. The change of basis matrix is then

$$M_\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -n & -k & 0 & m \\ k & -n & -m & 0 \end{pmatrix}$$

with determinant m^2. Thus γ generates $f_0\mathfrak{O}_{L,p}$ for all primes p that do not divide m. We may note that the determinants that correspond to the candidate generators $\sigma(\gamma)$, $\tau(\gamma)$ and $\sigma\tau(\gamma)$ are also m^2 so we consider candidate generators of the form $\gamma + \mu(\gamma)$.

Consider $\gamma + \sigma\tau(\gamma)$ which gives rise to the change of basis matrix

$$M_{\gamma+\sigma\tau(\gamma)} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ m-n & -k & k & m+n \\ k & m-n & -m-n & k \end{pmatrix}$$

with determinant $4n^2$. Clearly no odd prime that divides m^2 may divide $4n^2$ as the square of such a prime would divide b, contradicting that b is squarefree. Thus we have that $\mathfrak{O}_{L,p}$ is generated as a $\mathfrak{O}_{L,p}[N]^G$-module by the claimed x_p, when H has underlying subgroup $D_{\sigma,\rho}$. Hence, $\mathfrak{A}_{H,p} = \mathfrak{O}_{L,p}[N]^G$.

Similarly, choosing τ for s we get the same candidate generators giving rise to the same determinants of the change of basis matrices.

Choosing $\sigma\tau$ for s, we consider the candidate generators γ and $\gamma + \sigma(\gamma)$ giving rise to change of basis matrices

$$M_{\gamma} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -mk & 0 & b & -nk \\ nk & -b & 0 & -mk \end{pmatrix}$$

and

$$M_{\gamma+\sigma(\gamma)} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ -mk & mk & nk+b & -nk+b \\ nk-b & -nk-b & -mk & -mk \end{pmatrix}$$

respectively, with determinants b^2 and $4k^2n^2$ respectively. Suppose p is an odd prime dividing b^2. If $p|4k^2n^2$ then $p|k$ or $p|n$. If $p|k$ then $p|a$ since $p|b$, contradicting that a and b are coprime. If $p|n$ then $p|m$ and so $p^2|b$, contradicting that b is squarefree. This proves the claims for the structures with underlying subgroup $D_{s,\rho}$.

Finally, we recall from Proposition 3.4.1 that $D_{s,\rho}$ is the underlying subgroup of the opposite structure to that of $D_{s,\lambda}$ for each choice of s. From the proof of Theorem 2.3.9 (see [Tru18, Theorem 1.2]) we have that if $\mathfrak{O}_{L,p} = \mathfrak{O}_L[D_{s,\rho}]^G \cdot x_p$ then $\mathfrak{O}_{L,p} = \mathfrak{A}_{H,p} \cdot x_p$ where $H = L[D_{s,\lambda}]^G$. That is the local generators found for the structures with underlying subgroup $D_{s,\rho}$ are also local generators for the structures with underlying subgroup $D_{s,\lambda}$. □

Remark 6.3.2. *Above, we may perform the same process for the structures with underlying subgroup $D_{s,\lambda}$ as we did with $D_{s,\rho}$, however, this appears not to work. We find that any candidate generator of the form $c_0\gamma + c_1\mu(\gamma)$, where $c_0, c_1 = 0, 1$, gives rise to a determinant that is divisible by b. This implies that the associated order of the Hopf algebra with underlying subgroup $D_{s,\lambda}$ may not be equal to $\mathfrak{O}_L[D_{s,\lambda}]^G$ in general.*

We now find explicit local generators corresponding to the structures of type Q_8.

Lemma 6.3.3. *If H is of quaternion type then we have the local generators*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2, \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \neq 2. \end{cases}$$

Proof. From [Tru18, Theorem 1.1 & Theorem 1.2] we have that x_p generates $\mathfrak{O}_L$ as an $\mathfrak{A}_{\mathbb{Q}[G]}$-module if and only if x_p generates $\mathfrak{O}_L$ as an $\mathfrak{A}_{L[\lambda(G)]^G}$-module. Thus we need only prove the proposition for the structure with Hopf algebra $H = \mathbb{Q}[G]$.

Recall from Proposition 5.3.4 the definition of Γ_p. It is clear from this that for $H = \mathbb{Q}[G]$ we clearly have that $\mathfrak{O}_{L,p}$ is generated as an $\mathfrak{A}_H$-module by the claimed x_p for all odd p. □

We have proven Theorem 6.0.1.

6.4 Commutative structures

Recall that, by Proposition 2.3.12, $\mathfrak{A}_{H,p} = \mathfrak{O}_{L,p}[N]^G$ and $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_{H,p}$. In this section we find explicit local generators corresponding to the commutative structures. We will present local generators as in the previous section, and then verify the choice.

Lemma 6.4.1. *If H has elementary abelian type then we have the following local generators.*

1. *If $H = L[E_{\sigma,\tau}]^G$ then*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if} \quad p = 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if} \quad p | bn, p \neq 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma(\gamma) & \text{if} \quad p \nmid 2bn. \end{cases}$$

2. *If $H = L[E_{\tau,\sigma}]^G$ then*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if} \quad p = 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if} \quad p \nmid 2bm \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \tau(\gamma) & \text{if} \quad p | bm. \end{cases}$$

Proof. Let $H = L[E_{\sigma,\tau}]^G$. Then by Proposition 2.3.12 we have $\mathfrak{A}_H = \mathfrak{O}_L[E_{\sigma,\tau}]^G$ and by Proposition 6.1.3 we have that $x_2 = \frac{\gamma+\lambda}{2}$. We find a basis for the associated order at odd primes using the same theorem of Boltje and Bley as in Chapter 3; one may recall the orbit structure of the dual group $\widehat{E_{\sigma,\tau}}$ from Lemma 3.3.1 and apply Lemma 2.2.32 to find a basis of $f_0\mathfrak{A}_{H,p}$ is

$$\begin{aligned} f_0 :&= \frac{1}{2}\big(1 - \lambda(\sigma^2)\big), \\ f_1 &= \alpha f_0 \lambda(\sigma)\rho(\tau), \\ f_2 &= \beta f_0 \lambda(\tau)\rho(\sigma\tau), \\ f_3 &= \alpha\beta f_0 \lambda(\sigma\tau)\rho(\sigma). \end{aligned}$$

Note also that each of these lies in $\mathfrak{O}_{L,p}[N]^G$. We now consider the element $f_0 x_p = \gamma$ and find for which primes p this is a local generator for $f_0\mathfrak{O}_L$ over $f_0\mathfrak{A}_H$. We have

$$f_0 \cdot \gamma = \frac{1}{2}\big(1 - \lambda(\sigma^2)\big)\gamma = \frac{1}{2}\big(\gamma - (-\gamma)\big) = \gamma,$$

$$\begin{aligned} f_1 \cdot \gamma =& \frac{\alpha}{2}\big(\lambda(\sigma)\rho(\tau) - \lambda(\sigma^3)\rho(\tau)\big)\gamma \\ =& \frac{\alpha}{2}\big(\sigma\tau^{-1}(\gamma) - (-\sigma\tau^{-1}(\gamma))\big) \\ =& -\alpha\sigma\tau(\gamma) \\ =& n\gamma + k\sigma(\gamma) - m\sigma\tau(\gamma), \end{aligned}$$

$$\begin{aligned} f_2 \cdot \gamma =& \frac{\beta}{2} f_0\big(\lambda(\tau)\rho(\sigma\tau)\big) \cdot \gamma \\ =& \beta\tau^2\sigma(\gamma) \\ =& -\beta\sigma(\gamma) \\ =& m\sigma(\gamma) - n\tau(\gamma), \end{aligned}$$

$$\begin{aligned} f_3 \cdot \gamma =& \frac{\alpha\beta}{2} f_0\big(\lambda(\sigma\tau)\rho(\sigma)\big) \cdot \gamma \\ =& \alpha\beta\sigma\tau\sigma^{-1}(\gamma) \\ =& -\alpha\beta\tau(\gamma) \\ =& -mk\gamma + b\tau(\gamma) - nk\sigma\tau(\gamma). \end{aligned}$$

Hence the change of basis matrix between $f_0\mathfrak{O}_{L,p}$ and $\mathfrak{A}_{H,p}$ is

$$M_\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ n & k & 0 & -m \\ 0 & m & -n & 0 \\ -mk & 0 & b & -nk \end{pmatrix}$$

with determinant $D_\gamma = bm^2 - k^2n^2$. Therefore γ is a generator of $f_0\mathfrak{O}_{L,p}$ over $f_0\mathfrak{A}_{H,p}$ for $p \nmid D_\gamma$. For prime numbers dividing D_γ we require a different generator. First of all, the change of basis matrix obtained from generators $\sigma(\gamma)$, $\tau(\gamma)$ and $\sigma\tau(\gamma)$ all have the same determinant as above. We may consider the generator $f_0x_p = \gamma + \sigma(\gamma)$. This gives a change of basis matrix with determinant $D_{\gamma+\sigma(\gamma)} = -4bn^2$, found as above.

Let p be an odd prime dividing $D_\gamma = bm^2 - k^2n^2$. Now if $p|4bn^2$ then $p|b$ or $p|n$. If $p|b$ and since $p|(k^2n^2 - bm^2)$ then $p|n$ or $p|k$. If $p|n$ then since $p|b$ we also have $p|m$ so $p^2|b$ which contradicts that b must be squarefree. Alternatively, if $p|k$ then, since $p|b$, we also have $p|a$ which contradicts that a and b are coprime. So $p \nmid b$. Now if $p|n$ then $p|m$ or $p|b$. Since we know $p \nmid b$ we must have $p|m$, but then $p|m$ and $p|n$ which would require $p|b$, a contradiction. Thus if $p|D_\gamma$ then $p \nmid D_{\gamma+\sigma(\gamma)}$. This proves part (1) of the lemma.

We perform the same analysis for the other structure of elementary abelian type, $H = L[E_{\tau,\sigma}]^G$. Following the same working as above, with σ and τ in-

terchanged, we find a basis for $f_0\mathfrak{O}_{L,p}$ over $f_0\mathfrak{A}_{H,p}$ is

$$\begin{aligned} f_0 :=& \frac{1}{2}\big(1-\lambda(\sigma^2)\big),\\ f_1 =& \beta f_0\lambda(\tau)\rho(\sigma),\\ f_2 =& \alpha f_0\lambda(\sigma)\rho(\sigma\tau),\\ f_3 =& \alpha\beta f_0\lambda(\sigma\tau)\rho(\tau). \end{aligned}$$

Now, as above we find the action of these basis elements on the candidate generator element γ and construct the change of basis matrix between these and Γ_p. This matrix has determinant $D_\gamma = bm^2$. Since there exist odd primes that divide D_γ we now consider alternative candidate generators. As before, the determinants of the change of basis matrices corresponding to $\sigma(\gamma), \tau(\gamma)$ and $\sigma\tau(\gamma)$ are all also bm^2. Unlike in the previous case $\gamma + \sigma(\gamma)$ does not work as an alternative since the corresponding determinant is $4k^2m^2$, so any prime dividing m would divide both determinants.

As such we consider the candidate generator element $\gamma+\tau(\gamma)$. The change of basis matrix for this element has determinant $D_{\gamma+\tau(\gamma)} = 4k^2m^2 - 4bn^2$. Now suppose p is an odd prime dividing D_γ. Then $p|b$ or $p|m$. If $p|b$ and $p|(k^2m^2-bn^2)$ then $p|k$ or $p|m$. If $p|m$ then $p|n$ since $p|b$ so $p^2|b$ contradicting that b is squarefree. If $p|k$ then $p|a$ since $p|b$ but this contradicts that a and b are coprime. So $p \nmid b$. If, instead, $p|m$ and $p|(k^2m^2 - bn^2)$ then $p|b$ or $p|n$, in either case $p|b$ which we know is not possible. Thus no odd prime that divides D_γ may also divide $D_{\gamma+\tau(\gamma)}$. This completes the proof of part (2). □

We do the same for the structures of type $C_4 \times C_2$.

Lemma 6.4.2. *If H is of $C_4 \times C_2$ type then we have the following local generators.*

1. If $H = L[A_{\sigma,\tau}]^G$ *then*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p|b, p \nmid 2(k^2 + m^2) \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma(\gamma) & \text{if } \ p \nmid 2b \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma\tau(\gamma) & \text{if } \ p|b, p|(k^2 + m^2), p \neq 2. \end{cases}$$

2. If $H = L[A_{\sigma,\sigma\tau}]^G$ *then*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2b \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma(\gamma) & \text{if } \ p|b, p \nmid 2(k^2 + m^2) \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \tau(\gamma) & \text{if } \ p|b, p|(k^2 + m^2), p \neq 2. \end{cases}$$

3. If $H = L[A_{\tau,\sigma}]^G$ *then*

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2m \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \tau(\gamma) & \text{if } \ p|m. \end{cases}$$

4. If $H = L[A_{\tau,\sigma\tau}]^G$ then

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2b \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \tau(\gamma) & \text{if } \ p|b, p \neq 2. \end{cases}$$

5. If $H = L[A_{\sigma\tau,\sigma}]^G$ then

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2(k^2n^2 + b^2) \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \tau(\gamma) & \text{if } \ p|(k^2n^2 + b^2), p \nmid 2bk^2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma\tau(\gamma) & \text{if } \ p|(k^2n^2 + b^2), p|bk^2, p \neq 2. \end{cases}$$

6. If $H = L[A_{\sigma\tau,\tau}]^G$ then

$$x_p = \begin{cases} \frac{1}{2}\big(\gamma + \lambda\big) & \text{if } \ p = 2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2(k^2m^2 + b^2) \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma(\gamma) & \text{if } \ p|(k^2m^2 + b^2), p \nmid 2bk^2 \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma\tau(\gamma) & \text{if } \ p|(k^2m^2 + b^2), p|bk^2, p \neq 2. \end{cases}$$

Proof. We first recall a basis for $f_0\mathfrak{A}_{H,p}$ for all odd primes p where $H = L[A_{s,t}]^G$ from Lemma 3.3.2. Our basis of $f_0\mathfrak{A}_{H,p}$, then, is

$$f_0 = \frac{1}{2}\big(1 - \lambda(\sigma^2)\big),$$

$$f_1 = \omega f_0 \lambda(s)\rho(t),$$

$$f_2 = f_0\rho(t),$$

$$f_3 = \omega f_0\lambda(s).$$

The actions of each of these basis elements on some element of $\mathfrak{O}_L$ of the form $\mu(\gamma)$ where $\mu \in \{id, \sigma, \tau, \sigma\tau\}$ are as follows.

$$\begin{aligned} f_0 \cdot \mu(\gamma) &= \mu(\gamma), \\ f_1 \cdot \mu(\gamma) &= -\omega st\mu(\gamma), \\ f_2 \cdot \mu(\gamma) &= -t\omega(\gamma), \\ f_3 \cdot \mu(\gamma) &= \omega s\mu(\gamma). \end{aligned}$$

One may use these general equations with different choices of s and t dependent on the structure in question to form the change of basis matrices for any candidate generator of the form $\gamma + \mu(\gamma)$ using Lemma 6.2.3.

We must consider each structure from here on separately due to the nature of the action of the basis elements. First, for part (1) consider $H = L[A_{\sigma,\tau}]^G$. In the same way as above we first consider the candidate generator γ. The determinant of the corresponding change of basis matrix is $D_\gamma = k^2 + m^2$. Similarly to above we find the determinants for the change of basis matrix arising from the generators $\gamma + \sigma(\gamma)$ and $\gamma + \sigma\tau(\gamma)$ to be $4b$ and $4k^2 + 4n^2$ respectively.

Now, suppose some odd prime, p, exists that divides all of these determinants. Then p divides $(k^2+m^2)+(k^2+n^2)-b = 2k^2$. This implies that $p|k^2$ as p is odd and so $p|a$ since $p|b$. This contradicts that a and b are coprime so no such prime exists.

Similarly, for part (2) and the structure corresponding to the Hopf algebra $H = L[A_{\sigma,\sigma\tau}]^G$ we find the change of basis matrix determinants arising from the candidate generators γ, $\gamma + \sigma(\gamma)$ and $\gamma + \tau(\gamma)$. These are, respectively, b, $4k^2 + 4m^2$ and $4k^2 + 4n^2$. Following the exact same argument as above, an odd prime, p, dividing all of these determinants must also divide k^2 and

so would divide a since $p|b$. This contradicts that a and b are coprime and so no such prime exists.

For part (3) and the Hopf algebra $L[A_{\tau,\sigma}]^G$ we find the determinants of the change of basis matrices arising from the candidate generators γ and $\gamma + \tau(\gamma)$ to be m^2 and $4b$ respectively. Any odd prime dividing m^2 and $4b$ must also divide n so that $p^2|b$, contradicting that b is squarefree.

For part (4) and the Hopf algebra $L[A_{\tau,\sigma\tau}]^G$ we again find the determinants of the change of basis matrices arising from the candidate generators γ and $\gamma + \tau(\gamma)$. In this case these are b and $4m^2$ respectively. Any odd prime dividing $4m^2$ and b must also divide n so that $p^2|b$, as before, contradicting that b is squarefree.

For part (5) and the Hopf algebra $L[A_{\sigma\tau,\sigma}]^G$ we find the determinants of the change of basis matrices arising from the candidate generators γ and $\gamma + \tau(\gamma)$ and $\gamma + \sigma\tau(\gamma)$ to be $k^2n^2 + b^2$, $4k^2m^2 + 4k^2n^2$ and $4k^2m^2 + 4b^2$ respectively. Any odd prime dividing all of these determinants must also divide $(k^2n^2+b^2)-(k^2m^2+b^2) = k^2n^2-k^2m^2$ so must divide $(k^2n^2-k^2m^2)+(k^2n^2+k^2m^2) = 2k^2n^2$. Since p is odd this gives that $p|kn$. Similarly such a prime would have to divide b and km. No such prime can divide all of these as any prime dividing b cannot divide k else a and b would not be coprime, and cannot divide m or n else b would not be squarefree.

Finally, for part (6) and the Hopf algebra $L[A_{\sigma\tau,\tau}]^G$ we find the determinants of the change of basis matrices arising from the candidate generators γ and $\gamma + \sigma(\gamma)$ and $\gamma + \sigma\tau(\gamma)$ to be $k^2m^2 + b^2$, $4k^2m^2 + 4k^2n^2$ and $4k^2n^2 + 4b^2$ respectively. Following the same argument as in the previous case we find that no odd prime may divide all of these determinants either. □

Chapter 7

Global freeness of Hopf-Galois structures of dihedral type

In this chapter we focus on the structures of dihedral type. It is sufficient to study the structures with underlying subgroup $D_{s,\rho}$ due to Corollary 2.3.10 and Proposition 3.4.1. Let $L/\mathbb{Q}$ be a tame Fujisaki extension, let $H = L[D_{s,\rho}]^G$ for some $s \in \{\sigma, \tau, \sigma\tau\}$, let $\omega \in \{\alpha, \beta, \alpha\beta\}$ such that $s(\omega) = \omega$ and $t(\omega) = -\omega$ for any $t \in \{\sigma, \tau, \sigma\tau\}$ where $s \neq t$. Let $\mathfrak{A}_H$ be the associated order of $\mathfrak{O}_L$ in H. Start by recalling from Lemma 3.3.7 that the Artin-Wedderburn decomposition of H is $\mathbb{Q}^4 \times (-1, \omega^2)_{\mathbb{Q}}$, and so the Artin-Wedderburn decomposition of the centre of H, C, is $\mathbb{Q}^5$.

7.1 Class group conditions

In this section we find that $\mathfrak{O}_L$ having trivial class in the locally free class group is sufficient for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$. We also derive useful conditions that help us determine the class of $\mathfrak{O}_L$. First, we know that if $\mathfrak{O}_L$ has trivial class it is stably free as an $\mathfrak{A}_H$-lattice by Remark 2.4.4.

Lemma 7.1.1. *Stably free $\mathfrak{A}_H$-lattices are free.*

Proof. By Proposition 2.4.2 it is sufficient to show that H satisfies the Eichler condition relative to $\mathbb{Z}$. That is no Wedderburn component of H is a totally definite quaternion algebra over $\mathbb{Q}$. The first four components clearly satisfy this so we only need to consider the component $(-1,\omega^2)_{\mathbb{Q}}$. Since $\omega^2 > 0$ we clearly have that ω^2 is a square in $\mathbb{R}$ and so by part 1 of Proposition 2.2.38 we have $(-1,\omega^2)_{\mathbb{R}} \cong M_2(\mathbb{R})$. That is $(-1,\omega^2)_{\mathbb{Q}}$ does not remain a division ring when we extend scalars to $\mathbb{R}$ and so H does satisfy the Eichler condition relative to $\mathbb{Z}$. □

An obvious and useful corollary is the following.

Corollary 7.1.2. *$\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module if and only if it has trivial class in* $\mathrm{Cl}(\mathfrak{A}_H)$.

The reduced norm map $\mathrm{nr} : H^\times \to C^\times$ can be better understood with the known Artin-Wedderburn decomposition of H. We may note that any $h \in H$ corresponds to a 5-tuple in the decomposition, so let $h \in H$ correspond to $(c_0, c_1, c_2, c_3, z) \in \mathbb{Q}^4 \times (-1,\omega^2)_{\mathbb{Q}}$. Then the reduced norm of h corresponds to a 5-tuple that uses the norm of the quaternion algebra. In this case the norm N on $(-1,\omega^2)_{\mathbb{Q}}$ is defined by

$$N(z_0 + z_1u + z_2v + z_3uv) = z_0^2 + z_1^2 - \omega^2 z_2^2 - \omega^2 z_3^2$$

where $u^2 = -1, v^2 = \omega^2$. Then, explicitly, the reduced norm of h corresponds to $(c_0, c_1, c_2, c_3, N(z))$.

Lemma 7.1.3. *In this case the reduced norm map* $\mathrm{nr} : H^\times \to C^\times$ *is surjective.*

Proof. We study the reduced norm component by component as on the first four components the reduced norm is trivial. It therefore remains only to show that $N : (-1,\omega^2)_{\mathbb{Q}}^\times \to \mathbb{Q}^\times$ is surjective, since $\mathbb{Q}^\times$ is clearly the centre of $(-1,\omega^2)_{\mathbb{Q}}^\times$. First we view N as a quadratic form. By the Hasse-Minkowski

Theorem (see [Ser12, Part 1, Chapter 4, Theorem 8 and Corollary 1]), given $x \in \mathbb{Q}^\times$ the equation

$$z_0^2 + z_1^2 - \omega^2 z_2^2 - \omega^2 z_3^2 = x$$

has a solution in $\mathbb{Q}$ if and only if it has a solution in $\mathbb{R}$ and a solution in $\mathbb{Q}_p$ for each prime number p. For all x the equation clearly has a solution in $\mathbb{R}$ as one can trivially choose $z_0 = \sqrt{x}, z_1 = z_2 = z_3 = 0$ if $x \geq 0$ or $z_2 = \sqrt{-x/\omega^2}, z_0 = z_1 = z_3 = 0$ if $x < 0$. By [CR81, Theorem 7.45], this equation also has a solution in each $\mathbb{Q}_p$. □

Remark 7.1.4. *This lemma also means that the group C^+ is equal to $C^\times$ so we have*

$$\mathrm{Cl}(\mathfrak{A}_H) \cong \frac{\mathbb{J}(C)}{C^\times \prod_p \mathrm{nr}(\mathfrak{A}_{H,p}^\times)}. \tag{7.1}$$

We now present results that shed light on what it is that makes an element of $\mathfrak{A}_{H,p}$ a unit.

Lemma 7.1.5. *If p is odd then*

$$\mathfrak{A}_{H,p} \cong \mathbb{Z}_p^4 \times \mathfrak{B}_p$$

where $\mathfrak{B}_p$ is the following $\mathbb{Z}_p$-order in $(-1, \omega^2)_{\mathbb{Q}_p}$:

$$\mathfrak{B}_p = f_0 \mathfrak{A}_{H,p} = \frac{1 - \rho(s^2)}{2} \mathfrak{A}_{H,p}.$$

Proof. This follows immediately from the basis elements found in Lemma 3.3.7. □

Corollary 7.1.6. *If p is odd then $\mathfrak{A}_{H,p}^\times \cong (\mathbb{Z}_p^\times)^4 \times \mathfrak{B}_p^\times$.*

Lemma 7.1.7. *If $z \in \mathfrak{B}_p$ is an element whose reduced norm is a unit in $\mathbb{Z}_p$ then $z \in \mathfrak{B}_p^\times$.*

Proof. Let $z \in \mathfrak{B}_p$. Then, by Definition 2.2.42, $N(z) = z\bar{z}$ and thus $z(\frac{\bar{z}}{N(z)}) = 1$. Hence z is a unit with inverse $\bar{z}/N(z)$. □

Corollary 7.1.8. *An element $h \in \mathfrak{A}_{H,p}$ is a unit of $\mathfrak{A}_{H,p}$ if it corresponds to an element $(c_0, c_1, c_2, c_3, z) \in \mathbb{Z}_p^4 \times \mathfrak{B}_p^4$ where c_0, c_1, c_2, c_3 and $N(z)$ are units of $\mathbb{Z}_p$.*

We have a similar result for the remaining case where $p = 2$.

Lemma 7.1.9. *An element $z \in \mathfrak{A}_{H,2}$ is a unit if and only if $\varepsilon(z) \in \mathbb{Z}_2^\times$.*

Proof. Recall from Proposition 6.1.2 that $\mathfrak{A}_{H,2}$ is a local ring. By definition it therefore has a unique maximal left ideal $\mathcal{J}$ for which $\mathfrak{A}_{H,2}^\times = \mathfrak{A}_{H,2} - \mathcal{J}$. Therefore $z \in \mathfrak{A}_{H,2}$ is a unit if and only if it does not lie in $\mathcal{J}$. It is therefore sufficient to prove that $\mathcal{J} = 2\mathfrak{A}_{H,2} + \ker(\varepsilon)$ as an element $z \in \mathfrak{A}_{H,2}$ would have counit in $\mathbb{Z}_2^\times$ if and only if $z \notin \mathcal{J}$.

First, $2\mathfrak{A}_{H,2} + \ker(\varepsilon)$ is clearly a left ideal of $\mathfrak{A}_{H,2}$. Now there is a natural surjective homomorphism $\mathfrak{A}_{H,2} \to \mathfrak{A}_{H,2}/2\mathfrak{A}_{H,2}$, and a further surjective homomorphism $\bar{\varepsilon} : \mathfrak{A}_{H,2}/2\mathfrak{A}_{H,2} \to \mathbb{Z}_2/2\mathbb{Z}_2$ defined by $\bar{\varepsilon}(z + 2\mathfrak{A}_{H,2}) = \varepsilon(z) + 2\mathbb{Z}_2$. The composition of these homomorphisms has kernel $2\mathfrak{A}_{H,2} + \ker(\varepsilon)$ and image $\mathbb{Z}_2/2\mathbb{Z}_2$. Since the image is a field the kernel of the map must be maximal and hence equal to $\mathcal{J}$, the unique maximal left ideal of $\mathfrak{A}_{H,2}$. □

In fact, we can find a set of congruences that determine when some $z \in H_2$ lies in $\mathfrak{A}_{H,2}$. Here we recall the basis of $H = L[D_{s,\rho}]^G$ found in Lemma 3.3.7: $\{e_0, e_1, e_2, e_3, f_0, f_1, f_2, f_3\}$.

Lemma 7.1.10. *Let $z \in H_2$ have the form $z = c_0e_0 + c_1e_1 + c_2e_2 + c_3e_3 + d_0f_0 + d_1f_1$ where $c_i, d_i \in \mathbb{Q}$. Then z is an element of $\mathfrak{A}_{H,2}$ if and only if the following congruences have a solution:*

$$c_0 + c_1 + c_2 + c_3 + 4d_0 \equiv 0 \pmod 8, \tag{7.2}$$

$$c_0 - c_1 + c_2 - c_3 + 4d_1 \equiv 0 \pmod 8, \tag{7.3}$$

$$c_0 + c_1 - c_2 - c_3 \equiv 0 \pmod 8, \tag{7.4}$$

$$c_0 - c_1 - c_2 + c_3 \equiv 0 \pmod 8, \tag{7.5}$$

Proof. Write z in terms of a $\mathbb{Z}$-basis of $\mathfrak{A}_{H,2}$. Such a basis will not necessarily respect the Artin-Wedderburn decomposition but is easier to test for integrality. The basis we use is derived using Lemma 2.2.30 and is as follows:

$$1, \quad \rho(\sigma\tau), \quad \rho(\sigma^2), \quad \rho(\tau\sigma),$$
$$\lambda(\sigma\tau)\rho(\sigma) + \lambda(\tau\sigma)\rho(\sigma), \quad \frac{1+\alpha\beta}{2}\lambda(\sigma\tau)\rho(\sigma) + \frac{1-\alpha\beta}{2}\lambda(\tau\sigma)\rho(\sigma),$$
$$\lambda(\sigma\tau)\rho(\tau) + \lambda(\tau\sigma)\rho(\tau), \text{ and } \frac{1+\alpha\beta}{2}\lambda(\sigma\tau)\rho(\tau) + \frac{1-\alpha\beta}{2}\lambda(\tau\sigma)\rho(\tau).$$

By rewriting z in terms of this basis and requiring that each resultant coefficient is integral at 2 we find that $z_2 \in \mathfrak{A}_{H,2}^{\times}$ if and only if

$$c_0 + c_1 + c_2 + c_3 + 4d_0 \equiv 0 \pmod 8,$$
$$c_0 - c_1 + c_2 - c_3 + 4d_1 \equiv 0 \pmod 8,$$
$$c_0 + c_1 - c_2 - c_3 \equiv 0 \pmod 8,$$
$$c_0 - c_1 - c_2 + c_3 \equiv 0 \pmod 8,$$
$$c_0 + c_1 + c_2 + c_3 - 4d_0 \equiv 0 \pmod 8,$$
$$c_0 - c_1 + c_2 - c_3 - 4d_1 \equiv 0 \pmod 8,$$
$$c_0 \in \mathbb{Z}_2^{\times}.$$

Finally, since $-4d_i \equiv 4d_i \pmod 8$ for either $i = 0, 1$ we have derived the claimed congruences. □

7.2 Constructing idèles corresponding to $\mathfrak{O}_L$

Let $x = 1 + \alpha + \beta + \alpha\beta + \gamma$, then x is a free generator of L as an H-module. Recall from the previous chapter that a free generator of $\mathfrak{O}_{L,p}$ as an $\mathfrak{A}_{H,p}$-module, for each p, is denoted x_p. We define $h_p \in H_p$ by $h_p \cdot x = x_p$. Then the class of $\mathfrak{O}_L$ in $\mathrm{Cl}(\mathfrak{A}_H)$ corresponds to the sequence (h_p). Thus the class of $\mathfrak{O}_L$ is trivial if and only if there exists $c \in C^{\times}$ such that, for each prime p, $\mathrm{nr}(h_p) = cu_p$ for some $u_p \in \mathrm{nr}(\mathfrak{A}_{H,p}^{\times})$ by Equation (7.1).

7.2.1 Global freeness over the associated order in $L[D_{\sigma\tau,\rho}]^G$

Theorem 7.2.1. *Let $H = L[D_{\sigma\tau,\rho}]^G$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ if and only if $n \equiv 0 \pmod 4$. This, in turn, is equivalent to $\mathfrak{O}_L$ being free over the classical associated order $\mathbb{Z}[G]$ of $\mathbb{Q}[G]$ by Corollary 5.4.3.*

We will prove this theorem in stages. We start by finding the values of $\mathrm{nr}(h_p)$ before investigating whether these values have the form we want.

Lemma 7.2.2. *Let $H = L[D_{\sigma\tau,\rho}]^G$ and let h_p be defined as above. Then we have*

$$\mathrm{nr}(h_p) = \begin{cases} \frac{1}{8}\Big(e_0 + (-1)^{\frac{n}{2}} m e_1 + (-1)^{\frac{k}{2}} e_2 + (-1)^{\frac{k+n}{2}} mb e_3 + 2f_0\Big) & \text{if } \ p = 2, \\ e_0 + e_1 + e_2 + e_3 + \frac{2kn}{b} f_0 & \text{if } \ p \mid b \\ 1 & \text{if } \ p \nmid 2b. \end{cases}$$

Proof. Recall Lemma 6.3.1 which gives local generators:

$$x_p = \begin{cases} \frac{1}{8}\big(1 + (-1)^{\frac{k+n}{2}} mb\alpha + (-1)^{\frac{n}{2}} m\beta + (-1)^{\frac{k}{2}} \alpha\beta + 4\gamma\big) & \text{if } \ p = 2, \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2b, \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma(\gamma) & \text{if } \ p \mid b. \end{cases}$$

Furthermore, the proof of Lemma 3.3.7 gives a $\mathbb{Q}$-basis of $L[D_{\sigma\tau,\rho}]^G$. Letting $\eta_1 = \rho(\sigma\tau)$ and $\eta_2 = \lambda(\sigma\tau)\rho(\sigma)$ we recall the basis to be

$$\begin{aligned} e_0 &= \frac{1}{8}\big(1 + \eta_1 + \eta_1^2 + \eta_1^3 + \eta_2 + \eta_1\eta_2 + \eta_1^2\eta_2 + \eta_1^3\eta_2\big), \\ e_1 &= \frac{1}{8}\big(1 - \eta_1 + \eta_1^2 - \eta_1^3 + \eta_2 - \eta_1\eta_2 + \eta_1^2\eta_2 - \eta_1^3\eta_2\big), \\ e_2 &= \frac{1}{8}\big(1 + \eta_1 + \eta_1^2 + \eta_1^3 - \eta_2 - \eta_1\eta_2 - \eta_1^2\eta_2 - \eta_1^3\eta_2\big), \\ e_3 &= \frac{1}{8}\big(1 - \eta_1 + \eta_1^2 - \eta_1^3 - \eta_2 + \eta_1\eta_2 - \eta_1^2\eta_2 + \eta_1^3\eta_2\big), \end{aligned}$$

$$f_0 = \frac{1}{2}(1-\rho(\sigma^2)), \quad f_1 = f_0\rho(\sigma\tau),$$
$$f_2 = \alpha\beta f_0\lambda(\sigma\tau)\rho(\sigma), \text{ and } f_3 = \alpha\beta f_0\lambda(\sigma\tau)\rho(\tau).$$

We can easily describe the action of some of these basis elements:

$$e_0: \quad 1\mapsto 1, \quad \alpha\mapsto 0, \quad \beta\mapsto 0, \quad \alpha\beta\mapsto 0,$$
$$e_1: \quad 1\mapsto 0, \quad \alpha\mapsto 0, \quad \beta\mapsto \beta, \quad \alpha\beta\mapsto 0,$$
$$e_2: \quad 1\mapsto 0, \quad \alpha\mapsto 0, \quad \beta\mapsto 0, \quad \alpha\beta\mapsto \alpha\beta,$$
$$e_3: \quad 1\mapsto 0, \quad \alpha\mapsto \alpha, \quad \beta\mapsto 0, \quad \alpha\beta\mapsto 0,$$

and $e_i : \gamma \mapsto 0$ for all $i = 0, 1, 2, 3$. We further note that $f_0 : \omega \mapsto 0$ for all $\omega \in \{1, \alpha, \beta, \alpha\beta\}$ and $f_0 : \gamma \mapsto \gamma$. So, it is clear that

$$h_2 = \frac{1}{8}\left[e_0 + (-1)^{\frac{n}{2}}me_1 + (-1)^{\frac{k}{2}}e_2 + (-1)^{\frac{k+n}{2}}mbe_3 + 4f_0\right]. \tag{7.6}$$

Now, for primes p such that $p \nmid 2b$ we clearly have $h_p = 1$ so now consider primes p for which $p|b$. In this case it is clear what the coefficients of the e_i must be for each $i \in \{0, 1, 2, 3\}$ by the above actions so we mostly consider only f_0h_p from now on. Write $f_0h_p = c_0f_0+c_1f_1+c_2f_2+c_3f_3$ for some $c_i \in \mathbb{Q}$. Then we require $f_0h_p \cdot x = f_0x_p$ which is equivalent to $f_0h_p \cdot \gamma = \gamma + \sigma(\gamma)$. Equating coefficients of $\gamma, \sigma(\gamma), \tau(\gamma)$ and $\sigma\tau(\gamma)$ gives the following system of equations:

$$c_0 - mkc_2 + nkc_3 = 1,$$
$$-bc_3 = 1,$$
$$bc_2 = 0,$$
$$c_1 - nkc_2 - mkc_3 = 0.$$

The solution to this system is easily found to be $c_0 = (b + kn)/b, c_1 = -km/b, c_2 = 0$ and $c_3 = -1/b$. Therefore we find the reduced norm of h_p for

all primes for which $p|b$ by finding

$$\begin{aligned}\mathrm{nr}(f_0h_p) &= \frac{1}{b^2}\Big((b+kn)^2+(km)^2-ab\Big)f_0\\ &= \frac{1}{b^2}\Big(b^2+2bkn+k^2n^2+k^2m^2-ab\Big)f_0\\ &= \frac{1}{b^2}\Big(2bkn+b(b+k^2)-ab\Big)f_0\\ &= \frac{1}{b^2}\Big(2bkn\Big)f_0\\ &= \frac{2kn}{b}f_0.\end{aligned}$$

So we have

$$\mathrm{nr}(h_p) = \begin{cases} \frac{1}{8}\Big(e_0+(-1)^{\frac{n}{2}}me_1+(-1)^{\frac{k}{2}}e_2+(-1)^{\frac{k+n}{2}}mbe_3+2f_0\Big) & \text{if} \quad p=2,\\ e_0+e_1+e_2+e_3+\frac{2kn}{b}f_0 & \text{if} \quad p|b\\ 1 & \text{if} \quad p\nmid 2b. \end{cases}$$

□

Lemma 7.2.3. *Let $H = L[D_{\sigma\tau,\rho}]^G$. If $n \equiv 0 \pmod 4$ then $\mathfrak{O}_L$ is free (of rank one) over $\mathfrak{A}_H$.*

Proof. We need to show $\mathrm{nr}(h_p)$ found in Lemma 7.2.2 has the form cu_p where $c \in C^\times$ and $u_p \in \mathrm{nr}(\mathfrak{A}_{H,p}^\times)$ for all primes p by Equation (7.1). We start with an informed choice of c that we hope will simplify the next step for both the case $p=2$ and the case $p|b$. Let

$$c = \frac{1}{8}\Big(e_0+(-1)^{\frac{n}{2}}e_1+(-1)^{\frac{k}{2}}e_2+(-1)^{\frac{k+n}{2}}e_3\Big)+\frac{1}{4b}f_0.$$

First note that for $p\nmid 2b$ we have $u_p = c^{-1}$ which is certainly of the form we need. Consider the case $p|b$. We have

$$u_p = 8\Big(e_0+(-1)^{\frac{n}{2}}e_1+(-1)^{\frac{k}{2}}e_2+(-1)^{\frac{k+n}{2}}e_3+knf_0\Big)$$

and need to find some $z_p \in \mathfrak{A}_{H,p}$ such that $\mathrm{nr}(z_p) = u_p$. Clearly we need

$$z_p = 8\Big(e_0 + (-1)^{\frac{n}{2}}e_1 + (-1)^{\frac{k}{2}}e_2 + (-1)^{\frac{k+n}{2}}e_3\Big) + d_0f_0 + d_1f_1 + d_2f_2 + d_3f_3$$

for some $d_i \in \mathbb{Q}$ for each $i \in \{0,1,2,3\}$. Now, $\mathrm{nr}(f_0z_p) = (d_0^2 + d_1^2 - ab(d_2^2 + d_3^2))f_0$. We have that since $L/\mathbb{Q}$ is tame, $\mathbb{Q}(\beta)/\mathbb{Q}$ is also tame and so $b \equiv 1 \pmod 4$. Thus any prime dividing b that is -1 modulo 4 must occur in the prime decomposition of b to an even exponent. However b is squarefree and so any prime dividing b must be 1 modulo 4. As such, there exists $i \in \mathbb{Z}_p$ such that $i^2 = -1$ for all such p. Therefore we may choose $d_0 = n + 2k$, $d_1 = i(n - 2k)$ and $d_2 = d_3 = 0$. Then

$$\mathrm{nr}(f_0z_p) = (n+2k)^2 - (n-2k)^2 = n^2 + 4kn + 4k^2 - n^2 + 4kn - 4k^2 = 8kn$$

as required. The resulting z is clearly an element of $\mathfrak{A}_{H,p}$ and since the reduced norm $\mathrm{nr}(h_p)$ is a unit, by Corollary 7.1.8, we have $z_p \in \mathfrak{A}_{H,p}^{\times}$. That is h_p has the required form for all odd primes.

Now consider $p = 2$. Since we have chosen

$$c = \frac{1}{8}\Big(e_0 + (-1)^{\frac{n}{2}}e_1 + (-1)^{\frac{k}{2}}e_2 + (-1)^{\frac{k+n}{2}}e_3\Big) + \frac{1}{4b}f_0$$

we have $u_2 = e_0 + me_1 + e_2 + mbe_3 + bf_0$. We attempt to find z_2 such that $\mathrm{nr}(z_2) = u_2$ and $z_2 \in \mathfrak{A}_{H,2}^{\times}$. Let $z_2 = c_0e_0 + c_1e_1 + c_2e_2 + c_3e_3 + d_0f_0 + d_1f_1$ with $c_i, d_j \in \mathbb{Q}$ for each $i \in \{0,1,2,3\}$ and $j \in \{0,1\}$. Recall from Lemma 7.1.10 that $z_2 \in \mathfrak{A}_{H,2}$ if and only if the following conditions hold

$$c_0 + c_1 + c_2 + c_3 + 4d_0 \equiv 0 \pmod 8, \tag{7.7}$$

$$c_0 - c_1 + c_2 - c_3 + 4d_1 \equiv 0 \pmod 8, \tag{7.8}$$

$$c_0 + c_1 - c_2 - c_3 \equiv 0 \pmod 8, \tag{7.9}$$

$$c_0 - c_1 - c_2 + c_3 \equiv 0 \pmod 8, \tag{7.10}$$

and if these congruences are satisfied we have $z_2 \in \mathfrak{A}_{H,2}^{\times}$ if and only if $c_0 \in \mathbb{Z}_2^{\times}$.

We first choose $d_0 = m$ and $d_1 = n$ so that $\mathrm{nr}(f_0z_2) = bf_0$ as required. Suppose $n \equiv 0 \pmod 4$ then $b \equiv 1 \pmod 8$. We have the following;

- If $m \equiv 1 \pmod 8$ then we clearly have the solution $c_0 = c_2 = 1, c_1 = m$ and $c_3 = mb$;

- If $m \equiv -1 \pmod 8$ then we can simply negate the choices of c_1 and c_3 from the $m \equiv 1 \pmod 8$ case;

- If $m \equiv 3 \pmod 8$ then we have the solution $c_0 = c_2 = 1$, $c_1 = -m$ and $c_3 = -mb$ (as in the previous case);

- If $m \equiv -3 \pmod 8$ then we can again simply negate the choices of c_1 and c_3 from the previous case.

The resulting z_2 in each case has reduced norm u_2. Moreover, z_2 in each case has counit 1, so lies in $\mathfrak{A}_{H,2}^{\times}$ by Lemma 7.1.9. □

Lemma 7.2.4. *Let $H = L[D_{\sigma\tau,\rho}]^G$. If $n \equiv 2 \pmod 4$ then $\mathfrak{O}_L$ is **not** free over $\mathfrak{A}_H$.*

Proof. Following on from the previous proof we now suppose $n \equiv 2 \pmod 4$ so that $b \equiv 5 \pmod 8$. Recall the congruence conditions from Lemma 7.1.10. Suppose that $(u_p) \in C^{\times} \prod_p \mathrm{nr}(\mathfrak{A}_{H,p}^{\times})$. We will show that no solution to the congruences exists in this case. To do this we first note that the role of the central element c is now restricted.

Consider the sequence $(u_p) \in C^{\times} \prod_p \mathrm{nr}(\mathfrak{A}_{H,p}^{\times})$, and so, $(u_p) \in C^{\times}\mathbb{U}(Z(\mathfrak{A}_H))$. One may write $(u_p) = (c')(w_p)$ where $c' \in C^{\times}$ and $(w_p) \in \mathbb{U}(Z(\mathfrak{A}_H))$. Let $\Omega = \mathbb{Z}\langle e_0, e_1, e_2, e_3, f_0, f_1, f_2, f_3\rangle$ which contains $\mathrm{nr}(\mathfrak{O}_L[N]^G)$. Note that $\Omega_p = \mathfrak{A}_{H,p}$ for all odd p but that $\Omega_2 \supsetneq \mathfrak{A}_{H,2}$. Then $(w_p) \in \mathbb{U}(Z(\Omega))$. Moreover for odd p, the u_p found in Lemma 7.2.3 are shown to be elements of $\mathfrak{A}_{H,p}^{\times}$ and we can see that u_2 is certainly a central element in Ω. Thus $(u_p) \in \mathbb{U}(Z(\Omega))$ as well. Thus $(c') \in \mathbb{U}(Z(\Omega)) \cap C^{\times} = Z(\Omega)^{\times}$. Hence,

we may write $c' = c'_0e_0 + c'_1e_1 + c'_2e_2 + c'_3e_3 + c'_4f_0$ where c'_i are all elements of $\mathbb{Z}_p^\times$ for all primes p. Thus $\nu_p(c'_i) = 0$ for all $i = 0, 1, 2, 3, 4$ and for all primes p. Thus $c'_i = \pm 1$ for all $i = 0, 1, 2, 3, 4$.

Hence, we must have that $e_0 \pm me_1 \pm e_2 \pm mbe_3 \pm bf_0 \in \mathfrak{A}_{H,2}^\times$ for some choices of signs. That is, the congruences found in Lemma 7.1.10 must have a solution with $c_0 = 1, c_1 = \pm m, c_2 = \pm 1, c_3 = \pm mb \equiv \pm 5m, d_0 = \pm b \equiv \pm 5$ and $d_1 = 0$.

Now, with $n \equiv 2 \pmod 4$ and $b \equiv 5 \pmod 8$, we have the following.

- If $m \equiv 1 \pmod 8$ then congruence 7.7 has three solutions:

  $$(1, -1, -1, 5), (1, 1, -1, -5) \text{ and } (1, -1, 1, -5).$$

  The first and third solutions fail congruence 7.8 and the other solution fails congruence 7.9, so no solution exists.

- If $m \equiv -1 \pmod 8$ gave a solution then negating the values for c_2 and c_3 would give a solution for $m \equiv 1 \pmod 8$ which has no solution.

- If $m \equiv 3 \pmod 8$ then congruence 7.7 has three solutions:

  $$(1, 3, 1, -1), (1, 3, -1, 1) \text{ and } (1, -3, -1, -1).$$

  The first and second solutions fail congruence 7.9 and the third fails congruence 7.10.

- If $m \equiv -3 \pmod 8$ gave a solution then so would $m \equiv 3 \pmod 8$.

So no solution exists if $n \equiv 2 \pmod 4$. □

Combining Lemma 7.2.3 and Lemma 7.2.4: we have shown that $h_2 \in C^\times \mathrm{nr}(\mathfrak{A}_{H,2}^\times)$ if and only if $n \equiv 0 \pmod 4$ and that $h_p \in C^\times \mathrm{nr}(\mathfrak{A}_{H,p}^\times)$ for all odd p. This completes the proof of Theorem 7.2.1.

7.2.2 Global freeness over the associated order in $L[D_{\sigma,\rho}]^G$

We now follow an almost identical route to that of the previous section for an analogous lemma referring to the structures with underlying subgroup $D_{\sigma,\rho}$.

Theorem 7.2.5. *Let $H = L[D_{\sigma,\rho}]^G$. Suppose that for all primes p dividing m we have that $p \equiv 1 \pmod 4$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ if and only if $n \equiv 0 \pmod 4$ if and only if $\mathfrak{O}_L$ is free over the classical associated order $\mathbb{Z}[G]$ of $\mathbb{Q}[G]$.*

Lemma 7.2.6. *Let $H = L[D_{\sigma,\rho}]^G$ and let h_p be defined as above. Then we have*

$$\mathrm{nr}(h_p) = \begin{cases} \frac{1}{8}\Big(e_0 + (-1)^{\frac{k}{2}} e_1 + (-1)^{\frac{k+n}{2}} mbe_2 + (-1)^{\frac{n}{2}} me_3 + 2f_0\Big) & \text{if } \ p = 2, \\ e_0 + e_1 + e_2 + e_3 + \frac{2n}{m} f_0 & \text{if } \ p|m, \\ 1 & \text{if } \ p \nmid 2m. \end{cases}$$

Proof. We first recall the local generators found in Lemma 6.3.1:

$$x_p = \begin{cases} \frac{1}{8}\big(1 + (-1)^{\frac{k+n}{2}} mb\alpha + (-1)^{\frac{n}{2}} m\beta + (-1)^{\frac{k}{2}} \alpha\beta + 4\gamma\big) & \text{if } \ p = 2, \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2m, \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma\tau(\gamma) & \text{if } \ p|m. \end{cases}$$

Furthermore, the proof of Lemma 3.3.7 gives an F-basis of $L[D_{\sigma,\rho}]^G$. Letting $\eta_1 = \rho(\sigma)$ and $\eta_2 = \lambda(\sigma)\rho(\tau)$ we recall the basis to be

$$e_0 = \frac{1}{8}\big(1 + \eta_1 + \eta_1^2 + \eta_1^3 + \eta_2 + \eta_1\eta_2 + \eta_1^2\eta_2 + \eta_1^3\eta_2\big),$$

$$e_1 = \frac{1}{8}\big(1 - \eta_1 + \eta_1^2 - \eta_1^3 + \eta_2 - \eta_1\eta_2 + \eta_1^2\eta_2 - \eta_1^3\eta_2\big),$$

$$e_2 = \frac{1}{8}\big(1 + \eta_1 + \eta_1^2 + \eta_1^3 - \eta_2 - \eta_1\eta_2 - \eta_1^2\eta_2 - \eta_1^3\eta_2\big),$$

$$e_3 = \frac{1}{8}\big(1 - \eta_1 + \eta_1^2 - \eta_1^3 - \eta_2 + \eta_1\eta_2 - \eta_1^2\eta_2 + \eta_1^3\eta_2\big),$$

$$f_0 = \frac{1}{2}(1 - \rho(\sigma^2)), \quad f_1 = f_0\rho(\sigma),$$

$$f_2 = \alpha f_0\lambda(\sigma)\rho(\tau), \text{ and } f_3 = \alpha f_0\lambda(\sigma)\rho(\sigma\tau).$$

We can easily describe the action of some of these basis elements:

$$e_0 : \quad 1 \mapsto 1, \quad \alpha \mapsto 0, \quad \beta \mapsto 0, \quad \alpha\beta \mapsto 0,$$

$$e_1 : \quad 1 \mapsto 0, \quad \alpha \mapsto 0, \quad \beta \mapsto 0, \quad \alpha\beta \mapsto \alpha\beta,$$

$$e_2 : \quad 1 \mapsto 0, \quad \alpha \mapsto \alpha, \quad \beta \mapsto 0, \quad \alpha\beta \mapsto 0,$$

$$e_3 : \quad 1 \mapsto 0, \quad \alpha \mapsto 0, \quad \beta \mapsto \beta, \quad \alpha\beta \mapsto 0,$$

and $e_i : \gamma \to 0$ for all $i = 0, 1, 2, 3$. Moreover $f_0 : \gamma \mapsto \gamma$ and $f_0 : \omega \to 0$ for all $\omega \in \{1, \alpha, \beta, \alpha\beta\}$. So, it is clear that

$$h_2 = \frac{1}{8}\bigg[e_0 + (-1)^{\frac{k}{2}}e_1 + (-1)^{\frac{k+n}{2}}mbe_2 + (-1)^{\frac{n}{2}}me_3 + 4f_0\bigg]. \tag{7.11}$$

Now, for primes p such that $p \nmid 2m$ we clearly have $h_p = 1$ so we are left to consider primes for which $p|m$. Write $f_0h_p = c_0f_0 + c_1f_1 + c_2f_2 + c_3f_3$ for some $c_i \in \mathbb{Q}$. Then we require $f_0h_p \cdot x = f_0x_p$ which is equivalent to $f_0h_p \cdot \gamma = \gamma + \sigma\tau(\gamma)$. We equate the coefficients of γ, $\sigma(\gamma)$, $\tau(\gamma)$ and $\sigma\tau(\gamma)$ to give the following system of equations.

$$c_0 - nc_2 + kc_3 = 1,$$

$$c_1 - kc_2 - nc_3 = 0,$$

$$-mc_3 = 0,$$

$$mc_2 = 1,$$

with an easily found solution: $c_0 = (m+n)/m$, $c_1 = k/m$, $c_2 = 1/m$ and $c_3 = 0$. The reduced norm of $f_0 h_p$ for $p|m$ is

$$\begin{aligned}\mathrm{nr}(f_0 h_p) &= \frac{1}{m^2}\Big((m+n)^2 + k^2 - a\Big) f_0 \\ &= \frac{1}{m^2}(m^2 + n^2 + 2mn + k^2 - a) f_0 \\ &= \frac{1}{m^2}(2mn + a - a) f_0 \\ &= \frac{2n}{m} f_0.\end{aligned}$$

So we have

$$\mathrm{nr}(h_p) = \begin{cases} \frac{1}{8}\Big(e_0 + (-1)^{\frac{k}{2}} e_1 + (-1)^{\frac{k+n}{2}} mbe_2 + (-1)^{\frac{n}{2}} me_3 + 2f_0\Big) & \text{if } \ p = 2, \\ e_0 + e_1 + e_2 + e_3 + \frac{2n}{m} f_0 & \text{if } \ p|m, \\ 1 & \text{if } \ p \nmid 2m. \end{cases}$$

□

Lemma 7.2.7. *Let $H = L[D_{\sigma,\rho}]^G$. If $n \equiv 0 \pmod 4$ and for all primes p that divide m we have $p \equiv 1 \pmod 4$ then $\mathfrak{O}_L$ is free (of rank one) over $\mathfrak{A}_H$.*

Proof. We need to show that $\mathrm{nr}(h_p)$ found in Lemma 7.2.6 has the form cu_p where $c \in C^\times$ and $u_p \in \mathrm{nr}(\mathfrak{A}_{H,p}^\times)$ for all primes p. As before we make an informed choice of c as this value must be consistent regardless of the prime we are working with. Let

$$c = \frac{1}{8}\Big(e_0 + (-1)^{\frac{k}{2}} e_1 + (-1)^{\frac{k+n}{2}} e_2 + (-1)^{\frac{n}{2}} e_3\Big) + \frac{1}{4m} f_0.$$

Then for primes p such that $p|m$ we have

$$u_p = 8\Big(e_0 + (-1)^{\frac{k}{2}} e_1 + (-1)^{\frac{k+n}{2}} e_2 + (-1)^{\frac{n}{2}} e_3 + nf_0\Big).$$

We need to find some $z_p \in \mathfrak{A}_{H,p}$ with $\varepsilon(z_p) = 1$ and $\mathrm{nr}(z_p) = u_p$. Clearly we have

$$z_p = 8\big(e_0 + (-1)^{\frac{n}{2}} e_1 + (-1)^{\frac{k}{2}} e_2 + (-1)^{\frac{k+n}{2}} e_3\big) + d_0 f_0 + d_1 f_1 + d_2 f_2 + d_3 f_3$$

for some $d_i \in \mathbb{Q}$ for each $i \in \{0,1,2,3\}$. Now, $\mathrm{nr}(f_0 z_p) = (d_0^2 + d_1^2 - a(d_2^2 + d_3^2))f_0$.

Since we have that for primes p, if $p|m$ then $p \equiv 1 \pmod 4$ we have that a square root of -1 exists in $\mathbb{Z}_p$ for all $p|m$. So, let

$$f_0 z_p = (2+n)f_0 + i(2-n)f_1$$

where $i \in \mathbb{Z}_p$ such that $i^2 = -1$ so that

$$\mathrm{nr}(f_0 z_p) = (2+n)^2 - (2-n)^2 = 8n$$

as required. The resulting z_p is clearly an element of $\mathfrak{A}_{H,p}$ and since $\mathrm{nr}(h_p) = 1$ we also have $z_p \in \mathfrak{A}_{H,p}^\times$ by Corollary 7.1.8. So we have found that h_p has the required form for all odd primes.

Now consider $p = 2$. Then $u_2 = e_0 + e_1 + mbe_2 + me_3 + mf_0$. We attempt to find z_2 such that $\mathrm{nr}(z_2) = u_2$ and $z_2 \in \mathfrak{A}_{H,2}^\times$. Let $z_2 = c_0 e_0 + c_1 e_1 + c_2 e_2 + c_3 e_3 + d_0 f_0 + d_1 f_1$ with $c_i, d_j \in \mathbb{Q}$ for each $i \in \{0,1,2,3\}$ and $j \in \{0,1\}$. Since for any primes p if $p|m$ then $p \equiv 1 \pmod 4$ we must have that m is the sum of two squares, say $m = c^2 + d^2$ for $c, d \in \mathbb{Z}$. Since m is odd one of c and d is odd, so let c be odd, so that d is even, that is $d \equiv 0 \pmod 2$, and note that if $c \equiv -1 \pmod 4$ we may choose $-c$ instead so that we may assume $c \equiv 1 \pmod 4$. Next choose $d_0 = c$ and $d_1 = d$ so that $\mathrm{nr}(f_0 z_2) = mf_0 = f_0 u_2$ as required. Since either $c \equiv 1 \pmod 8$ or $c \equiv 5 \pmod 8$ we have that $4c \equiv 4 \pmod 8$ and that clearly $4d \equiv 0 \pmod 8$.

Therefore, we have $z_2 \in \mathfrak{A}_{H,2}$ if and only if a solution exists to the congruences found in Lemma 7.1.10 if and only if a solution exists to the following congruences

$$c_0 + c_1 + c_2 + c_3 \equiv 4 \pmod 8, \tag{7.12}$$

$$c_0 - c_1 + c_2 - c_3 \equiv 0 \pmod 8, \tag{7.13}$$

$$c_0 + c_1 - c_2 - c_3 \equiv 0 \pmod 8, \tag{7.14}$$

$$c_0 - c_1 - c_2 + c_3 \equiv 0 \pmod 8. \tag{7.15}$$

Suppose $n \equiv 0 \pmod 4$ so that $b \equiv 1 \pmod 8$. Whether $m \equiv 1 \pmod 8$ or $m \equiv 5 \pmod 8$, we have the solution $c_0 = c_1 = 1, c_2 = mb, c_3 = m$, for which the reduced norm of the resulting z_2 is u_2. Moreover, z_2 has counit 1, so lies in $\mathfrak{A}_{H,2}^{\times}$ by Lemma 7.1.9. □

Lemma 7.2.8. *Let $H = L[D_{\sigma,\rho}]^G$. If $n \equiv 2 \pmod 4$ and for all primes p that divide m we have $p \equiv 1 \pmod 4$ then $\mathfrak{O}_L$ is **not** free over $\mathfrak{A}_H$.*

Proof. Following on from the previous proof we now suppose $n \equiv 2 \pmod 4$ so that $b \equiv 5 \pmod 8$. Recall the congruence conditions from Lemma 7.1.10. As in the proof of Lemma 7.2.4 we suppose that $(u_p) \in C^{\times} \prod_p \mathrm{nr}(\mathfrak{A}_{H,p}^{\times})$ and show that no solution to these congruences exists. Following the proof of Lemma 7.2.4 we require that $e_0 \pm e_1 \pm mbe_2 \pm me_3 \pm mf_0 \in \mathfrak{A}_{H,2}^{\times}$ for some choices of signs. That is the congruences found in Lemma 7.1.10 must have a solution with $c_0 = 1$, $c_1 = \pm 1$, $c_2 = \pm mb \equiv \pm 5m$, $c_3 = \pm m$, $d_0 = \pm m$ and $d_1 = 0$.

Since $d_0 = \pm m$ we have that $4d_0 \equiv 4 \pmod 8$, thus we may assume that $d_0 = m$ and find that a solution exists to the congruences in Lemma 7.1.10 if and only if a solution exists to the congruences 7.12, 7.13, 7.14 and 7.15, found in the proof of Lemma 7.2.7. Note further that if a solution exists for $m \equiv -1 \pmod 8$ then a solution exists for $m \equiv 1 \pmod 8$ by negating the choices of c_2 and c_3. Similarly if a solution exists when $m \equiv -5 \pmod 8$ then a solution exists when $m \equiv 5 \pmod 8$. Finally, if a solution exists for $m \equiv 5 \pmod 8$ then it has the form $(1, \pm 1, \pm 1, \pm 5)$ modulo 8 and so a solution exists for $m \equiv 1 \pmod 8$ of the form $(1, \pm 1, \pm 5, \pm 1)$ modulo 8 since switching the roles of c_2 and c_3 in the congruences only permutes the congruences.

Suppose first that $m \equiv 1 \pmod 8$. Then congruence 7.12 has three solutions: $(1, -1, mb, -m), (1, 1, -mb, -m)$ and $(1, -1, -mb, m)$. The first

fails congruence 7.14, the second fails congruence 7.13 and the third fails congruence 7.15. Thus no solution exists for any value of m. □

By combining the statements of Lemma 7.2.7 and Lemma 7.2.8 we have proven Theorem 7.2.5.

7.2.3 Global freeness over the associated order of $L[D_{\tau,\rho}]^G$

For this subsection we follow an identical argument to that of the previous subsection for the structures with underlying subgroup $D_{\tau,\rho}$.

Theorem 7.2.9. *Let $H = L[D_{\tau,\rho}]^G$. Suppose that for all primes p dividing m we have that $p \equiv 1 \pmod 4$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ if and only if $n \equiv 0 \pmod 4$ if and only if $\mathfrak{O}_L$ is free over the classical associated order $\mathbb{Z}[G]$ of $\mathbb{Q}[G]$.*

Lemma 7.2.10. *Let $H = L[D_{\tau,\rho}]^G$. Then the reduced norm of the h_p is:*

$$\mathrm{nr}(h_p) = \begin{cases} \frac{1}{8}\Big(e_0 + (-1)^{\frac{k+n}{2}} mbe_1 + (-1)^{\frac{n}{2}} me_2 + (-1)^{\frac{k}{2}} e_3 + 2f_0\Big) & \text{if } \ p = 2, \\ e_0 + e_1 + e_2 + e_3 + \frac{2n}{m} f_0 & \text{if } \ p | m, \\ 1 & \text{if } \ p \nmid 2m. \end{cases}$$

Proof. We first recall the local generators found in Lemma 6.3.1, which are the same as those in the previous lemma:

$$x_p = \begin{cases} \frac{1}{8}\big(1 + (-1)^{\frac{k+n}{2}} mb\alpha + (-1)^{\frac{n}{2}} m\beta + (-1)^{\frac{k}{2}} \alpha\beta + 4\gamma\big) & \text{if } \ p = 2, \\ 1 + \alpha + \beta + \alpha\beta + \gamma & \text{if } \ p \nmid 2m, \\ 1 + \alpha + \beta + \alpha\beta + \gamma + \sigma\tau(\gamma) & \text{if } \ p | m. \end{cases}$$

Furthermore, the proof of Lemma 3.3.7 gives a $\mathbb{Q}$-basis of $L[D_{\tau,\rho}]^G$. Letting $\eta_1 = \rho(\tau)$ and $\eta_2 = \lambda(\tau)\rho(\sigma\tau)$ we recall the basis to be

$$e_0 = \frac{1}{8}\big(1 + \eta_1 + \eta_1^2 + \eta_1^3 + \eta_2 + \eta_1\eta_2 + \eta_1^2\eta_2 + \eta_1^3\eta_2\big),$$

$$e_1 = \frac{1}{8}(1 - \eta_1 + \eta_1^2 - \eta_1^3 + \eta_2 - \eta_1\eta_2 + \eta_1^2\eta_2 - \eta_1^3\eta_2),$$

$$e_2 = \frac{1}{8}(1 + \eta_1 + \eta_1^2 + \eta_1^3 - \eta_2 - \eta_1\eta_2 - \eta_1^2\eta_2 - \eta_1^3\eta_2),$$

$$e_3 = \frac{1}{8}(1 - \eta_1 + \eta_1^2 - \eta_1^3 - \eta_2 + \eta_1\eta_2 - \eta_1^2\eta_2 + \eta_1^3\eta_2),$$

$$f_0 = \frac{1}{2}(1 - \rho(\sigma^2)), \quad f_1 = f_0\rho(\tau),$$

$$f_2 = \alpha f_0\lambda(\tau)\rho(\sigma\tau), \text{ and } f_3 = \alpha f_0\lambda(\tau)\rho(\sigma).$$

The action of these basis elements can be described as follows

$$e_0 : \quad 1 \mapsto 1, \quad \alpha \mapsto 0, \quad \beta \mapsto 0, \quad \alpha\beta \mapsto 0,$$

$$e_1 : \quad 1 \mapsto 0, \quad \alpha \mapsto \alpha, \quad \beta \mapsto 0, \quad \alpha\beta \mapsto 0,$$

$$e_2 : \quad 1 \mapsto 0, \quad \alpha \mapsto 0, \quad \beta \mapsto \beta, \quad \alpha\beta \mapsto 0,$$

$$e_3 : \quad 1 \mapsto 0, \quad \alpha \mapsto 0, \quad \beta \mapsto 0, \quad \alpha\beta \mapsto \alpha\beta,$$

and $f_0 : \gamma \mapsto \gamma$. So, it is clear that

$$h_2 = \frac{1}{8}\Big[e_0 + (-1)^{\frac{k+n}{2}}mbe_1 + (-1)^{\frac{n}{2}}me_2 + (-1)^{\frac{k}{2}}e_3 + 4f_0\Big]. \tag{7.16}$$

Now, for primes p such that $p \nmid 2m$ we clearly have $h_p = 1$ so we are left to consider primes for which $p|m$. Suppose $f_0h_p = c_0f_0 + c_1f_1 + c_2f_2 + c_3f_3$ for some $c_i \in \mathbb{Q}$. Then we require $f_0h_p \cdot x = f_0x_p$ which is equivalent to $f_0h_p \cdot \gamma = \gamma + \sigma\tau(\gamma)$. As previously we have the following system of equations attained by equating the coefficients of γ, $\sigma(\gamma)$, $\tau(\gamma)$ and $\sigma\tau(\gamma)$.

$$c_0 + nc_3 = 1,$$

$$mc_2 = 0,$$

$$c_1 - nc_2 = 0,$$

$$-mc_3 = 1.$$

The system has the easily found solution $c_0 = (m+n)/m$, $c_1 = c_2 = 0$ and $c_3 = -1/m$. Thus we may find

$$\mathrm{nr}(f_0 h_p) = \frac{1}{m^2}\Big((m+n)^2 - b\Big) = \frac{2n}{m}$$

found in a similar way to the previous lemma. So we have

$$\mathrm{nr}(h_p) = \begin{cases} \frac{1}{8}\Big(e_0 + (-1)^{\frac{k+n}{2}} mbe_1 + (-1)^{\frac{n}{2}} me_2 + (-1)^{\frac{k}{2}} e_3 + 2f_0\Big) & \text{if} \quad p = 2, \\ e_0 + e_1 + e_2 + e_3 + \frac{2n}{m} f_0 & \text{if} \quad p|m, \\ 1 & \text{if} \quad p \nmid 2m. \end{cases}$$

□

Lemma 7.2.11. *Let $H = L[D_{\tau,\rho}]^G$. If $n \equiv 0 \pmod 4$ and for all primes p that divide m we have $p \equiv 1 \pmod 4$ then $\mathfrak{O}_L$ is free (of rank one) over $\mathfrak{A}_H$.*

Proof. As previously we now need to show that $\mathrm{nr}(h_p)$ has the form cu_p where $c \in C^\times$ and $u_p \in \mathrm{nr}(\mathfrak{A}_{H,p}^\times)$ for all primes p. We make an analogous choice of c to the previous lemma:

$$c = \frac{1}{8}\Big(e_0 + (-1)^{\frac{k+n}{2}} e_1 + (-1)^{\frac{n}{2}} e_2 + (-1)^{\frac{k}{2}} e_3\Big) + \frac{1}{4m} f_0.$$

We have the analogous u_p, for $p|m$, to that of Lemma 7.2.7:

$$u_p = 8\Big(e_0 + (-1)^{\frac{k}{2}} e_1 + (-1)^{\frac{k+n}{2}} e_2 + (-1)^{\frac{n}{2}} e_3 + nf_0\Big).$$

Therefore, we may make the same conclusion as in the previous lemma by following the analogous proof. That is, since we impose that for all primes p dividing m we have $p \equiv 1 \pmod 4$, there exists $z_p \in \mathfrak{A}_{H,2}^\times$ such that $\mathrm{nr}(z_p) = u_p$, specifically $f_0 z_p = (2+n)f_0 + i(2-n)f_1$ where i is a square root of -1 in $\mathbb{Z}_p$. So we have found that h_p has the required form for all odd primes.

Now consider $p = 2$. Then $u_2 = e_0 + mbe_1 + me_2 + e_3 + mf_0$, analogous to that of Lemma 7.2.7. Continuing to follow that proof, we may conclude

that some $z_2 = c_0e_0 + c_1e_1 + c_2e_2 + c_3e_3 + d_0f_0 + d_1f_1$ with $c_i, d_j \in \mathbb{Q}$ for each $i \in \{0,1,2,3\}$ and $j \in \{0,1\}$ lies in $\mathfrak{A}_{H,2}$ if and only if there exists a solution to the same congruences: 7.12,7.13, 7.14 and 7.15. Thus, for $n \equiv 0 \pmod 4$ we have the analogous solution $c_0 = c_3 = 1$, $c_1 = mb$, $c_2 = m$, $d_0 = c$ and $d_1 = d$ for some c, d such that $c^2 + d^2 = m$, $c \equiv 1 \pmod 4$ and $d \equiv 0 \pmod 2$. Again, the resulting z_2 has reduced norm u_2, and counit 1, so lies in $\mathfrak{A}_{H,2}^{\times}$ by Lemma 7.1.9. □

Lemma 7.2.12. *Let $H = L[D_{\tau,\rho}]^G$. If $n \equiv 2 \pmod 4$ and for all primes p that divide m we have $p \equiv 1 \pmod 4$ then $\mathfrak{O}_L$ is **not** free over $\mathfrak{A}_H$.*

Proof. Following on from the previous proof we now suppose $n \equiv 2 \pmod 4$ so that $b \equiv 5 \pmod 8$. Following the proof of Lemma 7.2.8, we know that we require that $e_0 \pm mbe_1 \pm me_2 \pm e_3 \pm mf_0 \in \mathfrak{A}_{H,2}^{\times}$ for some choices of signs. That is the congruences found in Lemma 7.2.7 have a solution with $c_0 = 1, c_1 = \pm mb, c_2 = \pm m, c_3 = \pm 1, d_0 = \pm m$ and $d_1 = 0$. Since the congruences permute when one permutes the order of c_1, c_2 c_3 we know that if a solution exists then a solution must exist with $c_0 = 1, c_1 = \pm 1, c_2 = \pm mb$ and $c_3 = \pm m$. We have shown no such solution exists in the proof of Lemma 7.2.8 and so we also have no solution in this case. □

By combining the statements of Lemma 7.2.11 and Lemma 7.2.12 we have proven Theorem 7.2.9.

Bibliography

[BB99] W. Bley and R. Boltje, *Lubin-Tate formal groups and module structure over Hopf orders*, Journal de théorie des nombres de Bordeaux **11** (1999), no. 2, 269–305.

[Byo97] N.P. Byott, *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications*, Journal de théorie des nombres de Bordeaux **9** (1997), no. 1, 201–219.

[Byo02] ———, *Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields*, Journal of Algebra **248** (2002), no. 1, 334–365.

[Chi00] L. N. Childs, *Taming wild extensions: Hopf algebras and local galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, 2000.

[CR81] C.W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders*, vol. 1, John Wiley & Sons inc., 1981.

[CR87] ———, *Methods of representation theory with applications to finite groups and orders*, vol. 2, John Wiley & Sons inc., 1987.

[CS20] T. Crespo and M. Salguero, *Computation of Hopf Galois structures on low degree separable extensions and classification of*

those for degrees p^2 and $2p$, Publicacions Matemàtiques **64** (2020), no. 1, 121–141.

[Eld18] G. Elder, *Ramified extensions of degree p and their Hopf-Galois module structure*, Journal de théorie des nombres de Bordeaux **30** (2018), no. 1, 19–40.

[Frö83] A. Fröhlich, *Galois module structure of algebraic integers*, vol. 3, A Series of Modern Surverys in Mathematics, no. 1, Springer-Verlag, 1983.

[FT93] A. Fröhlich and M.J. Taylor, *Algebraic number theory*, vol. 27, Cambridge studies in advanced Mathematics, 1993.

[Fuj90a] Genjiro Fujisaki, *An elementary construction of Galois quaternion extension*, Proc. Japan Acad. **66** (1990), no. A, 80–83.

[Fuj90b] ———, *A remark on quaternion extensions of the rational p-adic field*, Proceedings of the Japan Academy, Series A **66** (1990), no. 8, 257–259.

[GP87] C. Greither and B. Pareigis, *Hopf-Galois theory for separable field extensions.*, Journal of Algebra **1** (1987), 239–258.

[HGK81] E. Hecke, J.R. Goldman, and R. Kotzen, *Lectures on the theory of algebraic numbers*, vol. 77, New York: Springer, 1981.

[JY88] C. U. Jensen and N. Yui, *Quaternion extensions*, Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata **1** (1988), 155–182.

[KKTU19a] A. Koch, T. Kohl, P.J. Truman, and R. Underwood, *Isomorphism problems for Hopf-Galois structures on separable field*

extensions, Journal of Pure and Applied Algebra **223** (2019), no. 5, 2230–2245.

[KKTU19b] ———, *Normality and short exact sequences of Hopf-Galois structures*, Communications in Algebra **47** (2019), no. 5, 2086–2101.

[Koc15] A. Koch, *Scaffolds and integral Hopf-Galois module structure on purely inseparable extensions*, New York J. Math. **21** (2015), 73–91.

[Lam05] T.Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, 2005.

[Lam13] ———, *A first course in noncommutative rings*, vol. 131, Springer Science and Business Media, 2013.

[Mar69] J. Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de galois diédral d'ordre* $2p$, Annales de l'institut Fourier **19** (1969), no. 1, 1–80.

[Mar71] ———, *Modules sur l'algébre du groupe quaternionien*, Ann. Sci. Ecole Norm. Sup. **4** (1971), no. 4, 399–408.

[Neu13] J. Neukirch, *Algebraic number theory*, vol. 322, Springer Science and Business Media, 2013.

[Ser12] J.P. Serre, *A course in arithmetic*, vol. 7, Springer Science and Business Media, 2012.

[SV18] A. Smoktunowicz and L. Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86.

[Tay81] M.J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Inventiones mathematicae **63** (1981), no. 1, 41–79.

[Tho10] L. Thomas, *On the Galois module structure of extensions of local fields*, Publications Mathematiques de Besançon (2010), 157–194.

[Tru11] P.J. Truman, *Towards a generalisation of Noether's theorem to nonclassical Hopf-Galois structures*, New York J. Math. **17** (2011), 799–810.

[Tru12] ———, *Hopf-Galois module structure of tame biquadratic extensions*, Journal de théorie des nombres de Bordeaux **24** (2012), 173–199.

[Tru16] ———, *Canonical nonclassical Hopf-Galois module structure of nonabelian Galois extensions*, Communications in Algebra **44** (2016), no. 3, 1119–1130.

[Tru18] ———, *Commuting Hopf-Galois structures on a separable field extension*, Communications in Algebra **46** (2018), no. 4, 1420–1427.

[TT19] S. Taylor and P.J. Truman, *The structure of Hopf algebras giving Hopf-Galois structures on quaternionic extensions*, New York J. Math. **25** (2019), 219–237.

[Vau92] T.P. Vaughan, *Constructing quaternionic fields*, Glasgow Math. J. **34** (1992), no. 1, 43–54.

[Wit36] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, Journal für die reine und angewandte Mathematik (1936), no. 174, 237–245.