Hopf-Galois Module Structure Of Some Tamely Ramified Extensions

Submitted by

Paul James Truman

to the University of Exeter as a thesis for the degree of Doctor of Philosophy in Mathematics, June 2009.

I certify that all material in this thesis which is not my own work has been identified and that no material is included for which a degree has previously been conferred upon me.

.....

Paul James Truman

Abstract

We study the Hopf-Galois module structure of algebraic integers in some finite extensions of p-adic fields and number fields which are at most tamely ramified. We show that if L/K is a finite unramified extension of p-adic fields which is Hopf-Galois for some Hopf algebra H then the ring of algebraic integers $\mathfrak{O}_L$ is a free module of rank one over the associated order $\mathfrak{A}_H$. If H is a commutative Hopf algebra, we show that this conclusion remains valid in finite ramified extensions of p-adic fields if p does not divide the degree of the extension. We prove analogous results for finite abelian Galois extensions of number fields, in particular showing that if L/K is a finite abelian domestic extension which is Hopf-Galois for some commutative Hopf algebra H then $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$. We study in greater detail tamely ramified Galois extensions of number fields with Galois group isomorphic to $C_p \times C_p$, where p is a prime number. Byott has enumerated and described all the Hopf-Galois structures admitted by such an extension. We apply the results above to show that $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$ in all of the Hopf-Galois structures, and derive necessary and sufficient conditions for $\mathfrak{O}_L$ to be globally free over $\mathfrak{A}_H$ in each of the Hopf-Galois structures. In the case $p = 2$ we consider the implications of taking $K = \mathbb{Q}$. In the case that p is an odd prime we compare the structure of $\mathfrak{O}_L$ as a module over $\mathfrak{A}_H$ in the various Hopf-Galois structures.

Acknowledgements

First of all I would like to thank my supervisor Dr. Nigel Byott for all his advice, guidance and patience over the past three years. Also in Exeter, I am grateful to the other members of the Pure Mathematics group for enduring my many internal seminars, and to my Ph.D. office-mates for tea and catchphrases. Thanks are also due to the EPSRC for funding my research.

At home I would like to thank my parents for all their love and support, and for letting me talk about Mathematics at the dinner table. I am also grateful to Fr. Peter Stone for many excellent dinners, and to Andrew, Matt and both Sams for many good times.

In America I am grateful to the Lydon family for their hospitality whilst I was writing up, and to the Mathematics faculty at the University of Denver for allowing me access to their library. I would also like to thank Dr. Griff Elder for a fun and productive few days in Omaha.

Finally, I would like to thank Anna B. Lydon, who was in all of these places, for her constant love and support, and for all the adventures.

This thesis is dedicated to my Mother, who underwent a bone marrow transplant to treat Chronic Lymphocytic Leukaemia whilst it was being written.

Contents

Chapter 1

Introduction

Classical Galois module theory seeks to describe the algebraic integers in a finite Galois extension of global or local fields with respect to the Galois group. Let L/K be such an extension, with Galois group G. The Normal Basis Theorem states that there exists an element $z \in L$ such that the set $\{\sigma(z) \mid \sigma \in G\}$ is a K-basis for L (a normal basis). This is equivalent to L being a free module of rank one over the group algebra $K[G]$. It is natural to ask whether analogous results hold at integral level - does there exist an element $x \in \mathfrak{O}_L$ such that the set $\{\sigma(x) \mid \sigma \in G\}$ is an $\mathfrak{O}_K$-basis for $\mathfrak{O}_L$ (a normal integral basis of L)? Equivalently, is $\mathfrak{O}_L$ is a free module (necessarily of rank one) over the integral group ring $\mathfrak{O}_K[G]$? In the global case, the existence of a normal integral basis is a strong condition, as in general $\mathfrak{O}_L$ does not have a basis over $\mathfrak{O}_K$ at all, much less one consisting of the Galois conjugates of a single element. To address this problem we employ completion - for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we study the completed ring of integers $\mathfrak{O}_{L,\mathfrak{p}}$, which does have a basis over the completed ring of integers $\mathfrak{O}_{K,\mathfrak{p}}$. If $\mathfrak{O}_{L,\mathfrak{p}}$ is a free module over the completed integral group ring $\mathfrak{O}_{K,\mathfrak{p}}[G]$ for every prime $\mathfrak{p}$ of $\mathfrak{O}_K$ then we say that $\mathfrak{O}_L$ is *locally free* over $\mathfrak{O}_K[G]$; this property is necessary but not sufficient for global freeness. If $\mathfrak{O}_L$ is locally free over $\mathfrak{O}_K[G]$ then it defines a class in the locally free class group $\mathrm{Cl}\,(\mathfrak{O}_K[G])$. Frohlich's Hom Description [Frö83] of this group allows

us to calculate this class and determine the global structure of $\mathfrak{O}_L$ over $\mathfrak{O}_K[G]$, at least up to stable isomorphism.

Noether's theorem answers the local question above in terms of the ramification in the extension - if L/K is a finite Galois extension of local (respectively global) fields with group G, then $\mathfrak{O}_L$ is free (respectively locally free) over $\mathfrak{O}_K[G]$ if and only if L/K is at most tamely ramified. Since Noether's theorem provides a necessary and sufficient condition for freeness (respectively local freeness), it is clear that other techniques are required to study wildly ramified extensions. One of these is to study the structure of $\mathfrak{O}_L$ as a module over a different $\mathfrak{O}_K$-order in the group algebra $K[G]$, called the associated order:

$$\mathfrak{A}_{K[G]} = \{\alpha \in K[G] \mid \alpha(x) \in \mathfrak{O}_L \text{ for all } x \in \mathfrak{O}_L\}.$$

If L/K is at most tamely ramified then the associated order and the integral group ring coincide, but if the extension is wildly ramified then the integral group ring is properly contained in the associated order. By construction, the associated order is the largest $\mathfrak{O}_K$-order in $K[G]$ for which $\mathfrak{O}_L$ is a module.

The first success of this approach was Leopoldt's theorem [Leo59], that if $L/\mathbb{Q}$ is an abelian extension then $\mathfrak{O}_L$ is free over $\mathfrak{A}_{K[G]}$. This implies the corresponding result for extensions of $\mathbb{Q}_p$, and in this case a slightly stronger result holds - if L/K is an abelian extension of p-adic fields with Galois group G and additionally $L/\mathbb{Q}_p$ is an abelian extension then $\mathfrak{O}_L$ is free over $\mathfrak{A}_{K[G]}$ [Let98]. For extensions not covered by these general theorems, we seek criteria for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_{K[G]}$. It was in the search for such criteria that the Hopf algebra structure of the group algebra $K[G]$ was first exploited. Childs' theorem [Chi00, (12.7)] is that if L/K is a finite Galois extension of p-adic fields with Galois group G and $\mathfrak{A}_{K[G]}$ is a Hopf

order in $K[G]$ then $\mathfrak{O}_L$ is free over $\mathfrak{A}_{K[G]}$.

In a slightly different direction, we have the notion of a Hopf-Galois structure on a finite separable extension of fields L/K. This consists of a K-Hopf algebra of dimension $[L : K]$ acting on the extension in a "Galois like" way. If L/K is a Galois extension then the group algebra $K[G]$ gives one such structure, and we call this the classical structure. However, a given extension may also admit a number of nonclassical structures. A theorem of Greither and Pareigis [Chi00, (6.8)] reduces the enumeration of the Hopf-Galois structures admitted by a given separable extension to a purely group theoretic problem, and shows that the corresponding Hopf algebras all occur as "twisted" forms of certain group algebras. Work of Childs and Byott [Chi00, (7.3)] simplified the calculations required in the enumeration of Hopf-Galois structures, and a theorem of Byott [Byo96] identifies precisely those Galois extensions which admit only the classical Hopf-Galois structure.

For a finite separable extension of local or global fields L/K, Hopf-Galois module theory seeks to describe the ring of integers $\mathfrak{O}_L$ with respect to the various different Hopf-Galois structures admitted by the extension. Within each Hopf algebra H we define an associated order analogous to the associated order in the group algebra $K[G]$:

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

and study the structure of $\mathfrak{O}_L$ as a module over each $\mathfrak{A}_H$. If the extension L/K admits a number of Hopf-Galois structures, we can compare the structure of $\mathfrak{O}_L$ as a module over the associated orders in the various Hopf algebras. Childs' theorem generalises to this setting: if the K-Hopf algebra H gives a Hopf-Galois structure on a finite separable extension of p-adic fields L/K and the associated order $\mathfrak{A}_H$

is a Hopf order in H then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$. Byott [Byo00] exhibited a class of wildly ramified Galois extensions p-adic fields L/K for which $\mathfrak{O}_L$ is not free over $\mathfrak{A}_{K[G]}$, the associated order in the classical structure given by $K[G]$, but for which $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$, the associated order in some Hopf algebra H giving a nonclassical structure on the extension. So from the point of view of describing $\mathfrak{O}_L$, for these extensions the classical structure is not the "correct" structure to use, and a nonclassical structure gives a more satisfactory description of the algebraic integers.

As we have seen above, a motivation for the use of Hopf algebras in Galois module theory is a desire to have some generalisation of Noether's theorem hold for wildly ramified extensions. However, by Greither and Pareigis's theorem the number of Hopf-Galois structures admitted by an extension is independent of the ramification in the extension, and so a tamely ramified extension may admit a number of structures. If the extension L/K is Galois then it admits at least the classical structure, with Hopf algebra $K[G]$. If the extension is at most tamely ramified then Noether's theorem asserts that the associated order $\mathfrak{A}_{K[G]}$ coincides with the integral group ring $\mathfrak{O}_K[G]$ and that $\mathfrak{O}_L$ is free (or locally free) over $\mathfrak{O}_K[G]$. It is not known whether analogous results hold for any nonclassical structures admitted by the extension. It is certainly natural to investigate the structure of $\mathfrak{O}_L$ as a module over $\mathfrak{A}_H$ in each of the Hopf-Galois structures admitted by the extension, and we might also ask whether the associated order in each nonclassical structure has a simple description, as does the associated order in the classical structure. In this thesis we answer these questions for certain classes of tamely ramified extensions of number fields and p-adic fields.

Chapter 2 contains background information on algebras and orders, idèles and class groups, Galois module theory, Hopf algebras and Hopf-Galois module theory. In chapter 3 we prove two results concerning the Hopf-Galois module structure of

finite extensions of p-adic fields. We show that if L/K is a finite unramified Galois extension of p-adic fields and H is a Hopf algebra giving a Hopf-Galois structure on the extension then $\mathfrak{O}_L$ is free over the associated order $\mathfrak{A}_H$. We also show that if L/K is a finite extension of p-adic fields such that the degree of the extension is coprime to p and H is a commutative Hopf algebra giving a Hopf-Galois structure on the extension then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$. In both cases we find that the associated order has the same simple description. We also prove analogous results for abelian Galois extensions of number fields. In particular we show that if L/K is an abelian Galois extension of number fields and H is a Hopf algebra giving a Hopf-Galois structure on the extension then $\mathfrak{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{H,\mathfrak{p}}$ for almost all primes $\mathfrak{p}$ of $\mathfrak{O}_K$, and that if L/K is a tamely ramified abelian Galois extension of number fields of prime power degree and H is a commutative Hopf algebra giving a Hopf-Galois structure on the extension then $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$.

For the remainder of the thesis we consider a particular class of tamely ramified Galois extensions of number fields. By Byott's uniqueness theorem a Galois extension of prime degree p admits only the classical Hopf-Galois structure. We therefore consider the simplest case for which we have nonclassical structures, Galois extensions of degree p^2. In particular we consider Galois extensions of number fields L/K with group isomorphic to $C_p \times C_p$. We assume that our ground field contains a primitive p^{th} root of unity, and so such extensions are formed by adjoining the p^{th} roots of two elements of K. In chapter 4 we derive congruence conditions on these elements which are equivalent to the extension being tamely ramified, and calculate explicit bases of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$. In chapter 5 we reproduce results of Byott, who showed that an elementary abelian extension of degree p^2 admits precisely p^2 Hopf-Galois structures, and used Greither and Pareigis's theorem to describe the Hopf algebras, finding in particular that they are all commutative. We give the Wedderburn decompositions of these algebras as

products of extensions of K, and use these to describe the unique maximal order in each algebra, giving explict local bases for each prime of $\mathfrak{O}_K$. Finally we derive formulae for the action of the Hopf algebras on elements of L.

In the final three chapters we consider the local and global structure of $\mathfrak{O}_L$ over the associated orders in the various Hopf-Galois structures admitted by the extension. By the results of chapter 3 we know that $\mathfrak{O}_L$ is locally free over $\mathfrak{A}_H$ in each of the Hopf-Galois structures, and we begin chapter 6 by giving explicit generators of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$. We then give an explicit description of the unit group $\mathfrak{A}_{H,\mathfrak{p}}^{\times}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$, which we shall require when determining conditions for global freeness the final chapters.

Chapter 7 covers in detail the case $p = 2$, and chapter 8 the case when p is an odd prime number. Each of these chapters is structured in the same way. For each Hopf algebra H giving a Hopf-Galois structure on L/K we "sandwich" the locally free class group $\mathrm{Cl}(\mathfrak{A}_H)$ between products of ray class groups, and interpret the class representing $\mathfrak{O}_L$ as a product of classes of fractional ideals. This gives necessary and sufficient conditions for $\mathfrak{O}_L$ to be globally free over each $\mathfrak{A}_H$. In the case $p = 2$ we also consider in detail extensions where the base field is $\mathbb{Q}$, and derive a condition for $\mathfrak{O}_L$ to be free over each $\mathfrak{A}_H$ in terms of the representability questions for certain quadratic forms. We give examples of extensions exhibiting a variety of global behaviours. In the case when p is an odd prime we prove a partial result concerning the comparison of the structure of $\mathfrak{O}_L$ over $\mathfrak{A}_H$ in the various nonclassical Hopf-Galois structures admitted by the extension.

Chapter 2

Background

In this chapter we collect first the algebraic and arithmetic results which we shall require in what follows. We then introduce Hopf algebras and the notion of a Hopf-Galois structure on a finite separable extension of fields, along with theorems which allow us to enumerate and describe all of the Hopf-Galois structures admitted by a given extension. Finally we present Hopf-Galois module theory as a generalisation of classical Galois module theory, and results which will allow us to study the structure of a ring of algebraic integers with respect to a Hopf-Galois structure.

2.1 Preliminaries

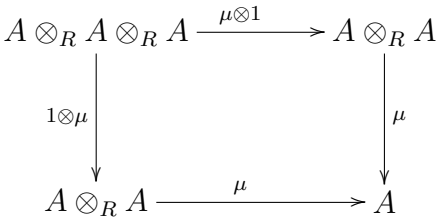
2.1.1 Algebras and Orders

Definition 2.1.1. Let R be a commutative ring with unity. An R-module A is called an *R-algebra* if it has the following additional structure:

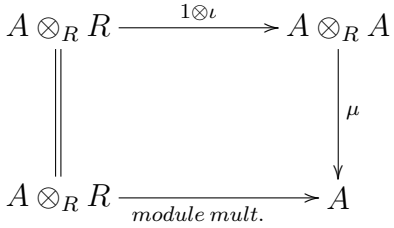
- A map $\mu : A \otimes_R A \to A$ called the *multiplication map*
- A map $\iota : R \to A$ called the *unit map*

such that the following diagrams commute:

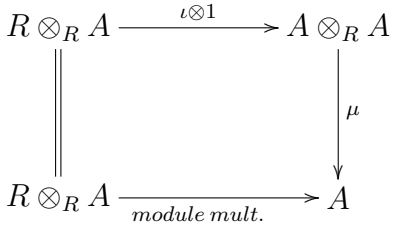
- Associativity:



- Unitary:



and



Definition 2.1.2. 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.

Definition 2.1.3. Let R be a Dedekind domain with field of fractions K and let A be a finite dimensional K-algebra. An *R-order* in A is a subring Λ of A satisfying the following conditions:

- The centre of Λ contains R.
- Λ is finitely generated as an R-module.
- $\Lambda \otimes_R K = A$.

An R-order in A is called *maximal* if it is not properly contained in any larger R-order in A.

Example 2.1.4. Let G be a group of order n. Let R be a Dedekind domain with field of fractions K, and suppose $\mathrm{char}(K) \nmid n$. Then the group algebra

$$K[G] = \left\{ \sum_{g \in G} k_g g \mid k_g \in K \right\}$$

is a separable K-algebra with multiplication μ induced linearly from the multiplication in G and unit map ι given by $k \mapsto k1_G$ for $k \in K$. The group ring

$$R[G] = \left\{ \sum_{g \in G} r_g g \mid r_g \in R \right\}$$

is an R-order in $K[G]$.

We now state two results concerning maximal orders. We shall use these in Chapter 3, where we shall require information about maximal orders in commutative group algebras.

Proposition 2.1.5. Let R be a Dedekind domain with field of fractions K, and let A be a commutative separable K-algebra. Then there is a unique maximal R-order in A, namely the integral closure of R in A.

Proof. See [CR81a, (26.10)]. □

Proposition 2.1.6. Let G be a group of order n. Let R be a Dedekind domain with field of fractions K, and suppose $\mathrm{char}(K) \nmid n$. Let Λ be any R-order in $K[G]$ containing $R[G]$. Then

$$R[G] \subseteq \Lambda \subseteq n^{-1}R[G].$$

In particular, $R[G]$ is maximal if and only if $n \in R^\times$.

Proof. See [CR81a, (27.1)]. □

2.1.2 Local Fields

Definition 2.1.7. 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 call a generator π of $\mathfrak{m}$ a *uniformiser* of R. Since R is a principal ideal domain, the unique non-zero prime ideal $\mathfrak{m}$ is a maximal ideal, and so the quotient ring $R/\mathfrak{m}$ is a field. It is called the *residue field* of R. The unit group $R^\times$ of R comprises precisely those elements of R which do not lie in $\mathfrak{m}$. Any nonzero element $x \in R$ may be written as $x = u\pi^n$ for some $u \in R^\times$ and $n \in \mathbb{N} \cup \{0\}$. The integer n is independent of the choice of π, and so we may define the *valuation* of x to be n. The units of R are precisely those elements having valuation zero. For $x, y \in R$, we write $x \sim y$ if x and y have the same valuation, i.e. differ only by a unit. Let K be the field of fractions of R. The valuation on R extends to a valuation $v : K \to \mathbb{Z} \cup \{\infty\}$, with the convention that $v(0) = \infty$. Conversely, if we are given a field K together with a valuation $v : K \to \mathbb{Z} \cup \{\infty\}$, then the set $R = \{x \in K \mid v(x) \geq 0\}$ is a discrete valuation ring. It is called the *valuation ring* or the *ring of integers* of K with respect to v.

Definition 2.1.8. Let K be a field, $v : K \to \mathbb{Z} \cup \{\infty\}$ a valuation on K with valuation ring R, and $\mathfrak{m}$ the unique prime ideal of R. Suppose that the residue field $R/\mathfrak{m}$ is finite, having q elements. We define the *normalised absolute value* on K associated to v, denoted $|.|_v$, by $|x|_v = q^{-v(x)}$. We call K a *local field* if it is complete with respect to this absolute value.

Example 2.1.9. Let K be a number field, and $\mathfrak{p}$ a prime of $\mathfrak{O}_K$ lying above a prime number $p \in \mathbb{Z}$. Then the residue field $\mathfrak{O}_K/\mathfrak{p}$ is finite. We define a valuation $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ as follows: we set $v_\mathfrak{p}(0) = \infty$, and for $x \in K^\times$, we set $v_\mathfrak{p}(x)$ to be the power of the prime $\mathfrak{p}$ appearing in the factorisation of the fractional ideal $x\mathfrak{O}_K$. The field K is not complete with respect to the absolute value associated to this valuation, but we may form its completion, which we denote by $K_\mathfrak{p}$. This is

a local field. We write $\mathfrak{O}_{K,\mathfrak{p}}$ for its valuation ring (ring of integers), and $\mathfrak{p}$ for its maximal ideal. Local fields obtained in this way are called *p-adic fields*, and will be one of our main objects of study in this thesis.

Definition 2.1.10. Let L/K be a finite separable extension of local fields, with valuations v_L, v_K, valuation rings R_L, R_K, maximal ideals $\mathfrak{m}_L, \mathfrak{m}_K$ and uniformisers π_L, π_K respectively. Let p be the characteristic of the residue field $R_K/\mathfrak{m}_K$. We define the *ramification index* $e_{L/K}$ by $e_{L/K} = v_L(\pi_K)$. The residue field $R_L/\mathfrak{m}_L$ is a finite extension of the residue field $R_K/\mathfrak{m}_K$, and we define the *residue field degree* $f_{L/K}$ to be the degree of this extension. We have the relation $[L : K] = e_{L/K} f_{L/K}$. The extension L/K is said to be *unramified* if $e_{L/K} = 1$, and *ramified* otherwise. If L/K is ramified, then we say that it is *tamely ramified* (or simply *tame*) if $(e_{L/K}, p) = 1$, and *wildly ramified* (or simply *wild*) otherwise.

We mention another characterisation of discrete valuation rings, which is based on the concept of a *local ring*. We shall make use of local rings in a different context in Chapter 6, using results presented at the end of this chapter.

Definition 2.1.11. A commutative ring R is said to be *local* if it has a unique maximal ideal.

Example 2.1.12. A commutative ring R is a discrete valuation ring if and only if it is local, with unique maximal ideal generated by a non-nilpotent element, and is *Noetherian*. That is, every increasing chain of ideals of R is eventually stationary.

2.1.3 Algebraic Number Theory

We now turn to a global setting, and review briefly some of the ramification theory of number fields.

Definition 2.1.13. Let L/K be a finite extension of number fields with rings of

integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$, and let

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

be the unique factorisation of $\mathfrak{p}\mathfrak{O}_L$ into prime ideals of $\mathfrak{O}_L$. For each $i = 1, \dots, g$, the residue field $\mathfrak{O}_L/\mathfrak{P}_i$ is a finite extension of the residue field $\mathfrak{O}_K/\mathfrak{p}$, and we denote the degree of this extension by f_i. We have the relation

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

The prime $\mathfrak{p}$ is said to be *unramified* in $\mathfrak{O}_L$ if $e_i = 1$ for all $i = 1, \dots, g$, and *ramified* in $\mathfrak{O}_L$ otherwise. Let p be the characteristic of the residue field $k = \mathfrak{O}_K/\mathfrak{p}$. If $\mathfrak{p}$ is ramified in $\mathfrak{O}_L$, then we say that it is *tamely ramified* if $(e_i, p) = 1$ for all $i = 1, \dots, g$, and *wildly ramified* otherwise. Equivalently, the prime $\mathfrak{p}$ is unramified (respectively, tamely ramified) in $\mathfrak{O}_L$ if the extension of p-adic fields $L_{\mathfrak{P}_i}/K_{\mathfrak{p}}$ is unramified (respectively, tamely ramified) for each $i = 1, \dots, g$.
We call the extension L/K *unramified* if all primes of $\mathfrak{O}_K$ are unramified in $\mathfrak{O}_L$, *tamely ramified* (or simply *tame*) if every prime of $\mathfrak{O}_K$ which is ramified in $\mathfrak{O}_L$ is tamely ramified, and *wildly ramified* (or simply *wild*) if any prime ramifies wildly. Finally, we shall call the extension L/K *domestic* if it is Galois and no prime $\mathfrak{p}$ of $\mathfrak{O}_K$ lying above a prime number dividing $[L : K]$ is ramified in $\mathfrak{O}_L$.

We shall primarily be interested in studying Galois extensions of number fields, where the Galois correspondence combined with the ramification theory outlined above yields the following:

Theorem 2.1.14. (Hilbert's Ramification Theory) Let L/K be a Galois extension of number fields with rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively, and Galois

group G. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$, and let

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

be the unique factorisation of $\mathfrak{p}\mathfrak{O}_L$ into prime ideals of $\mathfrak{O}_L$, with corresponding residue field degrees $f_1, \dots, f_g$. Then

- G acts transitively on the primes $\mathfrak{P}_i$ lying above $\mathfrak{p}$. The stabiliser of a prime $\mathfrak{P}$ is called the *decomposition group* of $\mathfrak{P}$ and is denoted by $G_\mathfrak{P}$,
  i.e. $G_\mathfrak{P} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$.

- The ramification indices e_i and residue field degrees f_i are independent of i, and so we have
  $$\mathfrak{p}\mathfrak{O}_L = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e$$
  with $[\mathfrak{O}_L/\mathfrak{P}_i : \mathfrak{O}_K/\mathfrak{p}] = f$ for each $i = 1, \dots, g$, and so $[L : K] = efg$.

- $|G_\mathfrak{P}| = ef$ for each prime $\mathfrak{P}$ lying above $\mathfrak{p}$. In particular, $|G_\mathfrak{P}| = 1$ if and only if $\mathfrak{p}$ is totally split in $\mathfrak{O}_L$.

- For $\sigma \in G$, we have $G_{\sigma\mathfrak{P}} = \sigma G_\mathfrak{P} \sigma^{-1}$, i.e. the decomposition groups of the primes lying above $\mathfrak{p}$ are conjugate. In particular, if G is abelian then they coincide.

Proof. See [Neu99, Chapter I, §9]. □

We now take a finite Galois extension L/K of number fields and consider the consequences for L of completing K with respect to the absolute value arising from some prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$, as in (2.1.9). In this case the corresponding completion of L need not be a local field, but is *semilocal*. That is, a finite product of local fields.

Theorem 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 $\mathfrak{O}_K$. Write $K_\mathfrak{p}$ for the

completion of K with respect to the absolute value arising from $\mathfrak{p}$. Write $L_\mathfrak{p}$ for the $K_\mathfrak{p}$-algebra $L \otimes_K K_\mathfrak{p}$. Then there is a bijection between the primitive idempotents of $L_\mathfrak{p}$ and the primes of $\mathfrak{O}_L$ which lie above $\mathfrak{p}$. This induces a decomposition:

$$L \otimes_K K_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$$

where $L_\mathfrak{P}$ is the completion of L with respect to the absolute value arising from the prime ideal $\mathfrak{P}$ of $\mathfrak{O}_L$. We also have an analogous decomposition at integral level:

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

Proof. See [FT91, Theorem 17]. □

Definition 2.1.16. A *Galois algebra* over a field K is a finite dimensional K-algebra $\mathcal{L}$ together with a group $G = G(\mathcal{L}/K)$ of algebra automorphisms of $\mathcal{L}$, such that $\mathcal{L} \cong K[G]$ as $K[G]$-modules. We call G the *Galois group* of $\mathcal{L}$. If K is the field of fractions of some Dedekind domain $\mathfrak{O}_K$, and $K_\mathfrak{p}$ is the completion of K with respect to the valuation arising from a prime $\mathfrak{p}$ of $\mathfrak{O}_K$, then $\mathcal{L}_\mathfrak{p} = \mathcal{L} \otimes_K K_\mathfrak{p}$ has the structure of a $K_\mathfrak{p}$-Galois algebra, with $G(\mathcal{L}_\mathfrak{p}/K_\mathfrak{p}) \cong G(\mathcal{L}/K)$.

Example 2.1.17. Any Galois extension of fields L/K is a K-Galois algebra with group $G = \mathrm{Gal}(L/K)$. If L/K is a Galois extension of number fields and $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$, then by (2.1.15)

$$L \otimes_K K_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$$

is a $K_\mathfrak{p}$-Galois algebra with group $G = \mathrm{Gal}(L/K)$. If $\mathfrak{P}'$ is a fixed prime ideal lying above $\mathfrak{p}$, and $\Sigma \subseteq G$ is a set of coset representatives for the decomposition group

$G_{\mathfrak{P}'}$ in G, then (2.1.14) yields

$$\prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}} = \prod_{\sigma\in\Sigma} L_{\sigma\mathfrak{P}'}.$$

This Galois algebra is clearly commutative and, since L/K is a separable extension, it is also a separable $K_{\mathfrak{p}}$-algebra.

2.1.4 Idèles and Class Groups

It is often desirable to pass from local results to global ones. Suppose we have a problem concerning a number field K, and that for each nonzero prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we can solve the corresponding problem for the completion $K_{\mathfrak{p}}$ of K with respect to the absolute value arising from $\mathfrak{p}$. It is natural to ask to what extent this information allows us to solve the original problem over K. In this section we introduce tools which allow us to answer this question.

Definition 2.1.18. Let K be a number field. The (finite) *idèle group* $\mathbb{J}(K)$ of K is defined to be the restricted topological product

$$\mathbb{J}(K) = \prod_{\mathfrak{p}\lhd\mathfrak{O}_K}{}' K_{\mathfrak{p}}^{\times} = \left\{(x_{\mathfrak{p}})_{\mathfrak{p}} \mid x_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times}, x_{\mathfrak{p}} \in \mathfrak{O}_{K,\mathfrak{p}}^{\times} \text{ for almost all } \mathfrak{p}\right\}$$

with multiplication defined componentwise. We interpret "almost all" as "for all but finitely many". For each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ we have an inclusion $K \hookrightarrow K_{\mathfrak{p}}$. These allow us to define a diagonal embedding $K^{\times} \hookrightarrow \mathbb{J}(K)$ by $x \mapsto (x)_{\mathfrak{p}}$; this is an idèle since $v_{\mathfrak{p}}(x) = 0$ for almost all primes $\mathfrak{p}$ and so $x \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$ for almost all $\mathfrak{p}$. The image of $K^{\times}$ in $\mathbb{J}(K)$ is called the group of *principal idèles*. The *group of unit idèles* is defined by

$$\mathbb{U}(\mathfrak{O}_K) = \prod_{\mathfrak{p}\lhd\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}}^{\times} = \left\{(x_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbb{J}(K) \mid x_{\mathfrak{p}} \in \mathfrak{O}_{K,\mathfrak{p}}^{\times} \text{ for all } \mathfrak{p}\right\}.$$

The introduction of idèles provides us with a new way to view the ideal class group of a number field, and leads to a useful generalisation.

Proposition 2.1.19. Let $\mathfrak{I}(K)$ and $\mathrm{Cl}\,(\mathfrak{O}_K)$ denote the fractional ideal group and ideal class group of K respectively. Define a surjective homomorphism

$$\mathbb{J}(K) \to \mathfrak{I}(K)$$

by

$$(x_\mathfrak{p})_\mathfrak{p} \mapsto \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})}.$$

Then this homomorphism induces an isomorphism

$$\frac{\mathbb{J}(K)}{K^\times \mathbb{U}(\mathfrak{O}_K)} \cong \mathrm{Cl}\,(\mathfrak{O}_K)\,.$$

Proof. See [Neu99, Chapter VI, §1, Definition (1.2) ff.]. □

Definition 2.1.20. Let $\mathfrak{m}$ be an ideal of $\mathfrak{O}_K$. Define a subgroup $\mathbb{U}_\mathfrak{m}(\mathfrak{O}_K)$ of $\mathbb{U}(\mathfrak{O}_K)$ by

$$\mathbb{U}_\mathfrak{m}(\mathfrak{O}_K) = \{(x_\mathfrak{p})_\mathfrak{p} \in \mathbb{U}(\mathfrak{O}_K) \mid x_\mathfrak{p} \in (1 + \mathfrak{m}\mathfrak{O}_{K,\mathfrak{p}}) \text{ for all } \mathfrak{p}\}\,.$$

Define the *ray class group* mod $\mathfrak{m}$ to be the quotient

$$\mathrm{Cl}_\mathfrak{m}(\mathfrak{O}_K) = \frac{\mathbb{J}(K)}{K^\times \mathbb{U}_\mathfrak{m}(\mathfrak{O}_K)}.$$

Using (2.1.19), we may interpret this as the group of those fractional ideals of $\mathfrak{O}_K$ which are prime to $\mathfrak{m}$, modulo those principal fractional ideals for which there exists a generator α satisfying $\alpha \equiv 1 \pmod^* \mathfrak{m}$. (That is, $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m})$ for all $\mathfrak{p} \mid \mathfrak{m}$, but possibly $\alpha \notin \mathfrak{O}_K$.)

We now define the idèle group of a finite dimensional separable algebra over a number field analogously to the definition of the idèle group of a number field in

(2.1.18).

Definition 2.1.21. Let K be a number field, A a finite dimensional separable K-algebra, and Λ an $\mathfrak{O}_K$-order in A. For $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, we write $A_\mathfrak{p} = A \otimes_K K_\mathfrak{p}$ and $\Lambda_\mathfrak{p} = \Lambda \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}}$. We define the (finite) *idèle group* $\mathbb{J}(A)$ of A by

$$\mathbb{J}(A) = \prod_{\mathfrak{p} \lhd \mathfrak{O}_K}{}' A_\mathfrak{p}^\times = \left\{ (a_\mathfrak{p})_\mathfrak{p} \mid a_\mathfrak{p} \in A_\mathfrak{p}^\times, a_\mathfrak{p} \in \Lambda_\mathfrak{p}^\times \text{ for almost all } \mathfrak{p} \right\}$$

with multiplication defined componentwise. This definition does not depend upon the choice of $\mathfrak{O}_K$-order Λ in A, since if Γ is another order then $\Lambda_\mathfrak{p} = \Gamma_\mathfrak{p}$ for all but finitely many primes $\mathfrak{p}$ of $\mathfrak{O}_K$. The group of *principal idèles* is defined to be the image of the diagonal embedding $A^\times \hookrightarrow \mathbb{J}(A)$ by $a \mapsto (a)_\mathfrak{p}$. The *group of unit idèles* of Λ is defined by

$$\mathbb{U}(\Lambda) = \prod_{\mathfrak{p} \lhd \mathfrak{O}_K} \Lambda_\mathfrak{p}^\times = \left\{ (a_\mathfrak{p})_\mathfrak{p} \in \mathbb{J}(A) \mid a_\mathfrak{p} \in \Lambda_\mathfrak{p}^\times \text{ for all } \mathfrak{p} \right\}.$$

We now introduce the type of problem which we shall study using idèle groups - the structure of a module for an order in a finite dimensional separable algebra over a number field.

Definition 2.1.22. Let K be a number field, A a finite dimensional separable K-algebra, and Λ an $\mathfrak{O}_K$-order in A. Let X be a finitely generated (say left) Λ-module. For $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, write $\Lambda_\mathfrak{p} = \Lambda \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}}$ and $X_\mathfrak{p} = X \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}}$. Then $X_\mathfrak{p}$ is a finitely generated $\Lambda_\mathfrak{p}$-module. The Λ-module X will be called *locally free* if $X_\mathfrak{p}$ is a free $\Lambda_\mathfrak{p}$-module for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$.

Definition 2.1.23. Retain the notation of (2.1.22). The *Grothendieck group* $\mathfrak{K}_0(\Lambda)$ of locally free Λ-modules is defined to be the abelian group with generators $[X]$ corresponding to Λ-isomorphism classes of locally free Λ-modules X and with relations $[X \oplus Y] = [X] + [Y]$. We define a homomorphism $\mathbb{N} \to \mathfrak{K}_0(\Lambda)$ by mapping n to

the class $[\Lambda^n]$ of the free Λ-module of rank n, and extend this to a homomorphism $\mathbb{Z} \to \mathfrak{K}_0(\Lambda)$. We then define the *locally free class group* $\mathrm{Cl}\,(\Lambda)$ to be the cokernel of this map. We have the following defining exact sequence:

$$0 \to \mathbb{Z} \to \mathfrak{K}_0(\Lambda) \to \mathrm{Cl}\,(\Lambda) \to 1.$$

A locally free Λ-module X has trivial class in the locally free class group $\mathrm{Cl}\,(\Lambda)$ if and only if it is a *stably free* Λ-module. That is, $X \oplus \Lambda^r$ is a free Λ-module for some natural number r. However, we shall only be interested in the case where A is a commutative algebra. In this case, A satisfies the *Eichler condition* relative to $\mathfrak{O}_K$, and so we may apply the Jacobinksi Cancellation Theorem (see [CR81b, 51.24]), and conclude that the order Λ has *locally free cancellation*. That is

$$X \text{ is a stably free } \Lambda\text{-module} \Leftrightarrow X \text{ is a free } \Lambda\text{-module.}$$

We summarise the above in the following proposition:

Proposition 2.1.24. Let K be a number field, A a commutative finite dimensional separable K-algebra, and Λ an $\mathfrak{O}_K$-order in A. Suppose that X is an $\mathfrak{O}_K$-module which is a locally free Λ-module. Then X is a free Λ-module if and only if X has trival class in the locally free class group $\mathrm{Cl}\,(\Lambda)$.

Proof. See [CR81b, §51]. □

In general, Fröhlich's so-called *Hom Description* provides a description of $\mathrm{Cl}\,(\Lambda)$ using the idèlic machinery defined in this section (see [Frö83]). Once again, we shall only apply this result in the case that A is a commutative algebra, when it reduces to the following:

Proposition 2.1.25. (Fröhlich) Let K be a number field, A a finite dimensional separable commutative K-algebra, and Λ an $\mathfrak{O}_K$-order in A. Then there is an

isomorphism of groups

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

Suppose that X is an $\mathfrak{O}_K$-module which is a locally free Λ-module and that $X \otimes_{\mathfrak{O}_K} K$ is a free A-module. Let Γ be a generator of $X \otimes_{\mathfrak{O}_K} K$ over A, and for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ let $\gamma_{\mathfrak{p}}$ be a generator of $X_{\mathfrak{p}}$ over $\Lambda_{\mathfrak{p}}$. For each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ define $a_{\mathfrak{p}} \in A_{\mathfrak{p}}$ by $a_{\mathfrak{p}}\Gamma = \gamma_{\mathfrak{p}}$. Then the class of X in $\mathrm{Cl}\,(\Lambda)$ corresponds to the class of the idèle $(a_{\mathfrak{p}})_{\mathfrak{p}}$ in the quotient group above.

Proof. See [CR81b, (49.22)]. □

2.2 Galois Module Theory

The Hopf-Galois module theory which we shall study in this thesis has its roots in classical Galois module theory. For field extensions, Galois theory provides the following theorem:

Theorem 2.2.1. (The Normal Basis Theorem) Let L/K be a finite Galois extension of fields with group G. Then there exists an element $x \in L$ such that the set $\{\sigma(x) \mid \sigma \in G\}$ is a basis for L over K. Equivalently, L is a free $K[G]$-module of rank one.

Proof. See [Lan99, VI, Theorem 13.1]. □

A question in Galois module theory is whether, in local fields or global fields, analogous results hold at integral level - when is $\mathfrak{O}_L$ a free $\mathfrak{O}_K[G]$-module? For local fields, this question was answered by Noether using the notions of tame ramification defined in (2.1.10) and (2.1.13).

Theorem 2.2.2. (Noether) Let L/K be a finite Galois extension of local fields with group G and rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. Then $\mathfrak{O}_L$ is free over $\mathfrak{O}_K[G]$ if and only if L/K is at most tamely ramified.

Proof. See [Frö83, Theorem 3]. □

This implies the corresponding result for number fields:

Corollary 2.2.3. Let L/K be a finite Galois extension of number fields with group G and rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. Then $\mathfrak{O}_L$ is Locally Free (cf. 2.1.22) over $\mathfrak{O}_K[G]$ if and only if L/K is at most tamely ramified.

Proof. See [Frö83, Corollary 2 to Theorem 3]. □

It is natural to ask whether some generalisation of Noether's theorem still holds when L/K is wildly ramified. One approach to studying this problem is to replace the integral group ring $\mathfrak{O}_K[G]$ with a larger $\mathfrak{O}_K$-order in $K[G]$, called the *associated order*.

Definition 2.2.4. Let L/K be a finite Galois extension of local fields or global fields with group G and rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. Define the *associated order* $\mathfrak{A}_{K[G]} \subseteq K[G]$ by

$$\mathfrak{A}_{K[G]} = \{\alpha \in K[G] \mid \alpha(x) \in \mathfrak{O}_L \text{ for all } x \in \mathfrak{O}_L\}.$$

The associated order is the largest order in $K[G]$ for which $\mathfrak{O}_L$ is a module. If L/K is wildly ramified then $\mathfrak{O}_K[G] \subsetneq \mathfrak{A}_{K[G]}$, but we may investigate the structure of $\mathfrak{O}_L$ as an $\mathfrak{A}_{K[G]}$-module. The first result in this direction was due to Leopoldt [Leo59], who showed that if $L/\mathbb{Q}$ is an abelian extension, then $\mathfrak{O}_L$ is a free $\mathfrak{A}_{\mathbb{Q}[G]}$-module. This implies that for any prime number p, $\mathfrak{O}_{L,p}$ is free over $\mathfrak{A}_{\mathbb{Q}_p[G]}$. Lettl [Let98] generalised the local version of this result to a relative extension L/K of p-adic fields, assuming that $L/\mathbb{Q}_p$ is abelian.

A motivation for the use of Hopf algebras in the context of Galois module theory is the desire to study the structure of $\mathfrak{O}_L$ as an $\mathfrak{A}_{K[G]}$-module in wildly ramified ex-

tensions. In this thesis, however, we shall only be concerned with tamely ramified extensions.

2.3 Hopf Algebras

Definition 2.3.1. Let R be a commutative ring with unity. An R-algebra A with multiplication map $\mu : A \otimes_R A \to A$ and unit map $\iota : R \to A$ is called an *R-bialgebra* if it has the following additional structure maps:

- An R-algebra homomorphism $\Delta : A \to A \otimes_R A$ called the *comultiplication map*
- An R-algebra homomorphism $\varepsilon : A \to R$ called the *counit map*

such that the following diagrams commute:

- Coassociativity:

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

- Counitary:

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

and

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

Remark 2.3.2. An R-module which is not necessarily an R-algebra but does possess counit and comultiplication maps as defined above is called an *R-coalgebra*. Comparing the diagrams above to those in (2.1.1), we see that this definition is "dual" to that of an R-algebra.

Example 2.3.3. Let K be a field and G a finite group. Then the group algebra $K[G]$ is a K-bialgebra, with comultiplication Δ given by $g \mapsto g \otimes g$ and counit ε given by $g \mapsto 1$ for all $g \in G$.

Definition 2.3.4. Let R be a commutative ring with unity. An R-bialgebra H with multiplication map $\mu : H \otimes_R H \to H$, unit map $\iota : R \to H$, comultiplication map $\Delta : H \to H \otimes_R H$ and counit map $\varepsilon : H \to R$ is called an *R-Hopf algebra* if there is a map $\lambda : H \to H$ with the following properties:

- λ is an R-algebra antihomomorphism. That is, $\lambda(hh') = \lambda(h')\lambda(h)$
- λ is an R-coalgebra antihomomorphism. That is, if $\tau : H \otimes_R H \to H$ denotes the *switch map*, $\tau(h \otimes h') = (h' \otimes h)$, then $\Delta\lambda(h) = (\lambda \otimes \lambda)\tau\Delta(h)$
- λ satisfies the *antipode property*: $\mu(1 \otimes \lambda)\Delta = \iota\varepsilon = \mu(\lambda \otimes 1)\Delta$

such a map is called the *antipode map*.

Definition 2.3.5. (Sweedler Notation) Let R be a commutative ring with unity and H an R-Hopf algebra. For $h \in H$, we shall write

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

Definition 2.3.6. An R-Hopf Algebra H is called

- *commutative* if it is commutative as an R-algebra.
- *cocommutative* if $\tau\Delta = \Delta$.

- *abelian* if it is both commutative and cocommutative.
- *finite* if it is finitely generated and projective as an R-module.

Example 2.3.7. Let K be a field and G a finite group. The K-bialgebra $K[G]$ is a finite K-Hopf algebra, with antipode λ given by $g \mapsto g^{-1}$ for all $g \in G$. Since the comultiplication Δ is given by $g \mapsto g \otimes g$, it is a cocommutative Hopf Algebra.

Definition 2.3.8. Let R be a commutative ring with unity, and H a finite R-Hopf algebra. Then the linear dual $H^* = \mathrm{Hom}_R(H, R)$ is an R-Hopf algebra, and so will be called the *dual algebra* to H.

Proposition 2.3.9. Let K be a field of characteristic zero, and let H be a finite commutative K-Hopf algebra. Then H is a separable K-algebra.

Proof. Since H is a finite K-Hopf algebra, it is an *Artinian* ring. That is, every decreasing chain of ideals terminates. Now by [Wat97, (11.4)], we have that H is *reduced*. That is,

$$\bigcap_{\mathfrak{p} \lhd H} \mathfrak{p} = 0,$$

where the product is taken over all prime ideals $\mathfrak{p}$. Using [CR81a, (5.18)], we may conclude that H is semisimple. Finally, since K has characteristic zero and H is commutative, we may use [CR81a, (7.6)] to conclude that H is separable. □

2.3.1 Hopf Orders

Definition 2.3.10. 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.

Example 2.3.11. Let R be a Dedekind domain with field of fractions K of characteristic zero. Let G be a finite group. Then the group ring $R[G]$ is a Hopf order in the group algebra $K[G]$. In fact it is minimal amongst all Hopf orders in $K[G]$. (See [Chi00, (5.2)]).

Proposition 2.3.12. Let R be a Dedekind domain with field of fractions K of characteristic zero. Let G be a finite group. Suppose that Λ is an $\mathfrak{O}_K$-order in the group algebra $K[G]$. If the comultiplication map $\Delta : H \to H \otimes H$ satisfies $\Delta(\Lambda) \subseteq \Lambda \otimes_{\mathfrak{O}_K} \Lambda$, then Λ is a Hopf order.

Proof. We need to show that the counit $\varepsilon : K[G] \to K$ and antipode $\lambda : K[G] \to K[G]$ also restrict to Λ. Let $\Delta : K[G] \to K[G] \otimes K[G]$ be the comultiplication map on $K[G]$, and $\mu : K[G] \otimes K[G] \to K[G]$ be the multiplication map on $K[G]$. We define recursively

$$\begin{aligned} \Delta_1 &= \Delta : K[G] \to K[G] \otimes K[G] \\ \Delta_i &= (\mathrm{id}^{i-1} \otimes \Delta) \circ \Delta_{i-1} : K[G] \to \bigotimes^{i+1} K[G] \end{aligned}$$

and

$$\begin{aligned} \mu_1 &= \mu : K[G] \otimes K[G] \to K[G] \\ \mu_i &= \mu_{i-1} \circ (\mathrm{id}^{i-1} \otimes \mu) : \bigotimes^{i+1} K[G] \to K[G] \end{aligned}$$

Then for $g \in G$,

$$\mu_i \Delta_i g = g^{i+1}$$

and so for $z = \sum_{g \in G} k_g g \in K[G]$,

$$\mu_{|G|-1}\Delta_{|G|-1}(z) = \sum_{g \in G} k_g g^{|G|} = \sum_{g \in G} k_g = \varepsilon(z),$$

and

$$\mu_{|G|-2}\Delta_{|G|-2}(z) = \sum_{g \in G} k_g g^{|G|-1} = \sum_{g \in G} k_g g^{-1} = \lambda(z).$$

Now $\Lambda \subset K[G]$ inherits the μ_i from $K[G]$, and since by assumption Δ restricts to Λ, it also inherits the Δ_i. So for all $z \in \Lambda$ we have $\lambda(z) \in \Lambda$, and $\varepsilon(z) \in K \cap \Lambda = R$. $\square$

2.3.2 Integrals

Definition 2.3.13. Let R be a commutative ring with unity and H an R-Hopf algebra. 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 $x \in H$, we have $\theta x = \varepsilon(x)\theta$.

Proposition 2.3.14. Let R be a commutative ring with unity and H an R-Hopf algebra. Then the module of left integrals of H is a rank one projective R-module. In particular, if R is a principal ideal domain, then the module of left integrals of H is a free R-module of rank one.

Proof. See [Chi00, Corollary 3.4]. □

2.4 Hopf-Galois Structures

The notion of a Hopf-Galois structure is defined for certain extensions of commutative rings. We shall be interested mainly in studying Hopf-Galois structures on finite separable extensions of fields.

Definition 2.4.1. Let R be a commutative ring with unity. 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

$$\begin{aligned} h(st) &= \sum_{(h)} h_{(1)}(s)h_{(2)}(t) \\ h(1) &= \varepsilon(h)1. \end{aligned}$$

Definition 2.4.2. Let R be a commutative ring with unity. Let H be an R-Hopf algebra, and let $S \supseteq R$ be a commutative ring such that S is an H-module algebra. We say that S is an *H-Galois extension of R* (*H-Galois* for short), or that H gives

a *Hopf-Galois structure* on the extension if the R-linear map

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

defined by

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

is an R-module isomorphism.

Example 2.4.3. Let L/K be a finite Galois extension of fields with group G. Then the Hopf algebra $K[G]$ gives a Hopf-Galois structure on the extension; this is called the *classical* structure. Any other Hopf-Galois structures admitted by the extension are called *nonclassical*.

2.4.1 Greither and Pareigis's Theorem

Given a finite separable extension of fields L/K, it is natural to ask how many different Hopf-Galois structures are admitted by the extension. The theorem of Greither and Pareigis provides an answer to this question, and also a theoretical description of the Hopf algebras.

Definition 2.4.4. Let $\mathrm{Perm}(X)$ denote the group of permutations of a finite set X. A subgroup N of $\mathrm{Perm}(X)$ is said to be *regular* if any two (and therefore all three) of the following are satisfied:

- N and X have the same cardinality.
- N acts transitively on X.
- The stabilizer $\mathrm{Stab}_N(x) = \{n \in N \mid nx = x\}$ is trivial for all $x \in X$.

Definition 2.4.5. Let G be a group and suppose G' is a subgroup of G. Let X be the left coset space G/G' of G' in G, so $X = \{xG' \mid x \in G\}$. We shall write $\overline{x}$ for

the coset xG'. Define the *left translation map*

$$\lambda : G \to \mathrm{Perm}(X)$$

by:

$$\lambda(g)(\overline{x}) = \overline{gx} \text{ for } g \in G \text{ and } \overline{x} \in X.$$

Proposition 2.4.6. Let L/K be a finite separable extension of fields with Galois closure E. Let $G = \mathrm{Gal}(E/K), G' = \mathrm{Gal}(E/L)$ and $X = G/G'$. Then the map λ is an embedding of G into $\mathrm{Perm}(X)$.

Proof. See [Chi00, 6.6]. □

Remark 2.4.7. If X is a group (i.e. in the above L/K is a Galois extension with group G and so $G' = \{1_G\}$) we may also define the *right translation map*

$$\rho : G \to \mathrm{Perm}(X)$$

by:

$$\rho(g)(x) = xg^{-1} \text{ for } g \in G \text{ and } x \in X.$$

This is an embedding of G into $\mathrm{Perm}(X)$.

Definition 2.4.8. We define a left action of G on $\mathrm{Perm}(X)$ by conjugation via the embedding λ. For $g \in G$ and $\pi \in \mathrm{Perm}(X)$ we set

$${}^{g}\pi = \lambda(g)\pi\lambda(g^{-1})$$

Theorem 2.4.9 (Greither and Pareigis). Let L/K be a finite separable extension of fields with Galois closure E. Let $G = \mathrm{Gal}(E/K), G' = \mathrm{Gal}(E/L)$ and $X = G/G'$. Then there is a bijection between regular subgroups N of $\mathrm{Perm}(X)$ normalised by $\lambda(G)$ and Hopf-Galois structures on L/K. If N is such a subgroup,

then G acts on the group algebra $E[N]$ by acting simultaneously on the coefficients as the Galois group and on the group elements by conjugation via the embedding λ. The Hopf algebra giving the Hopf-Galois structure corresponding to the subgroup N is

$$H = E[N]^G = \{z \in E[N] \mid {}^g z = z \text{ for all } g \in G\}.$$

Such a Hopf algebra then acts on the extension L/K as follows: if $\left(\sum_{n\in N} c_n n\right) \in H$ (with $c_n \in E$ a priori), then

$$\left(\sum_{n\in N} c_n n\right).x = \sum_{n\in N} c_n(n^{-1}(\overline{1_G}))x.$$

Proof. See [Chi00, 6.8]. □

Definition 2.4.10. If H is a Hopf algebra produced by (2.4.9), then we shall refer to the isomorphism class of the group N as the *type* of the Hopf algebra.

Remark 2.4.11. We shall only apply (2.4.9) to extensions of fields of characteristic zero, where separability is automatic. In fact, we shall mainly be concerned with Galois extensions. In the notation of (2.4.9) we then have that $G' = \{1_G\}$, and so the statement of the theorem is somewhat simpler.

Remark 2.4.12. Since all group algebras are cocommutative Hopf algebras (See 2.3.7), it follows that all of the Hopf algebras produced by (2.4.9) are cocommutative.

Remark 2.4.13. By (2.3.12) we have that in order to show that an order Λ in a group algebra over a field of characteristic zero is a Hopf order, it is sufficient to show that the comultiplication map Δ restricts to Λ. Since Hopf algebras produced by (2.4.9) inherit the Hopf algebra structure maps from group algebras, they also have this property.

2.4.2 Byott's Translation

If we use Greither and Pareigis's theorem directly to count Hopf-Galois structures on a given finite separable extension L/K, then we seek to study certain regular subgroups of $\mathrm{Perm}(X)$, a group of order $[L : K]!$. If $[L : K]$ is large, this is a difficult problem. A theorem of Byott, making precise an idea originally due to Childs, reverses the relationship between G and N, facilitating easier calculations.

Definition 2.4.14. Let N be a group. The *holomorph* of N, $\mathrm{Hol}(N)$, is the normaliser of $\lambda(N)$ in $\mathrm{Perm}(N)$:

$$\mathrm{Hol}(N) = \{\sigma \in \mathrm{Perm}(N) \mid \sigma \text{ normalises } N\}.$$

Proposition 2.4.15. Since N is a group, the right translation map $\rho : N \to \mathrm{Perm}(N)$ is an embedding of N into $\mathrm{Perm}(N)$ (see (2.4.7)), and we have:

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

Proof. See [Chi00, (7.2)] □

Theorem 2.4.16. (Byott's Translation) Let $G' \subset G$ be finite groups, let $X = G/G'$ and let N be an abstract group of order $|X|$. Then there is a bijection between the following two sets:

$$\mathcal{N} = \{\alpha : N \to \mathrm{Perm}(X) \mid \alpha \text{ an injective homomorphism such that } \alpha(N) \text{ is regular } \}$$

$$\mathcal{G} = \{\beta : G \to \mathrm{Perm}(N) \mid \beta \text{ an injective homomorphism such that } \beta(G') = \mathrm{Stab}_{\beta(G)}(1_N)\}$$

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

- $\alpha(N) = \alpha'(N)$ if and only if $\beta(G)$ and $\beta'(G)$ are conjugate by an element of $\mathrm{Aut}(N)$.

- $\alpha(N)$ is normalised by $\lambda(G) \subset \mathrm{Perm}(X)$ if and only if $\beta(G)$ is contained in $\mathrm{Hol}(N)$.

Proof. Originally [Byo96, Proposition 1]. This formulation [Chi00, (7.3)]. □

This theorem may be used to count Hopf-Galois structures on a given finite separable extension of fields as follows:

Corollary 2.4.17. Let L/K be a finite separable extension of fields with Galois closure E. Let $G = \mathrm{Gal}(E/K), G' = \mathrm{Gal}(E/L)$. Define

$$\mathrm{Aut}(G, G') = \{\sigma \in \mathrm{Aut}(G) \mid \sigma(G') = G'\}.$$

Let $\mathcal{S}$ be the set of isomorphism classes of groups N with $|N| = |G/G'|$. For each $[N] \in \mathcal{S}$, define $e'(G, G', N)$ to be the number of subgroups G^* of $\mathrm{Hol}(N)$ such that there exists an isomorphism from G^* to G taking the stabiliser in G^* of 1_N to G'. Then the number of Hopf-Galois structures of type N on L/K is given by

$$e(G, G', N) = \frac{|\mathrm{Aut}(G, G')|}{|\mathrm{Aut}(N)|} e'(G, G', N)$$

and the total number of Hopf-Galois structures admitted by the extension is given by

$$\sum_{[N] \in \mathcal{S}} e(G, G', N).$$

Proof. See [Chi00, (7.6)] □

We shall only apply this corollary in the case that the extension L/K is a Galois extension, when it reduces to the following:

Corollary 2.4.18. Let L/K be a Galois extension with group G. Then in the above, $G' = \{1_G\}, X = G$ and $\mathrm{Aut}(G, G') = \mathrm{Aut}(G)$. The quantity $e'(G, N) = e'(G, G', N)$ therefore counts the number of regular subgroups of $\mathrm{Hol}(N)$ which are

isomorphic to G, and we have

$$e(G,N) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e'(G,N).$$

Thus the total number of Hopf-Galois structures admitted by the extension is given by

$$\sum_{[N]\in\mathcal{S}} e(G,N).$$

2.5 Hopf-Galois Module Theory

Consider a finite separable extension of fields L/K. The following proposition implies a generalisation of the Normal Basis Theorem (2.2.1) to an arbitrary Hopf-Galois structure on the extension.

Proposition 2.5.1. Let R be a local ring and H an R-Hopf algebra. Suppose that S is an H-Galois extension of R (see (2.4.2). Then S is a free H-module of rank one.

Proof. See [Chi00, (2.16)]. □

Corollary 2.5.2. Let K be a field and H a K-Hopf algebra. Suppose that L is a finite separable extension of K which is H-Galois. Then L is a free H-module of rank one.

If L/K is an extension of local or global fields, it is natural to investigate analogous results at integral level. If H is a Hopf algebra giving a nonclassical structure on L/K, then there is no natural analogue in H to the integral group ring $\mathfrak{O}_K[G]$, the minimal Hopf order in $K[G]$. Indeed, H need not contain any Hopf orders at all. The notion of the associated order, however, generalises easily:

Definition 2.5.3. Let L/K be a finite, H-Galois extension of local fields or global fields with rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$ respectively. Define the *associated order* $\mathfrak{A}_H \subseteq$

H by

$$\mathfrak{A}_H = \{h \in H \mid h.x \in \mathfrak{O}_L \text{ for all } x \in \mathfrak{O}_L\}.$$

Analogously to (2.2.4), $\mathfrak{A}_H$ is the largest order in H for which $\mathfrak{O}_L$ is a module. In fact it is the only order in H over which $\mathfrak{O}_L$ can possibly be a free module, as is implied by the following proposition:

Proposition 2.5.4. Let R be a Dedekind domain with field of fractions K. Let H be a K-Hopf algebra, and Λ an R-order in H. Let $\mathcal{L}$ be a K-algebra which is an H-Galois extension of K, and S an R-order in $\mathcal{L}$. Write

$$\mathfrak{A}_S = \{h \in H \mid h.x \in S \text{ for all } x \in S\}.$$

Suppose S is a free Λ-module of rank one. Then $\Lambda = \mathfrak{A}_S$.

Proof. [Chi00, (12.5)]. Let t be a generator for S over Λ. Then t is a generator for $\mathcal{L}$ over H. Let $\alpha \in \mathfrak{A}_S$. Then $\alpha.t \in S$, so $\alpha.t = h.t$ for some $h \in \Lambda$. Since $\mathcal{L}$ is free over H with generator t, we have $\alpha = h$. Hence $\mathfrak{A}_S = \Lambda$. □

We shall be interested in determining conditions for $\mathfrak{O}_L$ to be a free (or locally free) $\mathfrak{A}_H$-module. The following results give sufficient conditions for this to hold in the local case. We shall make use these in Chapter 3.

Proposition 2.5.5. Let K be a p-adic field and let A be a commutative separable K-algebra. Let $\mathfrak{M}$ be the unique maximal order in A. Let S be a finitely generated projective $\mathfrak{O}_K$-module which is also an $\mathfrak{M}$-module. Suppose that $S \otimes_{\mathfrak{O}_K} K$ is a free A-module of rank one. Then S is a free $\mathfrak{M}$-module of rank one.

Proof. By [CR81a, (26.12)], $\mathfrak{M}$ is a *hereditary order*. That is, every one-sided ideal of $\mathfrak{M}$ is projective as an $\mathfrak{M}$-module. This implies that every finite $\mathfrak{O}_K$-module which is also an $\mathfrak{M}$-module is in fact a projective $\mathfrak{M}$-module. In particular, we may conclude that S is $\mathfrak{M}$-projective. Using the assumptions that K is a p-adic

field, A is commutative and $S \otimes_{\mathfrak{O}_K} K$ is a free A-module, we may conclude (see [CR81a, (35), Exercise 9]) that $S \cong \mathfrak{M}$ as $\mathfrak{M}$-modules. Since $\mathfrak{M}$ is obviously a free $\mathfrak{M}$-module, the result follows. □

Corollary 2.5.6. Let L/K be a finite separable extension of p-adic fields which is Hopf-Galois for some commutative Hopf algebra H. If the associated order $\mathfrak{A}_H$ is the unique maximal order in H, then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.

Theorem 2.5.7. (Childs) Let L/K be a finite H-Galois extension of local fields with rings of integers $\mathfrak{O}_L, \mathfrak{O}_K$ repectively. If the associated order $\mathfrak{A}_H$ is a Hopf order in H, then $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.

Proof. See [Chi00, (12.7)]. □

This striking result is proved in stages in chapter 3 of [Chi00]. We extract a definition and theorem which we shall use explicitly later. The former is a generalisation of the notion of tameness; the latter a generalisation of Noether's theorem applicable Hopf-Galois extensions of Galois algebras.

Definition 2.5.8. Let R be a commutative ring with unity and H a finite cocommutative R-Hopf algebra with module of left integrals I. Let S be a finitely generated projective R algebra. Suppose that S is an H-module algebra such that

$$\{s \in S \mid hs = \varepsilon(h)s \text{ for all } h \in H\} = R.$$

We say that S is a *tame H-extension of R* if

- $\text{rank}_R(S) = \text{rank}_R(H)$.
- S is a faithful H-module.
- $IS = R$.

Theorem 2.5.9. Let R be a local domain with quotient field K of characterstic zero. Let H be a finite cocommutative R-Hopf algebra and S be a finitely generated projective R-algebra. Suppose that S is a tame H-extension of R. Then S is a free H-module of rank one.

Proof. See [Chi00, (13.4)]. □

If in addition to the hypotheses for this theorem we assume that H is a local R-Hopf algebra then a theorem of Childs and Hurley provides an explicit generator of S over H.

Theorem 2.5.10 (**Childs and Hurley**)**.** Let R be a local ring with maximal ideal $\mathfrak{m}$ and H a local, cocommutative R-Hopf algebra with module of integrals $R\theta$. Suppose S is an H-tame extension of R, and let $t \in S$ satisfy $\theta t = 1$. Then $S = Ht$.

Proof. See [Chi00, Theorem 14.7]. □

Remark 2.5.11. In fact it is shown in [Chi00, Theorem 14.7] that when H is a local Hopf algebra over a local domain R, the following three conditions on an H-module algebra S are equivalent:

- S is H-tame.
- S is H-free.
- S is H-Galois.

Chapter 3

Conditions for Freeness over the Associated Order

3.1 Overview

In this chapter we prove the following two theorems regarding extensions of p-adic fields:

Theorem 3.1.1. Let L/K be a finite unramified extension of p-adic fields, and suppose that L/K is H-Galois for some Hopf algebra H. Let $\mathfrak{A}_H \subseteq H$ be the associated order of $\mathfrak{O}_L$. Then $\mathfrak{A}_H$ is a Hopf order in H and $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.

Theorem 3.1.2. Let L/K be a finite (not necessarily Galois) extension of p-adic fields such that $p \nmid [L : K]$. Suppose that L/K is H-Galois for some commutative Hopf algebra H. Let $\mathfrak{A}_H \subseteq H$ be the associated order of $\mathfrak{O}_L$. Then $\mathfrak{A}_H$ is the unique maximal order in H and $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.

We also prove two analogous theorems regarding extensions of number fields:

Theorem 3.1.3. Let L/K be a finite abelian extension of number fields, and suppose that L/K is H-Galois for some Hopf algebra H. Let $\mathfrak{A}_H \subseteq H$ be the

associated order of $\mathfrak{O}_L$. Suppose $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which is unramified in $\mathfrak{O}_L$. Then $\mathfrak{A}_{H,\mathfrak{p}}$ is a Hopf order in $H_{\mathfrak{p}}$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.

Theorem 3.1.4. Let L/K be a finite (not necessarily Galois) extension of number fields, and suppose that L/K is H-Galois for some commutative Hopf algebra H. Let $\mathfrak{A}_H \subseteq H$ be the associated order of $\mathfrak{O}_L$. Suppose that $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ lying above a prime number which does not divide $[L : K]$. Then $\mathfrak{A}_{H,\mathfrak{p}}$ is the unique maximal order in $H_{\mathfrak{p}}$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.

Some immediate corollaries of these theorems follow:

Corollary 3.1.5. Let L/K be a finite abelian Galois extension of number fields, and suppose that L/K is H-Galois for some Hopf algebra H. Then $\mathfrak{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{H,\mathfrak{p}}$ for all primes $\mathfrak{p}$ of $\mathfrak{O}_K$ which are unramified in $\mathfrak{O}_L$. Thus in order to determine whether $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module, it is sufficient to consider the structure of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ for each of the (finitely many) primes $\mathfrak{p}$ which are ramified in $\mathfrak{O}_L$.

Proof. Almost all primes $\mathfrak{p}$ of $\mathfrak{O}_K$ are unramified in $\mathfrak{O}_L$. For each of these, we apply (3.1.3), and conclude that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module. □

Remark 3.1.6. Recall from (2.1.13) that a Galois extension L/K of number fields is called *domestic* if no prime of $\mathfrak{O}_K$ lying above a prime number dividing $[L : K]$ ramifies in $\mathfrak{O}_L$.

Corollary 3.1.7. Let L/K be a finite domestic abelian Galois extension of number fields. 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. By (3.1.5), we have that $\mathfrak{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{H,\mathfrak{p}}$ for any prime $\mathfrak{p}$ of $\mathfrak{O}_K$ which is unramified in $\mathfrak{O}_L$. Suppose $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which is ramified in $\mathfrak{O}_L$. Then $\mathfrak{p}$ lies above a prime number p, and since L/K is domestic, we must have $p \nmid [L : K]$. We may therefore apply (3.1.4), and conclude that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module. □

Corollary 3.1.8. Let L/K be a tamely ramified abelian Galois extension of number fields of prime power degree. 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. By (3.1.7), it is sufficient to observe that since L/K has prime power degree, the assumption that it is tamely ramified is equivalent to the assumption that it is domestic. □

3.2 The $\mathfrak{O}_K$-order $\mathfrak{O}_E[N]^G$

Let L/K be a finite extension of p-adic fields or number fields with Galois closure E. Let $G = \mathrm{Gal}(E/K)$ and $G' = \mathrm{Gal}(E/L)$. Let X be the left coset space G/G' of G' in G. Suppose that L/K is H-Galois for some Hopf algebra H. By Greither and Pareigis's theorem (2.4.9), we have that $H = E[N]^G$ for N some regular subgroup of $\mathrm{Perm}(X)$ normalised by G. Within this algebra, we shall study the $\mathfrak{O}_K$-order $\mathfrak{O}_E[N]^G$.

Proposition 3.2.1. Let L/K be a finite extension of p-adic fields or number fields with Galois closure E, and suppose that L/K is H-Galois for the Hopf algebra $H = E[N]^G$. Then $\mathfrak{O}_E[N]^G \subseteq \mathfrak{A}_H$.

Proof. Let $z \in \mathfrak{O}_E[N]^G$. Then $z \in \mathfrak{O}_E[N]$, so we may write

$$z = \sum_{n \in N} c_n n, \text{ with } c_n \in \mathfrak{O}_E.$$

Since $z \in H$, the action of z on $x \in L$ is given by

$$\left(\sum_{n \in N} c_n n \right).x = \sum_{n \in N} c_n n^{-1}(\overline{1_G})x.$$

Now for each $n \in N$, any group element representing $n^{-1}(\overline{1_G})$ is a Galois automorphism of E, so if $x \in \mathfrak{O}_L$ then $n^{-1}(\overline{1_G})x \in \mathfrak{O}_E$. Therefore for $x \in \mathfrak{O}_L$ we

have

$$z.x = \sum_{n \in N} c_n n^{-1}(\overline{1_G})x \in \mathfrak{O}_E.$$

Since also $z.x \in L$, we have that $z.x \in \mathfrak{O}_E \cap L = \mathfrak{O}_L$, whence $z \in \mathfrak{A}_H$. □

The proofs of the results in this chapter involve showing that under appropriate conditions we have locally the reverse inclusion.

3.3 Unramified Extensions of p-adic Fields

Let L/K be a finite unramified extension of p-adic fields. Then L/K is automatically Galois, with cyclic Galois group, say G. By Greither and Pareigis's theorem (2.4.9), a Hopf algebra H giving a Hopf-Galois structure on L/K is of the form $L[N]^G$ for N some regular subgroup of Perm(G) normalised by G. We shall show that $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$, and that this is a Hopf order in H, which by (2.5.7) is sufficient to prove theorem (3.1.1). We begin with a technical result, which is essentially taken from [Byo97, Lemma 4.5]:

Theorem 3.3.1. (Byott) Let L/K be a finite unramified extension of p-adic fields with Galois group G. Let X be a G-set. Let $\mathfrak{O}_L X$ denote the free $\mathfrak{O}_L$-module on X, with G acting via both $\mathfrak{O}_L$ and X. Then

$$(\mathfrak{O}_L X)^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L = \mathfrak{O}_L X.$$

Proof. We first show that we may reduce to the case where G acts regularly on X. Since L/K is unramified, G is cyclic and therefore abelian, and so this is equivalent to G acting faithfully and transitively. Let $\{X_1, \ldots, X_m\}$ be the orbits of G in X.

Then

$$\begin{aligned}(\mathfrak{O}_L X)^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L &= \left(\bigoplus_{r=1}^{m} \mathfrak{O}_L X_r\right)^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L \\ &= \bigoplus_{r=1}^{m} (\mathfrak{O}_L X_r)^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L\end{aligned}$$

Now let $H_r \triangleleft G$ be the kernel of the action of G on X_r. Let F_r be the fixed field of H_r and let $\Gamma_r = G/H_r \cong \mathrm{Gal}(F_r/K)$. Then Γ_r acts transitively and faithfully on X_r and $(\mathfrak{O}_{F_r} X_r)^{\Gamma_r} = (\mathfrak{O}_L X_r)^G$. Using the above decomposition for $(\mathfrak{O}_L X)^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$, we have reduced to the case where G acts faithfully and transitively, and so regularly, on X. In this case, let $a_1, \ldots, a_n$ be a basis for $\mathfrak{O}_L$ over $\mathfrak{O}_K$, and fix some $x \in X$. Then the elements

$$b_i = \sum_{g \in G} g(a_i)^g x$$

are a basis for $(\mathfrak{O}_L X)^G$ over $\mathfrak{O}_K$. They therefore also form a basis for $(\mathfrak{O}_L X)^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$ over $\mathfrak{O}_L$. Now $\{{}^g x \mid g \in G\}$ is a basis of $\mathfrak{O}_L X$ over $\mathfrak{O}_L$, and so

$$\begin{aligned}[\mathfrak{O}_L X : (\mathfrak{O}_L X)^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L]^2_{\mathfrak{O}_L} &= \det g(a_i)^2 \\ &= \mathrm{Disc}\,(\mathfrak{O}_L/\mathfrak{O}_K)\,,\end{aligned}$$

and this is trivial since L/K is unramified. □

We now show that since L/K is unramified, we in fact have equality in the inclusion established in (3.2.1) above:

Theorem 3.3.2. Let L/K be a finite unramified extension of p-adic fields, and suppose that L/K is H-Galois for the Hopf algebra $H = L[N]^G$. Then $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$.

Proof. By (3.2.1), $\mathfrak{O}_L[N]^G \subseteq \mathfrak{A}_H$. On the other hand, since L/K is unramified, we have that $\mathfrak{O}_L \otimes_{\mathfrak{O}_K} \mathfrak{O}_L \cong \mathfrak{O}_L^{[L:K]}$, and this is the ring of integers of $L \otimes_K L \cong L^{[L:K]}$.

The L-algebra $H \otimes_K L \cong L[N]$ acts on $L \otimes_K L$, with associated order $\mathfrak{O}_L[N]$. Since $\mathfrak{A}_H \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$ also acts on $\mathfrak{O}_L \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$, we conclude that

$$\mathfrak{A}_H \otimes_{\mathfrak{O}_K} \mathfrak{O}_L \subseteq \mathfrak{O}_L[N].$$

So by (3.3.1) we have

$$\mathfrak{A}_H \otimes_{\mathfrak{O}_K} \mathfrak{O}_L \subseteq \mathfrak{O}_L[N]^G \otimes_{\mathfrak{O}_K} \mathfrak{O}_L,$$

and therefore

$$\mathfrak{A}_H \subseteq \mathfrak{O}_L[N]^G.$$

Hence $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$. □

We now use this explicit description of $\mathfrak{A}_H$ to show that $\mathfrak{A}_H$ is in fact a Hopf order. By (2.4.13), it is sufficient to prove that the comultiplication on H restricts to $\mathfrak{A}_H$.

Theorem 3.3.3. Let L/K be a finite unramified extension of p-adic fields, and suppose that L/K is H-Galois for the Hopf algebra $H = L[N]^G$. Then $\mathfrak{A}_H$ is a Hopf order in H.

Proof. By (3.3.2), $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$. As in the proof of (3.3.1), we may reduce to the case where G acts regularly on some orbit X - in general this is not a group, but is still a finite G-set. In this case, it is sufficient to show that we have

$$\Delta\left((\mathfrak{O}_L X)^G\right) \subseteq (\mathfrak{O}_L X)^G \otimes (\mathfrak{O}_L X)^G.$$

Let $a_1, \ldots, a_n$ be a basis for $\mathfrak{O}_L$ over $\mathfrak{O}_K$, and fix some $x \in X$. Then as in the proof of (3.3.1), the elements

$$b_i = \sum_{g \in G} (g a_i)({}^g x) \quad i = 1, \ldots, n$$

are a basis for $(\mathfrak{O}_L X)^G$ over $\mathfrak{O}_K$. For each $i = 1, \ldots, n$ we require that $\Delta(b_i) \in (\mathfrak{O}_L X)^G \otimes (\mathfrak{O}_L X)^G$. Since Δ is L-linear, we have

$$\Delta(b_i) = \sum_{g \in G} g(a_i)({}^g x \otimes {}^g x) \quad i = 1, \ldots, n.$$

This is fixed under the action of $G \times G$ on $LX \otimes_L LX$ since $b_i \in H$. Additionally, since L/K is unramified we have $\det(g(a_i)) \in \mathfrak{O}_K^\times$, so $\Delta(b_i) \in \mathfrak{O}_L X \otimes_{\mathfrak{O}_L} \mathfrak{O}_L X$. Thus $\Delta(b_i) \in (\mathfrak{O}_L X)^G \otimes_{\mathfrak{O}_K} (\mathfrak{O}_L X)^G$. □

We now restate and prove (3.1.1):

Corollary 3.3.4. Let L/K be a finite unramified extension of p-adic fields, and suppose that L/K is Hopf-Galois for some Hopf algebra H. Let $\mathfrak{A}_H \subseteq H$ be the associated order of $\mathfrak{O}_L$. Then $\mathfrak{A}_H$ is a Hopf order in H and $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.

Proof. By (3.3.3), $\mathfrak{A}_H$ is a Hopf order in H. Now apply (2.5.7). □

3.4 Unramified Completions of Number Fields

Let L/K be a finite abelian Galois extension of number fields, and suppose that L/K is Hopf-Galois for some Hopf algebra $H = L[N]^G$. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which is unramified in $\mathfrak{O}_L$. In this section we prove (3.1.3) - that $\mathfrak{A}_{H,\mathfrak{p}}$ is a Hopf order in $H_\mathfrak{p}$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module. Motivated by (3.3.2) we consider the $\mathfrak{O}_{K,\mathfrak{p}}$-order $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ in $H_\mathfrak{p}$.

Proposition 3.4.1. The $\mathfrak{O}_{K,\mathfrak{p}}$-order $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order in $H_\mathfrak{p}$.

Proof. This follows the proof of (3.3.3). Note that in this case we have explicitly assumed that G is abelian, so any faithful transitive action of a subgroup or quotient group of G is regular. □

We now restate and prove (3.1.3):

Proposition 3.4.2. The $\mathfrak{O}_{K,\mathfrak{p}}$-order $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ coincides with the completed associated order $\mathfrak{A}_{H,\mathfrak{p}}$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$-module.

Proof. By (3.4.1), $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order in $H_{\mathfrak{p}}$. We note that the trace element

$$\theta = \sum_{n \in N} n$$

is a left integral of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$, and since $\mathfrak{p}$ is unramified in $\mathfrak{O}_L$ there exists an element $t \in \mathfrak{O}_{L,\mathfrak{p}}$ such that $\theta.t = 1$. Thus $\mathfrak{O}_{L,\mathfrak{p}}$ is an $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$-tame extension of $\mathfrak{O}_{K,\mathfrak{p}}$ (see (2.5.8)). Now by (2.5.9) we have that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$-module. Thus by (2.5.4) we have $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$. □

3.5 Maximal Associated Orders

Let L/K be a finite extension of p-adic fields which is H-Galois for some commutative Hopf algebra H. In this section we determine a sufficient condition for the associated order $\mathfrak{A}_H$ to be the unique maximal order in H. When this occurs, it follows by (2.5.5) that $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module, as asserted in (3.1.2). Let E be the Galois closure of L/K with $G = \mathrm{Gal}(E/K)$, and let $G' = \mathrm{Gal}(E/L)$. Let X be the left coset space G/G' of G' in G. By Greither and Pareigis's theorem (2.4.9) we have that $H = E[N]^G$ for some abelian regular subgroup N of $\mathrm{Perm}(X)$ normalised by G. We begin by giving a sufficient condition for the integral group ring $\mathfrak{O}_E[N]$ to be the maximal order of the group algebra $E[N]$.

Proposition 3.5.1. Let E be a p-adic field with ring of integers $\mathfrak{O}_E$ and let N be a finite group. Suppose that $p \nmid |N|$. Then $\mathfrak{O}_E[N]$ is a maximal order in $E[N]$. In particular, if N is abelian then $\mathfrak{O}_E[N]$ is the unique maximal order in $E[N]$.

Proof. Since $p \nmid |N|$ we have $|N| \in \mathfrak{O}_E^\times$ and therefore $\mathfrak{O}_E[N]$ is a maximal order in $E[N]$ by (2.1.6). If N is abelian, then the maximal order is unique by (2.1.5). □

We now show that, in the situation described at the start of the section, if N is abelian and $\mathfrak{O}_E[N]$ is the unique maximal order in $E[N]$ then taking the fixed points under the action by G preserves this maximality, so that $\mathfrak{O}_E[N]^G$ is the unique maximal order in $E[N]^G$.

Proposition 3.5.2. Let E/K be a finite Galois extension of p-adic fields with group G and rings of integers $\mathfrak{O}_E, \mathfrak{O}_K$ respectively. Let N be a finite abelian group which is a G-set, and suppose that $p \nmid |N|$. Let G act on the group algebra $E[N]$ by acting via both E and N. Then $\mathfrak{O}_E[N]^G$ is the unique maximal $\mathfrak{O}_K$-order in the K-algebra $E[N]^G$.

Proof. Since N is abelian, by (2.1.5), $E[N]$ has a unique maximal $\mathfrak{O}_E$-order and $E[N]^G$ has a unique maximal $\mathfrak{O}_K$-order. Since $p \nmid |N|$ we have $p \in \mathfrak{O}_K^\times \subseteq \mathfrak{O}_E^\times$ and so the maximal $\mathfrak{O}_E$ order in $E[N]$ is $\mathfrak{O}_E[N]$ by (3.5.1). Denote by $\mathfrak{M}$ the maximal $\mathfrak{O}_K$-order in $E[N]^G$, and let $x \in \mathfrak{M}$. By (2.1.5) x is integral over $\mathfrak{O}_K$ in $E[N]^G$, so x is integral over $\mathfrak{O}_E$ in $E[N]$, whence $x \in \mathfrak{O}_E[N]$. So $x \in E[N]^G \cap \mathfrak{O}_E[N] = \mathfrak{O}_E[N]^G$. So $\mathfrak{O}_E[N]^G = \mathfrak{M}$. □

We now restate and prove (3.1.2):

Theorem 3.5.3. Let L/K be a finite (not necessarily Galois) extension of p-adic fields such that $p \nmid [L : K]$. Suppose that L/K is H-Galois for some commutative Hopf algebra H. Let $\mathfrak{A}_H \subseteq H$ be the associated order of $\mathfrak{O}_L$. Then $\mathfrak{A}_H$ is the unique maximal order in H and $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module.

Proof. Write $H = E[N]^G$. By (3.5.2), $\mathfrak{O}_E[N]^G$ is the unique maximal order in H. On the other hand, by (3.2.1) $\mathfrak{O}_E[N]^G \subseteq \mathfrak{A}_H$. So $\mathfrak{O}_E[N]^G = \mathfrak{A}_H$ is the maximal $\mathfrak{O}_K$-order in H and therefore by (2.5.5), $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module. □

3.6 Locally Maximal Associated Orders

Let L/K be a finite extension of number fields with Galois closure E. Suppose L/K is H-Galois for some commutative Hopf algebra $H = E[N]^G$. In this section we prove (3.1.4) by generalising the results of the previous section.

Proposition 3.6.1. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above a prime number p which does not divide $[L : K]$. Then $\mathfrak{A}_{H,\mathfrak{p}}$ is the unique maximal order in $H_\mathfrak{p}$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.

Proof. Let $\mathfrak{M}$ denote the unique maximal $\mathfrak{O}_K$-order in H, so that $\mathfrak{M}_\mathfrak{p}$ is the unique maximal $\mathfrak{O}_{K,\mathfrak{p}}$-order in $H_\mathfrak{p}$. Let $x \in \mathfrak{M}_\mathfrak{p}$. Then $x \in E_\mathfrak{p}[N]^G$, so $x \in E_\mathfrak{p}[N]$. Recall from (2.1.15) the isomorphism

$$E_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} E_\mathfrak{P},$$

where the $\mathfrak{P}$ are the primes of $\mathfrak{O}_E$ which lie above $\mathfrak{p}$. This induces an isomorphism

$$E_\mathfrak{p}[N] \cong \prod_{\mathfrak{P}|\mathfrak{p}} E_\mathfrak{P}[N],$$

where each factor on the right is a group algebra over a p-adic field whose residue characteristic is coprime to $|N|$. Now x is integral over $\mathfrak{O}_{K,\mathfrak{p}}$ in $H_\mathfrak{p}$, so x lies in the set of elements of $E_\mathfrak{p}[N]$ which are integral over $\mathfrak{O}_{K,\mathfrak{p}}$. The image of this set under the isomorphism above is contained in the product

$$\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{M}_{E_\mathfrak{P}[N]},$$

where each $\mathfrak{M}_{E_\mathfrak{P}[N]}$ is the unique maximal order in the group algebra $E_\mathfrak{P}[N]$. Since $\mathfrak{p}$ lies above a prime number which does not divide $[L : K] = |N|$, by (2.1.6) we

have that $\mathfrak{M}_{E_{\mathfrak{P}}[N]} = \mathfrak{O}_{E,\mathfrak{P}}[N]$ for each $\mathfrak{P} \mid \mathfrak{p}$. Thus

$$\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{M}_{E_{\mathfrak{P}}[N]} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{E,\mathfrak{P}}[N] \cong \mathfrak{O}_{E,\mathfrak{p}}[N],$$

and so $x \in \mathfrak{O}_{E,\mathfrak{p}}[N] \cap E_{\mathfrak{p}}[N]^G = \mathfrak{O}_{E,\mathfrak{p}}[N]^G$. Therefore $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{O}_{E,\mathfrak{p}}[N]^G$ and so $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{M}_{\mathfrak{p}}$. Finally, by (2.5.5) we have that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module. □

Chapter 4

Tamely Ramified $C_p \times C_p$ Extensions

For the remainder of this thesis, we shall study a tamely ramified Galois extension L/K of number fields with group isomorphic to $C_p \times C_p$, where p is a prime number. We shall assume that K contains a primitive p^{th} root of unity ζ; such extensions then have the form $L = K(\alpha, \beta)$, with $\alpha^p = a \in K^\times/K^{\times p}$ and $\beta^p = b \in K^\times/K^{\times p}$. In this chapter we derive congruence conditions on a and b which are equivalent to L/K being tamely ramified. For each prime $\mathfrak{p}$ of $\mathfrak{O}_K$, we also calculate explicit integral bases for $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$. We begin by classifying extensions of p-adic fields having degree p.

4.1 Local Extensions of Degree p

Theorem 4.1.1. Let p be a prime number and let L/K be a Galois extension of p-adic fields with group $G \cong C_p$. Let ζ be a primitive p^{th} root of unity in K. Write $L = K(\alpha)$, with $\alpha^p = a \in \mathfrak{O}_K$. Set $e = v_K(p), e' = e/(p-1) = v_K(\zeta - 1)$. Let π be a uniformiser for K. Then we may choose α so that one of the following holds for some $u \in \mathfrak{O}_K^\times$:

(i) $\alpha^p = u\pi$.

(ii) $\alpha^p = 1 + u\pi^k$, with $1 \leq k = pq + r < pe'$ and $0 < r \leq p - 1$.

(iii) $\alpha^p = 1 + u\pi^{pe'}$.

Proof. [Chi00, (24.2)]. Suppose first that $L = K(\beta)$ with $\beta^p = u\pi^d$. If $p \nmid d$ then we can find an s such that $sd = 1 + pq$, and taking $\alpha = \beta^s/\pi^q$ yields $\alpha^p = u^s\pi$. We still have $L = K(\alpha)$, and so this is case (i). If $p \mid d$ then write $d = pt$ and set $\alpha = \beta/\pi^t$. Then $\alpha^p = u \in \mathfrak{O}_K^\times$. We can thus reduce to this case. Suppose that $L = K(\beta)$ with $\beta^p = u \in \mathfrak{O}_K^\times$. Then since $\mathfrak{O}_K/\pi\mathfrak{O}_K$ is a finite field of characteristic p, there exists some $v \in \mathfrak{O}_K^\times$ such that $v^p \equiv u^{-1} \pmod{\pi\mathfrak{O}_K}$. Set $\alpha_1 = v\beta$. Then $\alpha_1^p = uv^p \equiv 1 \pmod{\pi\mathfrak{O}_K}$. So now suppose that $\alpha_1^p = 1 + u\pi^{pq+r}$, where $u \in \mathfrak{O}_K^\times$ and $0 < pq + r, 0 \leq r \leq p - 1$. Suppose $r = 0$. Set $c = 1 + v\pi^q$ where $q \neq 0$ and $v^p \equiv -u \pmod{\pi\mathfrak{O}_K}$. Let $\alpha_2 = c\alpha_1$. Then

$$\begin{aligned}
\alpha_2^p &= (\alpha_1 c)^p \\
&= (1 + u\pi^{pq})(1 + v\pi^q)^p \\
&= (1 + u\pi^{pq})\left(1 + \sum_{k=1}^{p-1}\binom{p}{k}v^k\pi^{qk} + v^q\pi^{pq}\right) \\
&= 1 + (u + v^p)\pi^{pq} + uv^p\pi^{2pq} + p\pi^q w
\end{aligned}$$

for some $w \in \mathfrak{O}_K$. If $pq < (p-1)e' + q$ (i.e. $q < e'$), then $v_K(\alpha_2^p - 1) > v_K(\alpha_1^p - 1)$. We may repeat this construction as needed, and so find α such that $L = K(\alpha)$ and $\alpha^p = 1 + u\pi^{pq+r}$ with $u \in \mathfrak{O}_K^\times$ and either $1 \leq r \leq p - 1$ (case (ii)) or $pq + r \geq pe'$. If we have equality here then this is case (iii). Otherwise $a = \alpha^p$ is a p^{th} power in K by Hensel's lemma, whence $\alpha \in K$ since $\zeta \in K$, and we do not have a proper extension. □

We now examine the ramification in each of the cases (i)-(iii) in the proposition above:

Proposition 4.1.2. If $L = K(\alpha)$ with $\alpha^p = u\pi$ for some $u \in \mathfrak{O}_K^\times$, then L/K is totally ramified and $\mathfrak{O}_L = \mathfrak{O}_K[\alpha]$.

Proof. The polynomial $x^p - u\pi$ is an Eisenstein polynomial and is satisfied by α, so L/K is totally ramified and α is a uniformizer for $\mathfrak{O}_L$ over $\mathfrak{O}_K$. See [FT91, Theorem 24] □

Proposition 4.1.3. If $L = K(\alpha)$ with $\alpha^p = 1 + u\pi^{pe'}$ for some $u \in \mathfrak{O}_K^\times$, then L/K is unramified, and $\mathfrak{O}_L = \mathfrak{O}_K\left[\frac{\alpha-1}{\zeta-1}\right]$.

Proof. [Chi00, (24.4)] Let $\lambda = \zeta - 1$ and $x = \frac{\alpha-1}{\lambda}$. Then $\alpha = 1 + \lambda x$, and so

$$1 + u\pi^{pe'} = \alpha^p = \sum_{k=0}^{p-1} \binom{p}{k} \lambda^k x^k + \lambda^p x^p.$$

Now note that $v_K(\lambda) = e'$, so $v_K(\lambda^p) = pv_K(\lambda) = pe'$. So subtracting 1 from each side of the equation above and dividing by λ^p we obtain

$$u\frac{\pi^{pe'}}{\lambda^p} = x^p + \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k}\frac{p\lambda^k x^k}{\lambda^p},$$

implying that x satisfies a monic polynomial in $\mathfrak{O}_K[t]$, whence $\mathfrak{O}_K[x] \subseteq \mathfrak{O}_L$. Now let σ be a generator for G satisfying $\sigma(\alpha) = \zeta\alpha$. Then

$$\sigma\left(\frac{\alpha-1}{\lambda}\right) = \frac{\zeta\alpha - 1}{\lambda} = \frac{(\zeta-1)\alpha}{\lambda} + \frac{\alpha-1}{\lambda},$$

so $\sigma(x) = \alpha + x$. Since α is a unit of $\mathfrak{O}_K[x]$, the inertia group

$$G_0 = \{\tau \in G \mid \tau(x) \equiv x \pmod{\mathfrak{m}} \text{ for all maximal ideals } \mathfrak{m} \text{ of } \mathfrak{O}_K[x]\}$$

is trivial, which is equivalent to $\mathfrak{O}_K[x]$ being unramified over $\mathfrak{O}_K$. (See [Chi00, (2.5)]). Therefore $\mathrm{Disc}\,(\mathfrak{O}_K[x]) = \mathfrak{O}_K$. But since $\mathfrak{O}_K[x] \subseteq \mathfrak{O}_L$, $\mathrm{Disc}\,(\mathfrak{O}_K[x]) \subseteq \mathrm{Disc}\,(\mathfrak{O}_L) \subseteq \mathfrak{O}_K$. So $\mathrm{Disc}\,(\mathfrak{O}_L) = \mathfrak{O}_K$ and therefore $\mathfrak{O}_K[x] = \mathfrak{O}_L$ and L/K is

unramified. □

Proposition 4.1.4. If $L = K(\alpha)$ with $\alpha^p = 1 + u\pi^k$ for some $u \in \mathfrak{O}_K^\times$ and $k = pq + 1 < pe'$, then L/K is totally ramified and $\mathfrak{O}_L = \mathfrak{O}_K\left[\frac{\alpha-1}{\pi^q}\right]$.

Proof. See [Chi00, Corollary 24.8]. □

4.2 Tame $C_p \times C_p$ Extensions of Number Fields

Throughout, let p be a prime number and let K be a number field containing a primitive p^{th} root of unity ζ. The Galois extensions of K with group $G \cong C_p \times C_p$ are then of the form $L = K(\alpha, \beta)$, with $\alpha^p = a$ and $\beta^p = b$ linearly independent elements of the $\mathbb{F}_p$-vector space $K^\times/K^{\times p}$.

Proposition 4.2.1. Let $L = K(\alpha, \beta)$. Then L/K is tamely ramified if and only if both $K(\alpha)/K$ and $K(\beta)/K$ are tamely ramified.

Proof. Since $[L : K] = p^2$, the extension L/K is tamely ramified if and only if no prime $\mathfrak{p}$ of $\mathfrak{O}_K$ lying above p is ramified. A prime $\mathfrak{p}$ of $\mathfrak{O}_K$ is ramified in $\mathfrak{O}_L$ if and only if it divides the discriminant $\mathrm{Disc}\,(L/K)$. Since L is the compositum of $K(\alpha)$ and $K(\beta)$, a prime $\mathfrak{p}$ divides $\mathrm{Disc}\,(L/K)$ if and only if it divides $\mathrm{Disc}\,(K(\alpha)/K)\,\mathrm{Disc}\,(K(\beta)/K)$ (See [Mol99, Theorem 4.67]). Therefore $\mathfrak{p}$ divides $\mathrm{Disc}\,(L/K)$ if and only if it divides either $\mathrm{Disc}\,(K(\alpha)/K)$ or $\mathrm{Disc}\,(K(\beta)/K)$, i.e. L/K is tamely ramified if and only if both $K(\alpha)/K$ and $K(\beta)/K$ are tamely ramified. □

For each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ which lies above p, we write $e_\mathfrak{p} = v_\mathfrak{p}(p)$. Since $\zeta \in \mathfrak{O}_K$, we have $e_\mathfrak{p} = (p-1)e'_\mathfrak{p}$ where $e'_\mathfrak{p} = v_\mathfrak{p}(\zeta - 1)$. Where there is no danger of confusion we shall write simply e and e'.

Proposition 4.2.2. The extension $K(\alpha)/K$ is tamely ramified if and only if $a = \alpha^p$ can be chosen to satisfy $a \equiv 1 \pmod{(\zeta-1)^p}^*$. (That is, $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}((\zeta-1)^p)$ for all $\mathfrak{p} \mid (\zeta-1)\mathfrak{O}_K$, but possibly $\alpha \notin \mathfrak{O}_K$.)

Proof. Since $[K(\alpha) : K] = p$, the extension is tamely ramified if and only if no prime $\mathfrak{p}$ lying above p ramifies. That is, for such a prime, each prime $\mathfrak{P}$ of $\mathfrak{O}_{K(\alpha)}$ lying above $\mathfrak{p}$ the completion $K(\alpha)_{\mathfrak{P}}/K_{\mathfrak{p}}$ is of the form given in case (iii) of (4.1.1), and therefore unramified by (4.1.3). So the extension is tamely ramified if and only if we can choose $a = \alpha^p$ such that for each $\mathfrak{p} \mid p\mathfrak{O}_K$, we have $a = 1 + u\pi_{\mathfrak{p}}^{pe'} \in \mathfrak{O}_{K,\mathfrak{p}}$ for some $u \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. If we can choose a in this way for each prime $\mathfrak{p}$ lying above p then by the Chinese Remainder Theorem (see [FT91, Theorem 4]) we can choose a such that the condition is satisfied for all such $\mathfrak{p}$ simultaneously. Finally, we note that for each such prime $v_{\mathfrak{p}}((\zeta - 1)^p) = pe'$, giving the congruence condition in the proposition. □

Proposition 4.2.3. If the extension $K(\alpha)/K$ is tamely ramified then without loss of generality we may assume that $a = \alpha^p \in \mathfrak{O}_K$.

Proof. By the Chinese Remainder Theorem (see [FT91, Theorem 4]) we may pick an element $l \in \mathfrak{O}_K$ satisfying the following conditions:

- $l \equiv 1 \pmod{(\zeta - 1)^p}$ for $\mathfrak{p} \mid p\mathfrak{O}_K$.
- $v_{\mathfrak{p}}(l) \geq v_{\mathfrak{p}}(a)$ for $\mathfrak{p} \nmid p\mathfrak{O}_K$.

This is a finite list of conditions since $v_{\mathfrak{p}}(a) = 0$ for almost all primes $\mathfrak{p}$. Then we can write $a = l/m$, where $m = l/a$. Then $m \in \mathfrak{O}_K$, for $m \equiv 1 \pmod[*]{(\zeta - 1)^p}$, and if $\mathfrak{p} \nmid p\mathfrak{O}_K$ then $v_{\mathfrak{p}}(m) = v_{\mathfrak{p}}(l) - v_{\mathfrak{p}}(a) \geq 0$. So we have $a = lm^{p-1}/m^p$, and if we define $a' = m^p a$ and $(\alpha')^p = a'$ then we have

- $a' \in \mathfrak{O}_K$
- $a' \equiv 1 \pmod{(\zeta - 1)^p}$
- $K(\alpha') = K(\alpha)$.

hence we may replace a with a'. □

Corollary 4.2.4. Let $L = K(\alpha, \beta)$. Then L/K is tamely ramified if and only if $a = \alpha^p$ and $b = \beta^p$ can be chosen to satisfy $a \equiv b \equiv 1 \pmod{(\zeta - 1)^p}$.

Proof. This is clear upon combining (4.2.1), (4.2.2) and (4.2.3). □

4.3 Local Integral Bases

Definition 4.3.1. For $x \in K^\times$ and $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, define $r_\mathfrak{p}(x)$ by

$$r_\mathfrak{p}(x) = \left\lfloor \frac{v_\mathfrak{p}(x)}{p} \right\rfloor = \max\left\{ n \in \mathbb{Z} \mid n \leq \frac{v_\mathfrak{p}(x)}{p} \right\}.$$

Proposition 4.3.2. Let $L = K(\alpha, \beta)$ with $\alpha^p = a, \beta^p = b$ and $a, b \in \mathfrak{O}_K/\mathfrak{O}_K^p$. Suppose a and b satisfy the congruence conditions of (4.2.4), so that L/K is tamely ramified. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which does not lie above p. Then the following is an $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{O}_{L,\mathfrak{p}}$.

$$\left\{ \frac{\alpha^i \beta^j}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^i b^j)}} \mid 0 \leq i, j \leq p-1 \right\}$$

Proof. Consider first the subextension $K(\alpha)/K$, with $\mathrm{Gal}(K(\alpha)/K) \cong C_p$. Let σ be a generator of $\mathrm{Gal}(K(\alpha)/K)$ satisfying $\sigma(\alpha) = \zeta\alpha$. Let

$$\omega = \left\{ \frac{\alpha^i}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^i)}} \mid 0 \leq i \leq p-1 \right\}.$$

Suppose first that $v_\mathfrak{p}(a) \equiv 0 \pmod{p}$. Then

$$\begin{aligned} \mathrm{Disc}(\omega) &= \det\left(\sigma^s \left(\frac{\alpha^i}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^i)}} \right) \right)^2 \\ &= \left(\prod_{i=0}^{p-1} \pi_\mathfrak{p}^{-2r_\mathfrak{p}(a^i)} \right) \det\left(\sigma^s\left(\alpha^i\right) \right)^2 \end{aligned}$$

We examine the two terms separately. Firstly we have

$$\begin{aligned}\det\left(\sigma^s\left(\alpha^i\right)\right)^2 &= \det\left(\zeta^{is}\alpha^i\right)^2 \\ &= \alpha^{\frac{2p(p-1)}{2}}\det\left(\zeta^{is}\right)^2.\end{aligned}$$

Now,

$$\begin{aligned}\det\left(\zeta^{is}\right) &= \prod_{0\le i<s\le p-1}\left(\zeta^s-\zeta^i\right) \\ &= \prod_{0\le i<s\le p-1}\zeta^i\left(\zeta^{s-i}-1\right) \\ &= \prod_{0\le i<s\le p-1}\zeta^i\prod_{0\le i<s\le p-1}\left(\zeta^{s-i}-1\right)\end{aligned}$$

The first term of this is a global unit, and the second is divisible only by primes lying above p. Therefore,

$$\det\left(\sigma^s\left(\alpha^i\right)\right)^2 \sim a^{(p-1)}.$$

On the other hand, we have

$$\begin{aligned}v_{\mathfrak{p}}\left(\prod_{i=0}^{p-1}\pi_{\mathfrak{p}}^{-2r_{\mathfrak{p}}(a^i)}\right) &= -2\sum_{i=0}^{p-1}r_{\mathfrak{p}}(a^i) \\ &= -\frac{2}{p}\sum_{i=0}^{p-1}v_{\mathfrak{p}}\left(a^i\right) \\ &= -\frac{2}{p}v_{\mathfrak{p}}\left(a\right)\sum_{i=0}^{p-1}i \\ &= -\frac{2}{p}\frac{p(p-1)}{2}v_{\mathfrak{p}}\left(a\right) \\ &= -(p-1)v_{\mathfrak{p}}\left(a\right) \\ &= -v_{\mathfrak{p}}\left(a^{(p-1)}\right).\end{aligned}$$

So $\mathrm{Disc}\left(\omega\right) = \mathfrak{O}_{K,\mathfrak{p}}$, and so ω is an integral basis for $\mathfrak{O}_{K(\alpha),\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$.

Suppose now that $\gcd(v_{\mathfrak{p}}(a), p) = 1$. Then $\mathfrak{p}$ is ramified in $K(\alpha)/K$, and so $\mathfrak{p}\mathfrak{O}_{K(\alpha)} = \mathfrak{P}^p$ for some prime ideal $\mathfrak{P}$ of $\mathfrak{O}_{K(\alpha)}$. Then

$$pv_{\mathfrak{p}}(a) = v_{\mathfrak{P}}(a) = v_{\mathfrak{P}}(\alpha^p) = pv_{\mathfrak{P}}(\alpha),$$

and so

$$v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{p}}(a).$$

We therefore have

$$\begin{aligned} v_{\mathfrak{P}}\left(\frac{\alpha^i}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^i)}}\right) &= v_{\mathfrak{P}}\left(\alpha^i\right) - v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^i)}\right) \\ &= v_{\mathfrak{P}}\left(\alpha^i\right) - pv_{\mathfrak{p}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^i)}\right) \\ &= v_{\mathfrak{P}}\left(\alpha^i\right) - pr_{\mathfrak{p}}(a^i) \\ &= v_{\mathfrak{p}}\left(a^i\right) - pr_{\mathfrak{p}}(a^i) \\ &\equiv iv_{\mathfrak{p}}(a) \pmod{p}, \end{aligned}$$

and since $\gcd(v_{\mathfrak{p}}(a), p) = 1$, this ranges over all residues modulo p as i varies. So ω contains a basis element of $\mathfrak{P}$-valuation k for each $0 \leq k \leq p-1$, and so ω is an integral basis of $\mathfrak{O}_{K(\alpha),\mathfrak{p}}$ over $\mathfrak{O}_{K,\mathfrak{p}}$. Analogous results for the subextension $K(\beta)/K$ follow by symmetry. If we consider $L = K(\alpha, \beta)$, there are three possible cases:

i) If $v_{\mathfrak{p}}(a) \equiv v_{\mathfrak{p}}(b) \equiv 0 \pmod{p}$, then

$$\mathrm{Disc}\left(\mathfrak{O}_{K(\alpha),\mathfrak{p}}/\mathfrak{O}_{K,\mathfrak{p}}\right) = \mathrm{Disc}\left(\mathfrak{O}_{K(\beta),\mathfrak{p}}/\mathfrak{O}_{K,\mathfrak{p}}\right) = \mathfrak{O}_{K,\mathfrak{p}},$$

and the extensions are arithmetically disjoint at $\mathfrak{p}$ (see [FT91, III, (2.13)]), whence $\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K(\alpha),\mathfrak{p}}\mathfrak{O}_{K(\beta),\mathfrak{p}}$.

ii) If exactly one of $v_{\mathfrak{p}}(a) \equiv 0 \pmod{p}$ and $v_{\mathfrak{p}}(b) \equiv 0 \pmod{p}$ holds, then

$$\gcd\left(\mathrm{Disc}\left(\mathfrak{O}_{K(\alpha),\mathfrak{p}}/\mathfrak{O}_{K,\mathfrak{p}}\right), \mathrm{Disc}\left(\mathfrak{O}_{K(\beta),\mathfrak{p}}/\mathfrak{O}_{K,\mathfrak{p}}\right)\right) = \mathfrak{O}_{K,\mathfrak{p}},$$

and again the extensions are arithmetically disjoint at $\mathfrak{p}$, whence $\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K(\alpha),\mathfrak{p}}\mathfrak{O}_{K(\beta),\mathfrak{p}}$.

iii) If both $v_{\mathfrak{p}}(a) \not\equiv 0 \pmod{p}$ and $v_{\mathfrak{p}}(b) \not\equiv 0 \pmod{p}$, then there exist integers m, n such that

$$mv_{\mathfrak{p}}(a) + nv_{\mathfrak{p}}(b) \equiv 0 \pmod{p}.$$

If we consider the elements

$$\left(\frac{\alpha^i}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^i)}}\right), \left(\frac{\alpha^{mj}\beta^{nj}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^{mj}b^{nj})}}\right) \quad 0 \le i, j \le p-1,$$

then we are again in case (ii).

All of these cases yield the description of $\mathfrak{O}_{L,\mathfrak{p}}$ given in the proposition. □

Proposition 4.3.3. Let $L = K(\alpha, \beta)$ with $\alpha^p = a, \beta^p = b$ and $a, b \in \mathfrak{O}_K^\times/\mathfrak{O}_K^{\times p}$. Suppose a and b satisfy the congruence conditions of (4.2.4), so that L/K is tamely ramified. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above p. Let $v_{\mathfrak{p}}(p) = e = (p-1)e'$. Then the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$.

$$\left\{\left(\frac{\alpha-1}{\pi_{\mathfrak{p}}^{e'}}\right)^i \left(\frac{\beta-1}{\pi_{\mathfrak{p}}^{e'}}\right)^j \mid 0 \le i, j \le p-1\right\}.$$

Proof. Consider first the subextension $K(\alpha)/K$. By (4.1.3) we have that an $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{O}_{K(\alpha),\mathfrak{p}}$ is

$$\left\{\left(\frac{\alpha-1}{\pi_{\mathfrak{p}}^{e'}}\right)^i \mid 0 \le i \le p-1\right\},$$

and the local extension $K(\alpha)_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified, so $\mathrm{Disc}\left(\mathfrak{O}_{K(\alpha),\mathfrak{p}}/\mathfrak{O}_{K,\mathfrak{p}}\right) = \mathfrak{O}_{K,\mathfrak{p}}$. Analogous results for the subextension $K(\beta)/K$ follow by symmetry. Since both

the subextensions $K(\alpha)_{\mathfrak{p}}$ and $K(\beta)_{\mathfrak{p}}$ are unramified, they are arithmetically disjoint at $\mathfrak{p}$, and so we obtain

$$\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K(\alpha),\mathfrak{p}}\mathfrak{O}_{K(\beta),\mathfrak{p}},$$

which yields the description of $\mathfrak{O}_{L,\mathfrak{p}}$ in the proposition. □

Remark 4.3.4. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ and consider the subextension $K(\alpha)/K$ of L/K. Let σ be a generator for $G = \mathrm{Gal}(K(\alpha)/K)$ such that $\sigma(\alpha) = \zeta\alpha$. If $\mathfrak{p}$ is split in $K(\alpha)/K$, then locally we have, by (2.1.14),

$$K(\alpha)_{\mathfrak{p}} \cong \prod_{\mathfrak{P}|\mathfrak{p}} K(\alpha)_{\mathfrak{P}},$$

where for each $\mathfrak{P} \mid \mathfrak{p}$, we have $K(\alpha)_{\mathfrak{P}} \cong K_{\mathfrak{p}}$, and so locally $\alpha \in K_{\mathfrak{p}}$. If now we fix some prime $\mathfrak{P} \mid \mathfrak{p}$, then we have

$$K(\alpha)_{\mathfrak{p}} \cong \prod_{r=0}^{p-1} K(\alpha)_{\sigma^r(\mathfrak{P})}.$$

Under this isomorphism we have

$$\begin{aligned} \alpha &\mapsto \left(\alpha, \sigma\alpha, \ldots, \sigma^{p-1}\alpha\right) \\ &= \left(\alpha, \zeta\alpha, \ldots, \zeta^{p-1}\alpha\right), \end{aligned}$$

so we must interpret α as a tuple of elements of $K_{\mathfrak{p}}$. We shall often tacitly make use of this convention in what follows.

Chapter 5

Hopf-Galois Structures on $C_p \times C_p$ Extensions

Let p be a prime number. We continue to denote by K a number field containing a primitive p^{th} root of unity ζ, and by L/K a tame Galois extension with group $G \cong C_p \times C_p$. In order to study the Hopf-Galois module structure of $\mathfrak{O}_L$, we shall need information about the Hopf-Galois structures admitted by the extension. Here we reproduce results from [Byo96] where it is shown that there are precisely p^2 structures. For odd p they all have type $C_p \times C_p$, whilst for $p = 2$ the classical structure has type $C_2 \times C_2$ and the nonclassical structures all have type C_4. A description of the Hopf algebras is given in [Byo02]. We extend this by determining idempotents giving the Wedderburn decompositions of the Hopf algebras. Since all the Hopf algebras are commutative, each Wedderburn component is an extension field of K. These decompositions also yield a description of the unique maximal $\mathfrak{O}_K$-order in each Hopf algebra. Finally, we derive formulae for the action of each Hopf algebra on the extension L/K.

5.1 Counting the Hopf-Galois Structures

Since the extension L/K is Galois, we use a corollary (2.4.18) to Byott's Translation Theorem (2.4.16) to count the Hopf-Galois structures admitted by the extension. For each of $N = C_{p^2}$ and $N = C_p \times C_p$, we shall need count the number of regular subgroups of $\mathrm{Hol}(N)$ which are isomorphic to $C_p \times C_p$.

Proposition 5.1.1. Let N be a cyclic group of order p^2 and let $M = \mathrm{Hol}(N)$.

i) If p is odd then M contains exactly one elementary abelian subgroup of order p^2, and this is not regular on N.

ii) If $p = 2$ then M contains exactly 2 elementary abelian subgroups of order 4, and exactly one of these is regular on N.

Proof. [Byo96, Lemma 1, parts (i) and (iii)]. We identify N with the additive group $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathrm{Aut}(N)$ with $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Then

$$M = \mathrm{Hol}(N) = \{\theta_{a,t} \mid a \in \mathbb{Z}/p^2\mathbb{Z}, t \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times\},$$

where

$$\theta_{a,t}(x) = a + tx \text{ for all } x \in N.$$

Recalling the decomposition $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$, we identify N with $\{\theta_{a,1} \mid a \in \mathbb{Z}/p^2\mathbb{Z}\}$ and $\mathrm{Aut}(N)$ with $\{\theta_{0,t} \mid t \in (\mathbb{Z}/p^2\mathbb{Z})^\times\}$. For $t \not\equiv 1 \pmod{p^2}$ we may show by induction that for all $x \in N$ we have

$$\theta_{a,t}^k(x) = a\left(\frac{t^k - 1}{t - 1}\right) + t^k x.$$

i) If p is odd then $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is cyclic of order $\phi(p^2) = p(p-1)$. We seek to determine when $\theta_{a,t}$ has order dividing p. Suppose first that $t \equiv 1 \pmod{p^2}$. Then $\theta_{a,1}(x) = a + x$ for all $x \in N$, and $\theta_{a,1}$ has order dividing p if and only

if a has order dividing p in N, i.e. if and only if $a = pA$ for some $A \in \mathbb{Z}/p\mathbb{Z}$. Now suppose $t \not\equiv 1 \pmod{p^2}$. Then

$$\begin{aligned} & \theta_{a,t}^p(x) && \equiv x \pmod{p^2} \, \forall x \in N \\ \Leftrightarrow \quad & a\left(\frac{t^p-1}{t-1}\right) + t^p x && \equiv x \pmod{p^2} \, \forall x \in N \\ \Leftrightarrow \quad & a\left(\frac{t^p-1}{t-1}\right) && \equiv (1-t^p)x \pmod{p^2} \, \forall x \in N \end{aligned}$$

and this holds if and only if $t^p - 1 \equiv 0 \pmod{p^2}$ and $a\left(\frac{t^p-1}{t-1}\right) \equiv 0 \pmod{p^2}$. So in fact

$$\theta_{a,t}^p(x) \equiv x \pmod{p^2} \, \forall x \in N \Leftrightarrow t^p \equiv 1 \pmod{p^2} \text{ and } a \equiv 0 \pmod{p}.$$

Write $a = pA$ and $t = 1 + pT$, where A and T are determined mod p. Then for $x \in N$,

$$\begin{aligned} \theta_{a,t}(x) &= a + tx \\ &= pA + (1+pT)x \\ &= p(A + Tx) + x \\ &\neq x \, \forall x \text{ unless } A = T = 0. \end{aligned}$$

So $\theta_{a,t}$ has order p unless $A = T = 0$, when $\theta_{a,t} = \theta_{0,1} = id$. We therefore have p^2 distinct elements of order 1 or p, which can be shown to commute, and therefore generate a unique elementary abelian subgroup of $\mathrm{Hol}(N)$ of order p^2. This subgroup is not regular on N, since for example if $a = 0$ then $\theta_{0,t}(0) = 0 + t0 = 0$ regardless of the value of t, whence $\mathrm{Stab}(0) \neq \{id\}$.

ii) If $p = 2$ then $M \cong D_8$, the dihedral group of order 8. This has two elementary

abelian subgroups of order 4, which we may present as

$$\begin{aligned} H_1 &= \{id, \theta_{0,3}, \theta_{2,1}, \theta_{2,3}\} \\ H_2 &= \{id, \theta_{3,3}, \theta_{2,1}, \theta_{1,3}\} \end{aligned}$$

The subgroup H_1 is not regular on N since $\mathrm{Stab}(0) = \{id, \theta_{0,3}\}$. The subgroup H_2 is regular on N.

□

Proposition 5.1.2. Let N be an elementary abelian group of order p^2 and let $M = \mathrm{Hol}(N)$.

i) If p is odd then M contains exactly $p^2 + p + 1$ elementary abelian subgroups of order p^2, of which exactly p^2 are regular on N.

ii) If $p = 2$ then M contains exactly 4 elementary abelian subgroups of order 4, of which exactly 1 is regular on N.

Proof. [Byo96, Lemma 2] We identify N with $\mathbb{F}_p^2$ and $\mathrm{Aut}(N)$ with $GL_2(\mathbb{F}_p)$. Then

$$M = \mathrm{Hol}(N) = \{\theta_{A,C} \mid A \in GL_2(\mathbb{F}_p), C \in \mathbb{F}_p^2\},$$

where $\theta_{A,C}(V) = C + AV$ for all $V \in N$. Recalling the decomposition $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$, we may identify N with $\{\theta_{1,C} \mid C \in \mathbb{F}_p^2\}$ and $\mathrm{Aut}(N)$ with $\{\theta_{A,0} \mid A \in GL_2(\mathbb{F}_p)\}$. Inductively we have

$$\theta_{A,C}^k(V) = (A^{k-1} + A^{k-2} + \ldots + A + I)C + A^k V$$

for all $V \in N$. Consider an elementary abelian subgroup H of M of order p^2. We have $|\mathrm{Aut}(N)| = |GL_2(\mathbb{F}_p)| = p(p^2-1)(p-1)$, which is not divisible by p^2, so the image of H in $GL_2(\mathbb{F}_p) \cong \mathrm{Hol}(N)/N$ is either trivial or of order p. If it is trivial

then $H = N$. In the latter case, $H \cap N$ has order p and H is generated by $\theta_{A,C}$ and $\theta_{I,D}$, where $A \in GL_2(\mathbb{F}_p)$ has order p and $C, D \in \mathbb{F}_p^2$ with $D \neq 0$. We require that $AD = D$ for the generators to commute. By Sylow's theorems, there are $p+1$ subgroups of order p in $GL_2(\mathbb{F}_p)$, and they are all conjugate. One such subgroup consists of all unipotent upper triangular matrices. We will count the possibilities for H when A lies in this subgroup, and then use the conjugacy of such subgroups to obtain a full count. Recall that $H = \langle \theta_{A,C}, \theta_{I,D} \rangle$. Replacing $\theta_{A,C}$ and $\theta_{I,D}$ by suitable powers, we may assume that

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

i) If p is odd then

$$\left(A^{p-1} + \ldots + I\right) = \begin{pmatrix} p & \binom{p}{2} \\ 0 & p \end{pmatrix} \equiv 0 \pmod{p}$$

and so any choice of C will give a subgroup of the required type. We may replace $\theta_{A,C}$ by $\theta_{I,D}^r \theta_{A,C}$ for any $r \in \mathbb{Z}$ without altering H, so H determines C only up to a multiple of D. There are therefore p groups H with A upper triangular. There are therefore $p(p+1)$ subgroups H satisfying $|H \cap N| = p$, and 1 satisfying $H = N$, giving a total of $p^2 + p + 1$ elementary abelian subgroups of order p^2 in M. In the case considered in detail above, we find that H is regular on N if and only if C is not a multiple of D. This gives $p - 1$ regular subgroups H. Arguing by conjugation, we find that there are exactly $p^2 - 1$ regular subgroups H with A upper triangular, and so in total exactly p^2 of the elementary abelian subgroups of N of order p^2 are regular on N.

ii) If $p = 2$ then we must insist that $(A+I)C = 0$ in order for $\theta_{A,C}$ to have order

2. We may adjust C by a multiple of D if necessary, and therefore assume $C = 0$. We therefore have only one group H with A upper triangular, and $p + 1 = 3$ elementary abelian subgroups H of M of order 4 and such that $|H \cap N| = 2$. Including the case $H = N$, we have exactly 4 elementary abelian subgroups of order 4 in M. Among these, the only one which is regular on N is $H = N$, since otherwise we have, for example,

$$\theta_{I,D}\theta_{A,C}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix},$$

whence the stabiliser of this element of $\mathbb{F}_p^2$ is nontrivial. (Arguing again by conjugation, we find that the remaining 3 elementary abelian subgroups of M of order 4 are not regular on N.)

□

Theorem 5.1.3 (Byott). Let L/K be an elementary abelian Galois extension of fields of degree p^2. Then L/K admits precisely p^2 Hopf-Galois Structures.

Proof. [Byo96, Corollary to Lemmas 1 and 2, part (iii)] We use (2.4.18). Since there are only two isomorphism classes of groups of order p^2, the number of Hopf-Galois structures on the extension is given by

$$\frac{|\mathrm{Aut}(C_p \times C_p)|}{|\mathrm{Aut}(C_{p^2})|} e'(C_p \times C_p, C_{p^2}) + \frac{|\mathrm{Aut}(C_p \times C_p)|}{|\mathrm{Aut}(C_p \times C_p)|} e'(C_p \times C_p, C_p \times C_p),$$

where for a group N, $e'(C_p \times C_p, N)$ denotes the number of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to $C_p \times C_p$. Suppose first that p is odd. Then by (5.1.1), $e'(C_p \times C_p, C_{p^2}) = 0$, and by (5.1.2), $e'(C_p \times C_p, C_p \times C_p) = p^2$. Thus the number of Hopf-Galois structures is

$$\frac{p(p^2-1)(p-1)}{p(p-1)} 0 + p^2 = p^2.$$

Now suppose that $p = 2$. Then $e'(C_2 \times C_2, C_4) = 1$, and $e'(C_2 \times C_2, C_2 \times C_2) = 1$, so the number of Hopf-Galois structures is

$$\frac{2(4-1)}{2} + 1 = 4 = p^2.$$

□

5.2 Determining the Hopf-Galois Structures

We now describe explicitly the p^2 regular subgroups of $\mathrm{Perm}(G)$ which are normalised by $\lambda(G)$.

Theorem 5.2.1 (Byott). Let L/K be a Galois extension of fields with group $G \cong C_p \times C_p$. Let $T \leq G$ have order p, let $d \in \{0, 1, \ldots, p-1\}$, and fix $\sigma, \tau \in G$ satisfying:

$$T = \langle \tau \rangle, \quad \sigma^p = 1, \quad G = \langle \sigma, \tau \rangle.$$

There are well defined elements $\rho, \eta \in \mathrm{Perm}(G)$ determined by:

$$\begin{aligned} \rho(\sigma^k \tau^l) &= \sigma^k \tau^{l-1} \\ \eta(\sigma^k \tau^l) &= \sigma^{k-1} \tau^{l+(k-1)d} \qquad \text{for } k, l \in \mathbb{Z}. \end{aligned}$$

We have $\rho\eta = \eta\rho$ and

$$\rho^p = 1, \quad \eta^p = \begin{cases} \rho & \text{if } p = 2,\ d = 1 \\ 1 & \text{otherwise.} \end{cases}$$

Now set $N = N_{T,d} = \langle \rho, \eta \rangle$. Then N is a subgroup of $\mathrm{Perm}(G)$ of order p^2, and $N \cong G$ unless $p = 2,\ d = 1$, when N is cyclic. In all cases, N is regular on G, and is normalised by $\lambda(G)$. Thus N gives rise to a Hopf-Galois structure on L/K, with Hopf Algebra $H = H_{T,d} = L[N_{T,d}]^G$. If $d = 0$ then $N = \lambda(G)$, giving the classical

structure regardless of the choice of d. If $d \neq 0$ then the $p-1$ possible choices of d, together with the $p+1$ possible choices of T, yield p^2-1 distinct groups N, each giving rise to a non-classical structure on L/K.

Proof. See [Byo02, Theorem 2.5] □

5.3 Describing the Hopf Algebras

Since $\zeta \in K$, the group algebra $K[\rho]$ has a basis of mutually orthogonal idempotents:

$$e_s = \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{-ks}\rho^k \quad \text{for } 0 \leq s \leq p-1,$$

satisfying

$$\rho e_s = \zeta^s e_s.$$

Let $M = L^T$ be the subfield of L fixed by $T = \langle\tau\rangle$. Thus M/K is cyclic of degree p. Fix $v \in M^\times$ satisfying

$$\sigma(v) = \zeta^{-d}v.$$

Write $v^p = V \in K$, and set

$$a_v = \sum_{s=0}^{p-1} v^s e_s \in M[\rho].$$

Proposition 5.3.1 (Byott). With the above notation, for $d \neq 0$, we have $H_{T,d} = K[\rho, a_v\eta]$.

Proof. [Byo02, Lemma 2.10]. Let $H = H_{T,d}$. By (2.4.9), $H = L[N]^G$ for some regular subgroup N of $\mathrm{Perm}(G)$ which is normalised by $\lambda(G)$, and where G acts on L as the Galois group and on N by conjugation via λ. In particular H has

dimension p^2 as a K-algebra. Since $\rho^p = 1_N$ and

$$(a_v\eta)^p = \sum_{s=0}^{p-1} v^{ps} e_s \eta^p = \sum_{s=0}^{p-1} v^{ps} e_s \in K[\rho],$$

we have that $K[\rho, a_v\eta]$ is also a K-subalgebra of $L[N]$ of dimension p^2. It will therefore suffice to show that $K[\rho, a_v\eta]$ is fixed elementwise by G. We see easily that ${}^g\rho = \rho$ for all $g \in G$, and so every element of $K[\rho]$ is fixed by G. In particular this implies that the idempotents $e_s \in K[\rho]$ are fixed by G. Now $K[a_v\eta, \rho]$ is generated over $K[\rho]$ by $a_v\eta$, so it remains only to show that $a_v\eta$ is fixed by G. We calculate ${}^\tau\eta = \eta, {}^\sigma\eta = \rho^d\eta$ and recall that $v \in L^T = L^{\langle\tau\rangle}$. Then:

$$\begin{aligned} {}^\tau(a_v\eta) &= \sum_{s=0}^{p-1} \tau(v)^s({}^\tau(e_s\eta)) \\ &= \sum_{s=0}^{p-1} v^s e_s \eta \\ &= a_v\eta \end{aligned}$$

and

$$\begin{aligned} {}^\sigma(a_v\eta) &= \sum_{s=0}^{p-1} \sigma(v)^s({}^\sigma(e_s\eta)) \\ &= \sum_{s=0}^{p-1} \sigma(v)^s e_s \rho^d \eta \\ &= \sum_{s=0}^{p-1} \zeta^{-ds} v^s e_s \zeta^{ds} \eta \\ &= a_v\eta \end{aligned}$$

This completes the proof. □

Since for all choices of T and d the Hopf algebra $H_{T,d}$ is commutative, it has a unique maximal $\mathfrak{O}_K$-order. In what follows, it will often be useful to have an explicit description of this maximal order. We determine idempotents giving the

Wedderburn decomposition of each $H_{T,d}$ into a product of extension fields of K. We then obtain a description of the maximal order in $H_{T,d}$ as the preimage of the product of rings of algebraic integers of the extension fields.

Proposition 5.3.2. With the above notation we have, for $d \neq 0$ and any choice of T, the following isomorphisms of K-algebras.

$$H_{T,d} \cong \begin{cases} K^2 \times K(w) & \text{if } p = 2 \\ K^p \times K(v)^{p-1} & \text{otherwise} \end{cases}$$

where w is defined by $w^2 = -v^2 = -V$.

Proof. Let $d \neq 0$. Take a basis of $H_{T,d} = K[\rho, a_v\eta]$:

$$\omega = \{\rho^s (a_v\eta)^t \mid 0 \leq s, t \leq p-1\}.$$

The set $\{\rho^s \mid 0 \leq s \leq p-1\}$ has $K-$span isomorphic to $K[\rho]$. We make the following change of generators of $H_{T,d}$:

$$\rho^s (a_v\eta)^t \quad \mapsto \quad e_s (a_v\eta)^t \text{ for } 0 \leq s, t \leq p-1$$

This is easily shown to be a change of basis, for since K is a field we have the explicit inversion formulae

$$\rho^k (a_v\eta)^t \quad = \quad \sum_{s=0}^{p-1} \zeta^{ks} e_s (a_v\eta)^t.$$

We shall write

$$\omega' = \{e_s (a_v\eta)^t \mid 0 \leq s, t \leq p-1\},$$

and examine properties of the basis ω'. Clearly

$$(e_s (a_v\eta)^t)(e_{s'} (a_v\eta)^{t'}) = 0$$

whenever $s \neq s'$. We examine first the properties of elements of the form $e_0(a_v\eta)^t$.

$$\begin{aligned} e_0(a_v\eta)^t &= (e_0 a_v \eta)^t \\ &= (e_0\eta)^t \\ &= e_0\eta^t \end{aligned}$$

So

$$e_0 H_{T,d} \cong K[\eta].$$

Clearly by forming orthogonal idempotents within $K[\eta]$ we have $K[\eta] \cong K^p$. The corresponding base change in $e_0 H_{T,d}$ is

$$e_0(a_v\eta)^t \mapsto \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{kdt} e_0(a_v\eta)^k.$$

Now suppose $s \neq 0$ and examine elements of the form $e_s(a_v\eta)^t$. For $p = 2$ we calculate

$$\begin{aligned} (e_1(a_v\eta))^2 &= (e_1 v\eta)^2 \\ &= e_1(v\eta)^2 \\ &= e_1 V\eta^2 \\ &= e_1 V\rho \quad \text{(since } N \text{ is cyclic)} \\ &= -e_1 V \quad \text{(by definition of } e_1) \end{aligned}$$

Recall the definition of w from the statement of the proposition. If we make the identifications

$$\begin{aligned} e_1 &\mapsto 1 \\ e_1(a_v\eta) &\mapsto w, \end{aligned}$$

we see that $e_1 H_{T,d} \cong K(w)$. This gives, for $p = 2$,

$$H_{T,d} \cong K^2 \times K(w).$$

For $p \neq 2$, we have

$$\begin{aligned} (e_s(a_v\eta))^p &= (e_s a_v \eta)^p \\ &= (e_s v^s \eta)^p \\ &= e_s (v^s \eta)^p \\ &= (V)^s e_s. \end{aligned}$$

So, making the identifications

$$\begin{aligned} e_s &\mapsto 1 \\ e_s(a_v\eta) &\mapsto v^s \end{aligned}$$

for $s = 1, \ldots, p-1$, we see that $e_s H_{t,d} \cong K(v^s) \cong K(v)$. Thus for $p \neq 2$ we have

$$H_{T,d} \cong K^p \times K(v)^{p-1}.$$

□

Definition 5.3.3. For $r = 0, \ldots, p-1$, we shall adopt the following notation for the idempotents defined in the proof of (5.3.2):

$$E_r = \frac{1}{p} \sum_{k=0}^{p-1} \zeta^{kdr} e_0 (a_v \eta)^k.$$

Corollary 5.3.4. We have the following description of the unique maximal $\mathfrak{O}_K$-

order $\mathfrak{M}_{T,d}$ in $H_{T,d}$.

$$\mathfrak{M}_{T,d} \cong \begin{cases} \mathfrak{O}_K^2 \times \mathfrak{O}_{K(w)} & \text{if } p = 2 \\ \mathfrak{O}_K^p \times \mathfrak{O}_{K(v)}^{p-1} & \text{otherwise.} \end{cases}$$

Remark 5.3.5. It is possible to choose the element v such that in the notation of (4.2.4) we have $v = \alpha^i \beta^j$ for some nonnegative integers i, j, and we shall always assume that we have done so. Choosing v in this way we have $v^p \equiv 1 \pmod{(\zeta - 1)^{pe'}}$, which allows us to use (4.1.1), (4.3.2)and (4.3.3) to describe locally the unique maximal $\mathfrak{O}_K$-order $\mathfrak{M}_{T,d}$.

Corollary 5.3.6. If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which does not lie above p, then we may use (4.3.2) to obtain an explicit $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{M}_{T,d,\mathfrak{p}}$, valid for both $p = 2$ and odd p.

$$\{E_r \mid 0 \leq r \leq p-1\} \cup \left\{ \frac{e_s(a_v\eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \mid 1 \leq s \leq p-1, 0 \leq t \leq p-1 \right\}.$$

Corollary 5.3.7. If p is odd and $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which lies above p, then we may use (4.3.3) to obtain an explicit description of $\mathfrak{M}_{T,d,\mathfrak{p}}$. We observe that since $V = v^p \equiv 1 \pmod{(\zeta - 1)^p}$, we also have $(v^s)^p \equiv 1 \pmod{(\zeta - 1)^p}$, and so an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{K(v^s),\mathfrak{p}}$ is

$$\left\{ \left(\frac{v^s - 1}{\pi_{\mathfrak{p}}^{e'}} \right)^t \mid 0 \leq t \leq p-1 \right\},$$

which implies that an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{M}_{T,d,\mathfrak{p}}$ is

$$\{E_r \mid 0 \leq r \leq p-1\} \cup \left\{ \left(\frac{e_s(a_v\eta) - e_s}{\pi_{\mathfrak{p}}^{e'}} \right)^t \mid 1 \leq s \leq p-1, 0 \leq t \leq p-1 \right\}.$$

If $p = 2$ then $H \cong K^2 \times K(w)$, where $w^2 = -V$, and so it is possible that $K(w)$ is wildly ramified at primes lying above 2. In order to obtain a description of $\mathfrak{M}_{T,d,\mathfrak{p}}$ in this case, we first obtain a description of $\mathfrak{O}_{K(w)}$:

Proposition 5.3.8. Let $p = 2$ and $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above 2, and write $2\mathfrak{O}_{K,\mathfrak{p}} = u\pi_{\mathfrak{p}}^e \in \mathfrak{O}_{K,\mathfrak{p}}$, so $e = v_{\mathfrak{p}}(2)$. Then there exists $e/2 \leq q_{\mathfrak{p}} \leq e$ and $c_{\mathfrak{p}} \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$ such that the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{K(w),\mathfrak{p}}$.

$$\left\{1, \left(\frac{c_{\mathfrak{p}}w - 1}{\pi_{\mathfrak{p}}^{q_{\mathfrak{p}}}}\right)\right\}$$

Proof. We omit the subscript $\mathfrak{p}$ and write simply c and q. Recall that $w^2 = W = -V$ and that $V \equiv 1 \pmod^* 4\mathfrak{O}_K$. So $V = 1 + u_1\pi_{\mathfrak{p}}^m$ for some $u_1 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$ and $m \geq 2e$. Then

$$\begin{aligned} W &= -1 - u_1\pi_{\mathfrak{p}}^m \\ &= 1 - 2 - u_1\pi_{\mathfrak{p}}^m \\ &= 1 - u\pi_{\mathfrak{p}}^e - u_1\pi_{\mathfrak{p}}^m \\ &= 1 + u_2\pi_{\mathfrak{p}}^e \end{aligned}$$

for some $u_2 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. We follow the proof of (4.1.1), case (ii). There exist some $c, u_c \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$ such that $(cw)^2 = 1 + u_c\pi_{\mathfrak{p}}^Q$ with either $Q < 2e$ and $Q \equiv 1 \pmod 2$ or $Q \geq 2e$. In the first case $K(w)_{\mathfrak{p}}/K_{\mathfrak{p}}$ is totally wildly ramified. We write $Q = 2q+1$ (so in particular $q < e$) and apply (4.1.4), which implies that the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{K(w),\mathfrak{p}}$:

$$\left\{1, \left(\frac{cw - 1}{\pi_{\mathfrak{p}}^q}\right)\right\}.$$

In the second case $K(w)_{\mathfrak{p}}/K_{\mathfrak{p}}$ is either unramified ($Q = 2e$) or not a proper extension ($Q > 2e$). We use (4.3.4) to handle these two cases together. (4.1.3) then implies that the following is an $\mathfrak{O}_{K,\mathfrak{p}}$ basis of $\mathfrak{O}_{K(w),\mathfrak{p}}$:

$$\left\{1, \left(\frac{cw - 1}{\pi_{\mathfrak{p}}^e}\right)\right\}$$

□

Corollary 5.3.9. Let $p = 2$ and $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2. Then for $c = c_{\mathfrak{p}}$ and $q = q_{\mathfrak{p}}$ as defined above, the following is an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{M}_{T,d,\mathfrak{p}}$:

$$\left\{ E_0, E_1, e_1, \frac{ce_1(a_v\eta) - e_1}{\pi_{\mathfrak{p}}^q} \right\}.$$

5.4 Action of the Hopf Algebras on L/K

In addition to the notation established in the previous sections, we now fix an element $x \in (\mathfrak{O}_L^{\langle\sigma\rangle})^\times$ satisfying $\tau(x) = \zeta x$. As in (5.3.5), it is possible to choose the element x such that in the notation of (4.2.4) we have $x = \alpha^i\beta^j$ for some nonnegative integers i, j, and we shall always assume that we have done so. We shall write $x^p = X$, and we have have $x^p \equiv 1 \pmod{(\zeta - 1)^{pe'}}$. Then

$$L = K(x, v),$$

so to determine the action of the Hopf algebra H on L/K, we need only consider the action of each K-basis element of H on an arbitrary product x^iv^j. Recall that H has K-basis

$$\{E_r \mid 0 \le r \le p-1\} \cup \left\{e_s(a_v\eta)^t \mid 1 \le s \le p-1, 0 \le t \le p-1\right\}.$$

By Greither and Parigeis theory (2.4.9), the action of H on L is given by

$$\left(\sum_{n\in N} c_n n\right).x = \sum_{n\in N} c_n n^{-1}(1_G)x.$$

We calculate:

$$\begin{aligned}\rho^r\eta^t(\sigma^k\tau^l) &= \eta^t(\sigma^k\tau^{l-r}) \\ &= \sigma^{k-t}\tau^{l-r+dtk-(dt(t+1))/2} \\ &= 1_G \text{ if and only if } k=t \text{ and } l = r - \frac{dt(t-1)}{2}\end{aligned}$$

and so

$$(\rho^r\eta^t)^{-1}(1_G) = \sigma^t\tau^{r-(dt(t-1))/2} \tag{5.1}$$

In particular,

$$(\rho^r)^{-1}(1_G) = \tau^r.$$

Proposition 5.4.1. For $s = 0, \ldots, p-1$ we have

$$e_s(x^iv^j) = \begin{cases} x^iv^j & \text{if } s = i \\ 0 & \text{otherwise} \end{cases}$$

Proof. Each $e_s \in H$, so we use equation (5.1) to calculate $e_s(x^iv^j)$.

$$\begin{aligned}e_s(x^iv^j) &= \frac{1}{p}\sum_{k=0}^{p-1}\zeta^{-ks}\rho^k x^iv^j \\ &= \frac{1}{p}\sum_{k=0}^{p-1}\zeta^{-ks}\tau^k(x^iv^j) \\ &= \frac{1}{p}\sum_{k=0}^{p-1}\zeta^{-ks}\zeta^{ki}x^iv^j \\ &= \frac{x^iv^j}{p}\sum_{k=0}^{p-1}\zeta^{k(i-s)} \\ &= \begin{cases} x^iv^j & \text{if } s = i \\ 0 & \text{otherwise} \end{cases}\end{aligned}$$

□

Proposition 5.4.2. For $t = 0, \ldots, p-1$ we have

$$(a_v\eta)^t(x^iv^j) = \zeta^{-dtj}\zeta^{-dit(t-1)/2}x^iv^{j+it}.$$

Proof. First we observe that

$$\begin{aligned}(a_v\eta)^t &= \left(\sum_{s=0}^{p-1} v^s e_s\eta\right)^t \\ &= \sum_{s=0}^{p-1} v^{st} e_s\eta^t\end{aligned}$$

since the e_s are orthogonal idempotents. Now each $(a_v\eta)^t \in H$, so we use equation (5.1) to calculate $(a_v\eta)^t(x^iv^j)$.

$$\begin{aligned}(a_v\eta)^t(x^iv^j) &= \sum_{s=0}^{p-1} v^{st} e_s\eta^t(x^iv^j) \\ &= \frac{1}{p}\sum_{s=0}^{p-1}\sum_{k=0}^{p-1} v^{st}\zeta^{-ks}\rho^k\eta^t(x^iv^j) \\ &= \frac{1}{p}\sum_{s=0}^{p-1}\sum_{k=0}^{p-1} v^{st}\zeta^{-ks}\sigma^t\tau^{k-dt(t-1)/2}(x^iv^j) \\ &= \frac{1}{p}\sum_{s=0}^{p-1}\sum_{k=0}^{p-1} v^{st}\zeta^{-ks}\zeta^{-dtj}\zeta^{ki-dit(t-1)/2}x^iv^j \\ &= \frac{\zeta^{-dtj}\zeta^{-dit(t-1)/2}x^iv^j}{p}\sum_{s=0}^{p-1}\sum_{k=0}^{p-1}\zeta^{k(i-s)}v^{st} \\ &= \zeta^{-dtj}\zeta^{-dit(t-1)/2}x^iv^{j+it}.\end{aligned}$$

□

Proposition 5.4.3. For $s = 0, \ldots, p-1$ and $t = 0, \ldots, p-1$, we have

$$e_s(a_v\eta)^t(x^iv^j) = \begin{cases} \zeta^{-dtj}\zeta^{-dit(t-1)/2}x^iv^{j+it} & \text{if } i = s \\ 0 & \text{otherwise.}\end{cases}$$

Proof. By (5.4.2),

$$(a_v\eta)^t(x^iv^j) = \zeta^{-dtj}\zeta^{-dit(t-1)/2}x^iv^{j+it}.$$

Then by (5.4.1),

$$e_s(\zeta^{-dtj}\zeta^{-dit(t-1)/2}x^iv^{j+it}) = \begin{cases} \zeta^{-dtj}\zeta^{-dit(t-1)/2}x^iv^{j+it} & \text{if } i = s \\ 0 & \text{otherwise.} \end{cases}$$

□

Proposition 5.4.4. For $r = 0, \ldots, p-1$, we have

$$E_r(x^iv^j) = \begin{cases} v^r & \text{if } i = 0, j = r \\ 0 & \text{otherwise} \end{cases}$$

Proof. Recall that

$$E_r = \frac{1}{p}\sum_{k=0}^{p-1}\zeta^{kdr}e_0(a_v\eta)^k.$$

By (5.4.3),

$$e_0(a_v\eta)^k(x^iv^j) = \begin{cases} \zeta^{-dkj}v^j & \text{if } i = 0 \\ 0 & \text{otherwise} \end{cases}$$

Now

$$E_r(x^iv^j) = \frac{1}{p}\sum_{k=0}^{p-1}\zeta^{kdr}e_0(a_v\eta)^k(x^iv^j),$$

So it is clear from (5.4.3) that $E_r(x^i v^j) = 0$ unless $i = 0$. So we consider

$$\begin{aligned} E_r(v^j) &= \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{kdr} e_0 (a_v \eta)^k (v^j) \\ &= \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{kdr} \zeta^{-kdj} v^j \\ &= \frac{v^j}{p}\sum_{k=0}^{p-1} \zeta^{kd(j-r)} \\ &= \begin{cases} v^r & \text{if } j = r \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

□

Chapter 6

Local Generators and Local Units

We retain the notation of the previous chapter: p is a prime number, K is a number field containing a primitive p^{th} root of unity ζ, and L/K is a tamely ramfied Galois extension with group $G \cong C_p \times C_p$. An arbitrary nonclassical Hopf-Galois structure $H = H_{T,d}$ on L/K has the form $H_{T,d} = L[N_{T,d}]^G$ for some regular subgroup $N = N_{T,d}$ of $\mathrm{Perm}(G)$ normalised by G. We have fixed generators σ, τ, and so subgroups $S = \langle\sigma\rangle$ and $T = \langle\tau\rangle$ of G, and a value of $d \in \{1, \ldots, p-1\}$. We have also fixed elements $x \in \mathfrak{O}_L^S$ and $v \in \mathfrak{O}_L^T$ satisfying $\tau(x) = \zeta x$, $\sigma(v) = \zeta^{-d}v$, $x^p \equiv v^p \equiv 1 \pmod{(\zeta-1)^p}$ and $L = K(x, v)$.

By the results of chapter 3 we have that $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module in all of the Hopf-Galois structures admitted by L/K. This immediately leads us to ask under what conditions $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module. In later chapters we shall use Fröhlich's Hom Description of the locally free class group $\mathrm{Cl}\,(\mathfrak{A}_H)$ (see section (2.1.4)) to address this question. In order to do this we shall need detailed local information, which we collect in this chapter. We provide explicit generators of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$. We also study the idèle group $\mathbb{J}(H)$, and in particular the group of unit idèles $\mathbb{U}(\mathfrak{A}_H)$.

6.1 Explicit Local Generators

Theorem 6.1.1. Let $H = L[N]^G$ be a Hopf algebra giving a Hopf-Galois structure on L/K, and let $\mathfrak{A}_H \subseteq H$ be the associated order. Then:

i) The ring of integers $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module.

ii) If $\mathfrak{p}$ does not lie above p, then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ and this is the unique maximal order in $H_{\mathfrak{p}}$.

iii) If $\mathfrak{p}$ lies above p, then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ and this is a Hopf order in $H_{\mathfrak{p}}$.

Proof. We use results from chapter 3:

i) This follows immediately from (3.1.8).

ii) Since $\mathfrak{p}$ does not lie above p, we may apply (3.1.4).

iii) Since L/K is tamely ramified of degree p^2 and $\mathfrak{p}$ lies above p, we must have that $\mathfrak{p}$ is unramified in $\mathfrak{O}_L$. We may therefore apply (3.1.3).

□

Having established that $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module, we now seek conditions for global freeness. $\mathfrak{O}_L$ defines a class in the locally free class group $\mathrm{Cl}\,(\mathfrak{A}_H)$, and, since H is commutative, $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module precisely when this class is trivial (see (2.1.24)). We shall use the isomorphism in (2.1.25) to determine when this occurs.

$$\mathrm{Cl}\,(\mathfrak{A}_H) \cong \frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathfrak{A}_H)}.$$

Recall from (2.1.25) that the class of $\mathfrak{O}_L$ corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbb{J}(H)$, where for some fixed generator Γ of L over H, the element $h_{\mathfrak{p}} \in H_{\mathfrak{p}}$ is defined by $h_{\mathfrak{p}}\Gamma = \gamma_{\mathfrak{p}}$, where $\gamma_{\mathfrak{p}}$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. We seek first to determine these local generators.

Proposition 6.1.2. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which does not lie above p. Define $0 \leq j_{\mathfrak{p}} \leq p-1$ as follows:

$$\begin{cases} j_{\mathfrak{p}} = 0 & \text{if } v_{\mathfrak{p}}(X) \equiv 0 \pmod{p} \text{ or } v_{\mathfrak{p}}(V) \equiv 0 \pmod{p} \\ v_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}}) \equiv 0 \pmod{p} & \text{otherwise.} \end{cases}$$

Then the following element $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$ is a generator for $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module:

$$\gamma_{\mathfrak{p}} = \sum_{j=0}^{p-1} \frac{v^j}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^j)}} + \sum_{s=1}^{p-1} \frac{x^s v^{sj_{\mathfrak{p}}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})}}.$$

Proof. Since $\mathfrak{O}_{L,\mathfrak{p}}$ and $\mathfrak{A}_{H,\mathfrak{p}}$ are both free $\mathfrak{O}_{K,\mathfrak{p}}$-modules of rank p^2, it suffices to show that the images of $\gamma_{\mathfrak{p}}$ under the $\mathfrak{O}_{K,\mathfrak{p}}$-basis elements of $\mathfrak{A}_{H,\mathfrak{p}}$ form an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$. We note that for each $s = 0, \ldots, p-1$ we have $e_s \mathfrak{O}_{L,\mathfrak{p}} \subset \mathfrak{O}_{L,\mathfrak{p}}$, and in fact $\mathfrak{O}_{L,\mathfrak{p}} = \sum_{s=0}^{p-1} e_s \mathfrak{O}_{L,\mathfrak{p}}$. Recall from (4.3.2) that an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$ is given by

$$\left\{ \frac{x^i v^j}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^i V^j)}} \mid 0 \leq i, j \leq p-1 \right\}.$$

In particular, for $s = 0, \ldots, p-1$ an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $e_s \mathfrak{O}_{L,\mathfrak{p}}$ is given by

$$\left\{ \frac{x^s v^j}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s V^j)}} \mid 0 \leq j \leq p-1 \right\}.$$

Recall also from (3.1.2) that $\mathfrak{O}_{L,\mathfrak{p}}$ admits the maximal order $\mathfrak{M}_{H,\mathfrak{p}}$, which by (5.3.4) has $\mathfrak{O}_{K,\mathfrak{p}}$-basis

$$\{E_r \mid 0 \leq r \leq p-1\} \cup \left\{ \frac{e_s (a_v \eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \mid 1 \leq s \leq p-1, 0 \leq t \leq p-1 \right\}.$$

Now for each $r = 0, \ldots, p-1$, we have by (5.4.4) that

$$E_r \gamma_{\mathfrak{p}} = \frac{v^r}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^r)}},$$

giving an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $e_0\mathfrak{O}_{L,\mathfrak{p}}$. For $s \neq 0$ and $t = 0, \ldots, p-1$, we have by (5.4.3) that

$$\begin{aligned} \frac{e_s(a_v\eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}}\gamma_{\mathfrak{p}} &= \frac{e_s(a_v\eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \frac{x^s v^{sj_{\mathfrak{p}}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}})}} \\ &\sim \frac{v^{st}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \frac{x^s v^{sj_{\mathfrak{p}}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}})}} \\ &= \frac{x^s v^{sj_{\mathfrak{p}}+st}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}+st})}}, \end{aligned}$$

the final equality holding since by the choice of $j_{\mathfrak{p}}$ we have

$$r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}}) + r_{\mathfrak{p}}(V^{st}) = r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}+st}).$$

For each $s \neq 0$, these generate an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $e_s\mathfrak{O}_{L,\mathfrak{p}}$ as t varies. Together with the basis of $e_0\mathfrak{O}_{L,\mathfrak{p}}$, we have an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$. □

Remark 6.1.3. We note that $j_{\mathfrak{p}} \neq 0$ if and only if $(v_{\mathfrak{p}}(X), p) = (v_{\mathfrak{p}}(V), p) = 1$, that is, if and only if $\mathfrak{p}$ is ramified in both of the subextensions $K(x)/K$ and $K(v)/K$.

If $\mathfrak{p}$ is a prime lying above p, then $\mathfrak{p}$ is unramified in $\mathfrak{O}_L$ since L/K is tamely ramified of degree p^2. We then have by (3.4.1) that $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a Hopf order in $H_{\mathfrak{p}}$ and by (3.4.2) that $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$. We shall use the theorem of Childs and Hurley (2.5.10) to determine an explicit local generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ for these primes. We shall need to show that $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a local ring. The following proposition provides a criterion for this.

Proposition 6.1.4. Let R be a complete discrete valuation ring with maximal ideal $\mathfrak{m}$, and A a commutative R-algebra which is finitely generated as an R-module. Then A is a local ring if and only if A contains no nontrivial idempotents.

Proof. Suppose first that A is a local ring. If A contains a nontrivial idempotent e then $1-e$ is also a nontrivial idempotent and so $eA, (1-e)A$ are two distinct

maximal ideals of A, a contradiction. Conversely, supppose that A contains no nontrivial idempotents. Let rad(A) denote the Jacobson radical of A:

$$\text{rad(A)} = \bigcap \mathfrak{a}, \text{ where } \mathfrak{a} \text{ ranges over all maximal ideals of } A,$$

and let $\overline{A} = A/\text{rad(A)}$. Then $\overline{A}$ is semisimple by [CR81a, (5.22)], and by [CR81a, (5.21)], A is local if and only if $\overline{A}$ is a field. Suppose that $\overline{A}$ is not a field. Then it has at least one proper ideal, and by semisimplicity this ideal is a direct summand of $\overline{A}$, whence $\overline{A}$ contains a nontrivial idempotent ε. Since R is complete with respect to the $\mathfrak{m}$-adic topology, A is complete with respect to the rad(A)-adic topology, and therefore by [CR81a, (6.7)] we may lift idempotents from $\overline{A}$ to A. So ε corresponds to a nontrivial idempotent $e \in A$. This contradicts the assumption that A contains no nontrivial idempotents. So $\overline{A}$ is a field, and therefore A is a local ring. □

Proposition 6.1.5. Let p be a prime number, and R a discrete valuation ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$ having characteristic p. Let G be a group of p-power order. Then the group ring $R[G]$ is a local ring.

Proof. See [CR81a, (5.25)]. □

Proposition 6.1.6. Suppose L/K is a Galois extension of number fields of p-power degree which is at most tamely ramified, and that $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ lying above p. Suppose that L/K is H-Galois for a commutative Hopf algebra $H = L[N]^G$. Then $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is a local ring.

Proof. We note first that $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is finitely generated as an $\mathfrak{O}_{K,\mathfrak{p}}$-module, so by (6.1.4) it is sufficient to show that $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ contains no nontrivial idempotents. Recall from (2.1.15) the isomorphism

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

This induces an isomorphism

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

and the G-action on each side yields

$$\mathfrak{O}_{L,\mathfrak{p}}[N]^G \cong \left(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{L,\mathfrak{P}}[N] \right)^G.$$

Now each $\mathfrak{O}_{L,\mathfrak{P}}$ is a discrete valuation ring with residue field of characteristic p, so each $\mathfrak{O}_{L,\mathfrak{P}}[N]$ is a local ring, and therefore has no nontrivial idempotents by (6.1.4). Now suppose that $x \in \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is an idempotent. Then x is also an idempotent of $\mathfrak{O}_{L,\mathfrak{p}}[N]$, and so the image $(x_1, \ldots, x_g)$ of x is an idempotent in $\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{L,\mathfrak{P}}[N]$. Since each $\mathfrak{O}_{L,\mathfrak{P}}[N]$ has no nontrivial idempotents, each x_i is either equal to 1 or 0. If $x_i = 0$ for all i then $x = 0$, and if $x_i = 1$ for all i then $x = 1$. In all other cases, since by (2.1.14) G permutes transitively the primes $\mathfrak{P} \mid \mathfrak{p}$, there exists some $\sigma \in G$ such that $\sigma(x_1, \ldots, x_g) \neq (x_1, \ldots, x_g)$. This contradicts the assumption that $x \in \mathfrak{O}_{L,\mathfrak{p}}[N]^G$. So $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ contains no nontrivial idempotents and is therefore a local ring. □

Proposition 6.1.7. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ which lies above p. Then the following element $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$ is a generator for $\mathfrak{O}_{L,\mathfrak{p}}$ as an $\mathfrak{A}_{H,\mathfrak{p}}$-module:

$$\gamma_{\mathfrak{p}} = \frac{1}{p^2} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} x^i v^j$$

Proof. By (3.4.2), we have $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$. By (3.4.1), this is an $\mathfrak{O}_{K,\mathfrak{p}}$-Hopf algebra, and by (6.1.6) it is local. The trace element

$$\theta = \sum_{n \in N} n$$

lies in $\mathfrak{O}_{L,\mathfrak{p}}[N]$ and is clearly fixed by G. It is a generator for the module of integrals of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$. By (2.5.10), it suffices to prove that $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$ and that $\theta(\gamma_{\mathfrak{p}}) = 1$. To show that $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$, we observe first that

$$\gamma_{\mathfrak{p}} = \left(\frac{1}{p}\sum_{i=0}^{p-1} x^i\right)\left(\frac{1}{p}\sum_{j=0}^{p-1} v^j\right).$$

So it is sufficient to show that

$$\left(\frac{1}{p}\sum_{i=0}^{p-1} x^i\right) \in \mathfrak{O}_{L,\mathfrak{p}}$$

since then, arguing by symmetry, we may conclude that $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$. Recall from (4.3.3) that an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$ is given by

$$\left\{\left(\frac{x-1}{\pi_{\mathfrak{p}}^{e'}}\right)^i\left(\frac{v-1}{\pi_{\mathfrak{p}}^{e'}}\right)^j | 0 \le i,j \le p-1\right\},$$

where $v_{\mathfrak{p}}(p) = e = (p-1)e'$. In particular, the element

$$\left(\frac{x-1}{\pi_{\mathfrak{p}}^{e'}}\right)^{p-1} \sim \frac{1}{p}\sum_{k=0}^{p-1}\binom{p-1}{k}(-1)^k x^k$$

lies in $\mathfrak{O}_{L,\mathfrak{p}}$. But for $k = 0,\ldots,p-1$ we have

$$\begin{aligned}\binom{p-1}{k} &= \frac{(p-1)\ldots(p-k)}{1\ldots k}\\ &\equiv \frac{\underbrace{(-1)\ldots(-1)}_{k}}{} \pmod p\\ &\equiv (-1)^k \pmod p\end{aligned}$$

Therefore

$$\sum_{k=0}^{p-1}\binom{p-1}{k}(-1)^k x^k \equiv \sum_{k=0}^{p-1} x^k \pmod p,$$

and so

$$\left(\frac{1}{p}\sum_{i=0}^{p-1} x^i\right) \in \mathfrak{O}_{L,\mathfrak{p}},$$

whence $\gamma_{\mathfrak{p}} \in \mathfrak{O}_{L,\mathfrak{p}}$. To show that $\theta(\gamma_{\mathfrak{p}}) = 1$, we calculate:

$$\begin{aligned}
\theta(\gamma_{\mathfrak{p}}) &= \frac{1}{p^2}\sum_{g\in G} g\left(\sum_{i,j=0}^{p-1} x^i v^j\right) \\
&= \frac{1}{p^2}\sum_{s,t=0}^{p-1} \sigma^s\tau^t\left(\sum_{i,j=0}^{p-1} x^i v^j\right) \\
&= \frac{1}{p^2}\sum_{i,j=0}^{p-1}\sum_{s,t=0}^{p-1} \sigma^s\tau^t(x^i v^j) \\
&= \frac{1}{p^2}\sum_{i,j=0}^{p-1}\sum_{s,t=0}^{p-1} \zeta^{it}\zeta^{-dsj} x^i v^j \\
&= \frac{1}{p^2}\sum_{i,j=0}^{p-1} x^i v^j \sum_{s,t=0}^{p-1} \zeta^{it-dsj}
\end{aligned}$$

Now

$$\sum_{s,t=0}^{p-1} \zeta^{it-dsj} = \begin{cases} p^2 & \text{if } i=j=0 \\ 0 & \text{otherwise} \end{cases}$$

so $\theta\gamma_{\mathfrak{p}} = 1$. □

6.2 Local Units of the Associated Order

We now seek a more explicit description of the group

$$\frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathfrak{A}_H)}.$$

From (5.3.2) we have

$$H^\times \cong \begin{cases} (K^\times)^2 \times K(w)^\times & \text{if } p = 2 \\ (K^\times)^p \times (K(v)^\times)^{p-1} & \text{otherwise} \end{cases}$$

and

$$\mathbb{J}(H) \cong \begin{cases} \mathbb{J}(K)^2 \times \mathbb{J}(K(w)) & \text{if } p = 2 \\ \mathbb{J}(K)^p \times \mathbb{J}(K(v))^{p-1} & \text{otherwise.} \end{cases}$$

So it remains to describe the group

$$\mathbb{U}(\mathfrak{A}_H) = \left\{(h_\mathfrak{p})_\mathfrak{p} \in \mathbb{J}(H) \mid h_\mathfrak{p} \in \mathfrak{A}_{H,\mathfrak{p}}^\times \text{ for all } \mathfrak{p}\right\} = \prod_{\mathfrak{p} \lhd \mathfrak{O}_K} \mathfrak{A}_{H,\mathfrak{p}}^\times.$$

By (3.4.2) and (3.6.1), we have

$$\mathfrak{A}_{H,\mathfrak{p}}^\times = \begin{cases} \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times & \text{if } \mathfrak{p} \mid p\mathfrak{O}_K \\ \mathfrak{M}_{H,\mathfrak{p}}^\times & \text{otherwise} \end{cases}$$

and by (5.3.4) we have

$$\mathfrak{M}_{H,\mathfrak{p}}^\times \cong \begin{cases} (\mathfrak{O}_{K,\mathfrak{p}}^\times)^2 \times \mathfrak{O}_{K(w),\mathfrak{p}}^\times & \text{if } p = 2 \\ (\mathfrak{O}_{K,\mathfrak{p}}^\times)^p \times (\mathfrak{O}_{K(v),\mathfrak{p}}^\times)^{p-1} & \text{otherwise.} \end{cases}$$

So it remains, for $\mathfrak{p} \mid p\mathfrak{O}_K$, to describe the group $\mathfrak{A}_{H,\mathfrak{p}}^\times = \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$.

Proposition 6.2.1. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p. For $0 \le i \le p-1$ and $1 \le t \le p-1$ define

$$\omega_{i,t} = p\pi_\mathfrak{p}^{-ie'} \sum_{s=0}^{i} \binom{i}{s} (-1)^{i-s} e_s (a_v \eta)^t.$$

Then an $\mathfrak{O}_{K,\mathfrak{p}}$-basis for $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is given by

$$\{\rho^k \mid 0 \leq k \leq p-1\} \cup \{\omega_{i,t} \mid 0 \leq i \leq p-1, 1 \leq t \leq p-1\}.$$

Proof. Let $N = \langle \rho, \eta \rangle$ be the regular subgroup of $\mathrm{Perm}(G)$ which determines H. Since $\mathfrak{p}$ is unramified in $\mathfrak{O}_L$, we have by (3.3.1) that $\mathfrak{O}_{L,\mathfrak{p}}[N] = \mathfrak{O}_{L,\mathfrak{p}}[N]^G \otimes_{\mathfrak{O}_{K,\mathfrak{p}}} \mathfrak{O}_{L,\mathfrak{p}}$, so an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ is precisely an $\mathfrak{O}_{L,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}[N]$ which is fixed elementwise by G. As in the proof of (3.3.1), we decompose N into its G-orbits. Since G acts on N by conjugation, $\{1_N\}$ is an orbit, so G does not act transitively on N, and therefore N may be decomposed into orbits of lengths 1 and p. We recall from (5.3.1) that ${}^g\rho = \rho$ for all $g \in G$ and ${}^\tau\eta = \eta, {}^\sigma\eta = \rho^d\eta$. The orbits of G in N of length 1 are therefore

$$\{\rho^k\} \text{ for } 0 \leq k \leq p-1,$$

and the orbits of G in N of length p are

$$\{\rho^k\eta^t \mid 0 \leq k \leq p-1\} \text{ for } 1 \leq t \leq p-1.$$

Since the set $\{\rho^k\eta^t \mid 0 \leq k, t \leq p-1\}$ is an $\mathfrak{O}_{L,\mathfrak{p}}$-basis for $\mathfrak{O}_{L,\mathfrak{p}}[N]$, it remains to show that for each $t \neq 0$, the set $\{\omega_{i,t} \mid 0 \leq i \leq p-1\}$ has the same $\mathfrak{O}_{L,\mathfrak{p}}$-span as the set $\{\rho^k\eta^t \mid 0 \leq k \leq p-1\}$. For a fixed $1 \leq t \leq p-1$ we calculate

$$e_s(a_v\eta)^t = e_s v^{st}\eta^t = \frac{1}{p}\sum_{k=0}^{p-1} \zeta^{-ks}\rho^k v^{st}\eta^t,$$

and so

$$\begin{aligned}
\omega_{i,t} &= p\pi_{\mathfrak{p}}^{-ie'} \sum_{s=0}^{i} \binom{i}{s} (-1)^{i-s} e_s (a_v \eta)^t \\
&= \pi_{\mathfrak{p}}^{-ie'} \sum_{s=0}^{i} \binom{i}{s} (-1)^{i-s} \sum_{k=0}^{p-1} \zeta^{-ks} \rho^k v^{st} \eta^t \\
&= \sum_{k=0}^{p-1} \left(\pi_{\mathfrak{p}}^{-ie'} \sum_{s=0}^{i} \binom{i}{s} (-1)^{i-s} \zeta^{-ks} v^{st} \right) \rho^k \eta^t \\
&= \sum_{k=0}^{p-1} \left(\frac{\zeta^{-k} v^t - 1}{\pi_{\mathfrak{p}}^{e'}} \right)^i \rho^k \eta^t.
\end{aligned}$$

In the "t -part" of the $\mathfrak{O}_{L,\mathfrak{p}}$-order $\mathfrak{O}_{L,\mathfrak{p}}[N]$, the matrix giving the change of generators $\rho^k \eta^t \mapsto \omega_{i,t}$ has $(i,k)^{th}$ element

$$\left(\frac{\zeta^{-k} v^t - 1}{\pi_{\mathfrak{p}}^{e'}} \right)^i.$$

It is a Vandermonde matrix, and therefore has determinant

$$\begin{aligned}
\prod_{0 \le j < k \le p-1} \left(\frac{\zeta^{-j} v^t - 1}{\pi_{\mathfrak{p}}^{e'}} - \frac{\zeta^{-k} v^t - 1}{\pi_{\mathfrak{p}}^{e'}} \right) &= \prod_{0 \le j < k \le p-1} \left(\frac{(\zeta^{-j} - \zeta^{-k}) v^t}{\pi_{\mathfrak{p}}^{e'}} \right) \\
&\sim \prod_{0 \le j < k \le p-1} \zeta^{-k} \left(\frac{\zeta^{k-j} - 1}{\pi_{\mathfrak{p}}^{e'}} \right) v^t.
\end{aligned}$$

Now since $v_{\mathfrak{p}} \left(\zeta^{k-j} - 1 \right) = e'$ for all choices of $j \neq k$, every factor in the product lies in $\mathfrak{O}_{L,\mathfrak{p}}^{\times}$, so this is indeed a change of basis. That the stated basis is fixed elementwise by G follows from (5.3.1). □

We also include the formulae for inverting the above, i.e. expressing $e_s (a_v \eta)^t$ in terms of the $\omega_{i,t}$ for each $t \neq 0$.

Proposition 6.2.2. Fix $1 \le t \le p-1$. Then for $0 \le j \le p-1$ we have

$$e_j (a_v \eta)^t = \frac{1}{p} \sum_{i=0}^{j} \binom{j}{i} \pi_{\mathfrak{p}}^{ie'} \omega_{i,t}$$

Proof. We calculate:

$$\begin{aligned}\frac{1}{p}\sum_{i=0}^{j}\binom{j}{i}\pi_{\mathfrak{p}}^{ie'}\omega_{i,t} &= \frac{1}{p}\sum_{i=0}^{j}\binom{j}{i}\pi_{\mathfrak{p}}^{ie'}p\pi_{\mathfrak{p}}^{-ie'}\sum_{s=0}^{i}\binom{i}{s}(-1)^{i-s}e_s(a_v\eta)^t \\ &= \sum_{i=0}^{j}\sum_{s=0}^{i}\binom{j}{i}\binom{i}{s}(-1)^{i-s}e_s(a_v\eta)^t.\end{aligned}$$

The coefficient of a given $e_s(a_v\eta)^t$ is

$$\sum_{i=s}^{j}\binom{j}{i}\binom{i}{s}(-1)^{i-s}.$$

Now

$$\begin{aligned}\binom{j}{i}\binom{i}{s} &= \frac{j!}{i!(j-i)!}\frac{i!}{s!(i-s)!} \\ &= \frac{j!}{s!(j-s)!}\frac{(j-s)!}{(j-i)!(i-s)!} \\ &= \binom{j}{s}\binom{j-s}{i-s}\end{aligned}$$

So, setting $k = i - s$, we obtain

$$\begin{aligned}\sum_{i=s}^{j}\binom{j}{i}\binom{i}{s}(-1)^{i-s} &= \binom{j}{s}\sum_{i=s}^{j}\binom{j-s}{i-s}(-1)^{i-s} \\ &= \binom{j}{s}\sum_{k=0}^{j-s}\binom{j-s}{k}(-1)^{k} \\ &= \begin{cases}1 & \text{if } s=j \\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

So

$$\frac{1}{p}\sum_{i=0}^{j}\binom{j}{i}\pi_{\mathfrak{p}}^{ie'}\omega_{i,t} = e_j(a_v\eta)^t.$$

□

Proposition 6.2.3. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p. Let $I = \mathfrak{p}\mathfrak{O}_{L,\mathfrak{p}}[N] +$

$\ker \varepsilon \lhd \mathfrak{O}_{L,\mathfrak{p}}[N]$. Then I^G is the maximal ideal of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$.

Proof. For $z \in \mathfrak{O}_{L,\mathfrak{p}}[N]^G$, let $[z]$ denote the class of z in $\mathfrak{O}_{L,\mathfrak{p}}[N]^G/I^G$. Now

$$\frac{\mathfrak{O}_{L,\mathfrak{p}}[N]^G}{I^G} \hookrightarrow \frac{\mathfrak{O}_{L,\mathfrak{p}}[N]}{I} \cong \prod_{\mathfrak{P}|\mathfrak{p}} \frac{\mathfrak{O}_{L,\mathfrak{P}}}{\mathfrak{P}\mathfrak{O}_{L,\mathfrak{P}}}$$

by

$$[z] = z + I^G \mapsto z + I,$$

so z corresponds to

$$(Z_1, \ldots, Z_g) \in \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{L,\mathfrak{P}}$$

and

$$(Z_1, \ldots, Z_g)^x = (Z_1, \ldots, Z_g) \quad \forall x \in G$$

so in fact $Z_1, \ldots, Z_g \in \mathfrak{O}_{K,\mathfrak{p}}$ and

$$\overline{Z}_1 = \ldots = \overline{Z}_g \in \frac{\mathfrak{O}_{K,\mathfrak{p}}}{\mathfrak{p}}.$$

So $z = c + I^G$ for some $c \in \mathfrak{O}_{K,\mathfrak{p}}$, and

$$\frac{\mathfrak{O}_{L,\mathfrak{p}}[N]^G}{I^G} \cong \frac{\mathfrak{O}_{K,\mathfrak{p}}}{\mathfrak{p}},$$

which is a field. Therefore I^G is a maximal ideal of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$, and is unique since the latter is a local ring. □

Corollary 6.2.4. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p, and let $z \in \mathfrak{O}_{L,\mathfrak{p}}[N]^G$. Then $z \in (\mathfrak{O}_{L,\mathfrak{p}}[N]^G)^\times$ if and only if $\varepsilon(z) \in \mathfrak{O}_{K,\mathfrak{p}}^\times$.

Chapter 7

Hopf-Galois Module Structure:

$p = 2$

We recall from (5.3.2) that for $p = 2$ we have the following isomorphism of K-algebras:

$$H \cong K^2 \times K(w),$$

where $w^2 = W = -V$, and so the following description of the unique maximal $\mathfrak{O}_K$-order in H:

$$\mathfrak{M}_H \cong \mathfrak{O}_K^2 \times \mathfrak{O}_{K(w)}.$$

Furthermore, from (5.3.6) and (5.3.9) we have that for $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, and for c and q as in (5.3.8), an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{M}_{H,\mathfrak{p}}$ is given by

$$\begin{cases} \left\{E_0, E_1, e_1, \frac{ce_1(a_v\eta)-e_1}{\pi_{\mathfrak{p}}^q}\right\} & \text{if } \mathfrak{p} \mid 2 \\ \left\{E_0, E_1, e_1, \frac{e_1(a_v\eta)}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(W)}}\right\} & \text{otherwise} \end{cases}$$

7.1 Sandwiching $\mathbf{Cl}\left(\mathfrak{A}_H\right)$

Proposition 7.1.1. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2, and write $2 = u\pi_{\mathfrak{p}}^e \in \mathfrak{O}_{K,\mathfrak{p}}$, with $u \in \mathfrak{O}_{K,\mathfrak{p}}^\times$. Let $z \in \mathfrak{M}_{H,\mathfrak{p}}$ and write

$$z = a_0E_0 + a_1E_1 + a_{1,0}e_1 + a_{1,1}\frac{ce_1(a_v\eta) - e_1}{\pi_{\mathfrak{p}}^q}$$

with $a_0, a_1, a_{1,0}, a_{1,1} \in \mathfrak{O}_{K,\mathfrak{p}}$ and c, q as in (5.3.8). Then $z \in \mathfrak{A}_{H,\mathfrak{p}}^\times$ if and only if

i) $a_{1,1} \equiv 0 \pmod{\pi_{\mathfrak{p}}^q}$

ii) $a_0 - a_1 + 2\pi_{\mathfrak{p}}^{-q}ca_{1,1} \equiv 0 \pmod 4$

iii) $a_0 + a_1 - 2a_{1,0} + 2\pi_{\mathfrak{p}}^{-q}a_{1,1} \equiv 0 \pmod 4$

iv) $a_0 + a_1 + 2a_{1,0} - 2\pi_{\mathfrak{p}}^{-q}a_{1,1} \equiv 0 \pmod 4$

v) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^\times$

Proof. We rewrite z in terms of the basis elements of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ given in (6.2.1). By (6.2.4), we then have that $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$ if and only if the coefficients of these basis elements lie in $\mathfrak{O}_{K,\mathfrak{p}}$ and $\varepsilon(z) \in \mathfrak{O}_{K,\mathfrak{p}}^\times$. We calculate:

$$\begin{aligned}
z &= a_0\frac{1}{2}\left(e_0 + e_0(a_v\eta)\right) + a_1\frac{1}{2}\left(e_0 - e_0(a_v\eta)\right) + a_{1,0}e_1 + a_{1,1}\pi_{\mathfrak{p}}^{-q}ce_1(a_v\eta) - a_{1,1}\pi_{\mathfrak{p}}^{-q}e_1 \\
&= \frac{1}{2}\left(a_0 + a_1\right)e_0 + a_{1,0}e_1 - \pi_{\mathfrak{p}}^{-q}a_{1,1}e_1 + \frac{1}{2}\left(a_0 - a_1\right)e_0(a_v\eta) + \pi_{\mathfrak{p}}^{-q}a_{1,1}ce_1(a_v\eta) \\
&= \frac{1}{2}\left(a_0 + a_1\right)\frac{1}{2}\left(1 + \rho\right) + a_{1,0}\frac{1}{2}\left(1 - \rho\right) - \pi_{\mathfrak{p}}^{-q}a_{1,1}\frac{1}{2}\left(1 - \rho\right) + \frac{1}{2}\left(a_0 - a_1\right)\frac{1}{2}\omega_{0,1} \\
&\quad + \pi_{\mathfrak{p}}^{-q}a_{1,1}c\left(\frac{\omega_{0,1}}{2} + u^{-1}\omega_{1,1}\right) \\
&= \frac{1}{4}\left(a_0 + a_1 + 2a_{1,0} - 2\pi_{\mathfrak{p}}^{-q}a_{1,1}\right) + \frac{1}{4}\left(a_0 + a_1 - 2a_{1,0} + 2\pi_{\mathfrak{p}}^{-q}a_{1,1}\right)\rho \\
&\quad + \frac{1}{4}\left(a_0 - a_1 + 2\pi_{\mathfrak{p}}^{-q}a_{1,1}c\right)\omega_{0,1} + \pi_{\mathfrak{p}}^{-q}a_{1,1}cu^{-1}\omega_{1,1}
\end{aligned}$$

Considering the coefficients of $\omega_{1,1}, \omega_{0,1}, \rho$ and 1 in turn now yields the congruence

conditions in parts (i)-(iv) of the proposition. Finally, we observe that

$$\varepsilon(z) = a_0\varepsilon(E_0) + a_1\varepsilon(E_1) + \left(a_{1,0} - \pi_{\mathfrak{p}}^{-q}a_{1,1}\right)\varepsilon(e_1) + \left(\pi_{\mathfrak{p}}^{-q}ca_{1,1}\right)\varepsilon(e_1(a_v\eta)).$$

Now

$$\varepsilon(e_s(a_v\eta)^t) = \begin{cases} 1 & \text{if } s = 0 \\ 0 & \text{if } s = 1 \end{cases}$$

and

$$\begin{aligned} \varepsilon(E_r) &= \frac{1}{2}\left(\varepsilon(e_0) + (-1)^r\varepsilon(e_0(a_v\eta))\right) \\ &= \begin{cases} 1 & \text{if } r = 0 \\ 0 & \text{if } r = 1 \end{cases} \end{aligned}$$

so $\varepsilon(z) = a_0$ and, assuming $z \in \mathfrak{O}_{L,\mathfrak{p}}[N]^G$, we have $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$ if and only if $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^\times$. □

We now seek necessary and sufficient conditions for $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$. These will be in terms of higher unit groups of $\mathfrak{O}_{K,\mathfrak{p}}$ and $\mathfrak{O}_{K(w),\mathfrak{p}}$.

Definition 7.1.2. Define an isomorphism

$$\Theta : (K^\times)^2 \times K(w)^\times \cong H^\times$$

by composing the automorphism of $(K^\times)^2 \times K(w)^\times$ defined by

$$(z_0, z_1, y_1) \mapsto (z_0, z_0z_1, z_0y_1)$$

with the isomorphism $K^2 \times K(w) \cong H$ defined in (5.3.2). We shall also write Θ for the induced isomorphism $(K_{\mathfrak{p}}^\times)^2 \times (K(w)_{\mathfrak{p}})^\times \cong H_{\mathfrak{p}}^\times$, where $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$, and the isomorphism $\mathbb{J}(K)^2 \times \mathbb{J}(K(w)) \cong \mathbb{J}(H)$.

Proposition 7.1.3. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2. Then

$$\Theta\left(\mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1+4\mathfrak{O}_{K,\mathfrak{p}}) \times (1+4\mathfrak{O}_{K(w),\mathfrak{p}})\right) \subseteq \mathfrak{A}_{H,\mathfrak{p}}^{\times}$$

Proof. The image under Θ of an element of

$$\mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1+4\mathfrak{O}_{K,\mathfrak{p}}) \times (1+4\mathfrak{O}_{K(w),\mathfrak{p}})$$

has the form

$$z = a_0E_0 + a_1E_1 + a_{1,0}e_1 + a_{1,1}\frac{ce_1(a_v\eta) - e_1}{\pi_{\mathfrak{p}}^q}$$

with $a_0, a_1, a_{1,0}, a_{1,1} \in \mathfrak{O}_{K,\mathfrak{p}}$ and

a) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$

b) $a_1 \equiv a_0 \pmod{4\mathfrak{O}_{K,\mathfrak{p}}}$

c) $a_{1,0} \equiv a_0 \pmod{4\mathfrak{O}_{K,\mathfrak{p}}}$

d) $a_{1,1} \equiv 0 \pmod{4\mathfrak{O}_{K,\mathfrak{p}}}$

We recall the conditions of (7.1.1):

i) $a_{1,1} \equiv 0 \pmod{\pi_{\mathfrak{p}}^q}$

ii) $a_0 - a_1 + 2\pi_{\mathfrak{p}}^{-q}ca_{1,1} \equiv 0 \pmod 4$

iii) $a_0 + a_1 - 2a_{1,0} + 2\pi_{\mathfrak{p}}^{-q}a_{1,1} \equiv 0 \pmod 4$

iv) $a_0 + a_1 + 2a_{1,0} - 2\pi_{\mathfrak{p}}^{-q}a_{1,1} \equiv 0 \pmod 4$

v) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$

and show that z satisfies these conditions.

i) Since $a_{1,1} \equiv 0 \pmod 4$ and $q \leq e$, we clearly have $a_{1,1} \equiv 0 \pmod{\pi_{\mathfrak{p}}^q}$.

ii) We have $a_1 - a_0 \equiv 0 \pmod 4$ and $a_{1,1} \equiv 0 \pmod 4$. Since $q \leq e$, we have $\pi_{\mathfrak{p}}^{e-q} a_{1,1} \equiv 0 \pmod 4$, and so the congruence holds.

iii) Since $a_0 \equiv a_1 \equiv a_{1,0} \pmod 4$, we have $a_0 + a_1 - 2a_{1,0} \equiv 0 \pmod 4$. Since $\pi_{\mathfrak{p}}^{e-q} a_{1,1} \equiv 0 \pmod 4$, the congruence holds.

iv) This is essentially the same as (iii)

v) We have that $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$ by (a).

□

Proposition 7.1.4. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above 2. Then

$$\Theta^{-1}\left(\mathfrak{A}_{H,\mathfrak{p}}^{\times}\right) \subseteq \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + 2\mathfrak{O}_{K,\mathfrak{p}}) \times (1 + \pi_{\mathfrak{p}}^{\left\lceil \frac{e_{\mathfrak{p}}}{2} \right\rceil} \mathfrak{O}_{K(w),\mathfrak{p}})$$

Proof. Let

$$z = a_0 E_0 + a_1 E_1 + a_{1,0} e_1 + a_{1,1} \frac{c e_1(a_v \eta) - e_1}{\pi_{\mathfrak{p}}^q}$$

with $a_0, a_1, a_{1,0}, a_{1,1} \in \mathfrak{O}_{K,\mathfrak{p}}$, and suppose that $z \in \mathfrak{A}_{H,\mathfrak{p}}^{\times}$. In particular, $a_0, a_1, a_{1,0}$ and $a_{1,1}$ satisfy the conditions of (7.1.1):

i) $a_{1,1} \equiv 0 \pmod{\pi_{\mathfrak{p}}^q}$

ii) $a_0 - a_1 + 2\pi_{\mathfrak{p}}^{-q} c a_{1,1} \equiv 0 \pmod 4$

iii) $a_0 + a_1 - 2a_{1,0} + 2\pi_{\mathfrak{p}}^{-q} a_{1,1} \equiv 0 \pmod 4$

iv) $a_0 + a_1 + 2a_{1,0} - 2\pi_{\mathfrak{p}}^{-q} a_{1,1} \equiv 0 \pmod 4$

v) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$.

We shall show that this implies

$$\Theta^{-1}(z) \in \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + 2\mathfrak{O}_{K,\mathfrak{p}}) \times (1 + \pi_{\mathfrak{p}}^{\left\lceil \frac{e_{\mathfrak{p}}}{2} \right\rceil} \mathfrak{O}_{K(w),\mathfrak{p}}).$$

Adding (iii) and (iv) yields $2a_0 + 2a_1 \equiv 0 \pmod 4$, which implies that $a_0 \equiv a_1 \pmod 2$. Adding (ii) and (iii) yields

$$2a_0 - 2a_{1,0} + 2(c+1)\pi_{\mathfrak{p}}^{-q} \equiv 0 \pmod 4,$$

which implies that

$$a_0 - a_{1,0} + (c+1)\pi_{\mathfrak{p}}^{-q} a_{1,1} \equiv 0 \pmod 2.$$

Now $\pi_{\mathfrak{p}}^{-q} a_{1,1} \in \mathfrak{O}_{K,\mathfrak{p}}$, and $v_{\mathfrak{p}}(c+1) \geq \lceil \frac{e_{\mathfrak{p}}}{2} \rceil$, so we obtain $a_{1,0} \equiv a_0 \pmod{\pi_{\mathfrak{p}}^{\lceil \frac{e_{\mathfrak{p}}}{2} \rceil}}$. Since we also have from (i) that $a_{1,1} \equiv 0 \pmod{\pi_{\mathfrak{p}}^{q}}$ and from (v) that $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$, the result follows. □

Proposition 7.1.5. Define an ideal $\mathfrak{e}$ of $\mathfrak{O}_K$ by

$$\mathfrak{e} = \prod_{\mathfrak{p} | 2\mathfrak{O}_K} \mathfrak{p}^{\lceil \frac{e_{\mathfrak{p}}}{2} \rceil},$$

where $e_{\mathfrak{p}} = v_{\mathfrak{p}}(2)$. Then there are injections:

$$\begin{array}{ccc} \mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_4(\mathfrak{O}_K) \times \mathbb{U}_4(\mathfrak{O}_{K(w)}) \\ \downarrow \\ \mathbb{U}(\mathfrak{A}_H) \\ \downarrow \\ \mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_2(\mathfrak{O}_K) \times \mathbb{U}_{\mathfrak{e}}(\mathfrak{O}_{K(w)}) \end{array}$$

and therefore surjections:

$$\begin{array}{ccccc} \mathrm{Cl}\left(\mathfrak{O}_K\right) & \times & \mathrm{Cl}_4(\mathfrak{O}_K) & \times & \mathrm{Cl}_4(\mathfrak{O}_{K(w)}) \\ & & \downarrow & & \\ & & \mathrm{Cl}\left(\mathfrak{A}_H\right) & & \\ & & \downarrow & & \\ \mathrm{Cl}\left(\mathfrak{O}_K\right) & \times & \mathrm{Cl}_2(\mathfrak{O}_K) & \times & \mathrm{Cl}_{\mathfrak{e}}(\mathfrak{O}_{K(w)}) \end{array}$$

Proof. Recall from (2.1.21) that

$$\mathbb{U}(\mathfrak{A}_H) = \prod_{\mathfrak{p} \lhd \mathfrak{O}_K} \mathfrak{A}_{H,\mathfrak{p}}^{\times} = \left\{ (a_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbb{J}(H) \mid a_{\mathfrak{p}} \in \mathfrak{A}_{H,\mathfrak{p}}^{\times} \text{ for all } \mathfrak{p} \right\}.$$

By (6.1.1) and (5.3.4) we have that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which does not lie above 2 then

$$\mathfrak{A}_{H,\mathfrak{p}}^{\times} = \mathfrak{M}_{H,\mathfrak{p}}^{\times} \cong \left(\mathfrak{O}_{K,\mathfrak{p}}^{\times}\right)^2 \times \mathfrak{O}_{K(w),\mathfrak{p}}^{\times}.$$

From (7.1.4) and (7.1.3) we have that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which lies above 2 then there are injections:

$$\begin{array}{c} \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + 4\mathfrak{O}_{K,\mathfrak{p}}) \times \left(1 + 4\mathfrak{O}_{K(w),\mathfrak{p}}\right) \\ \downarrow \\ \mathfrak{A}_{H,\mathfrak{p}}^{\times} \\ \downarrow \\ \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1 + 2\mathfrak{O}_{K,\mathfrak{p}}) \times \left(1 + \pi_{\mathfrak{p}}^{\left\lceil \frac{e_{\mathfrak{p}}}{2} \right\rceil} \mathfrak{O}_{K(w),\mathfrak{p}}\right) \end{array}$$

where $e_{\mathfrak{p}} = v_{\mathfrak{p}}(2)$. Recalling definition (2.1.20), this implies that there are injections

$$\begin{array}{c} \mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_4(\mathfrak{O}_K) \times \mathbb{U}_4(\mathfrak{O}_{K(w)}) \\ \downarrow \\ \mathbb{U}(\mathfrak{A}_H) \\ \downarrow \\ \mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_2(\mathfrak{O}_K) \times \mathbb{U}_{\mathfrak{e}}(\mathfrak{O}_{K(w)}). \end{array}$$

The existence of the surjections asserted by the proposition then follows from the isomorphism (see (2.1.25))

$$\mathrm{Cl}\,(\mathfrak{A}_H) \cong \frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathfrak{A}_H)}.$$

□

7.2 The Class Representing $\mathfrak{O}_L$

Proposition 7.2.1. The class of $\mathfrak{O}_L$ in the locally free class group

$$\mathrm{Cl}\,(\mathfrak{A}_H) \cong \frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathfrak{A}_H)}$$

corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$, where $h_{\mathfrak{p}}$ is defined by

$$h_{\mathfrak{p}} = \begin{cases} E_0 + E_1 + e_1 + e_1(a_v\eta) & \mathfrak{p} \mid 2\mathfrak{O}_K \\ E_0 + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)} E_1 + \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}})} e_1(a_v\eta)^{j_{\mathfrak{p}}} & \mathfrak{p} \mid XV\mathfrak{O}_K \\ 1 & \text{otherwise} \end{cases}$$

and where (see (6.1.2)):

$$j_{\mathfrak{p}} = \begin{cases} 1 & \text{if } v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(V) \equiv 1 \pmod 2 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Define

$$\Gamma = \frac{1}{4}\left(1 + v + x\right).$$

Using the formulae for the action of the K-basis elements of H on those of L in (5.4.3) and (5.4.4), we see that Γ is a generator of L over H. By (2.1.25), to show that the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\left(\mathfrak{A}_H\right)$ corresponds to the class of the idèle $(h_\mathfrak{p})_\mathfrak{p}$ in $\mathbb{J}(H)/H^\times\mathbb{U}(\mathfrak{A}_H)$ we must show that for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$, the element $h_\mathfrak{p}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. We recall the local generators $\gamma_\mathfrak{p}$ given in (6.1.2) and (6.1.7):

$$\gamma_\mathfrak{p} = \begin{cases} \frac{1}{4}\left(1 + x + v + xv\right) & \text{if } \mathfrak{p} \mid 2\mathfrak{O}_K \\ 1 + \pi_\mathfrak{p}^{-r_\mathfrak{p}(V)}v + \pi_\mathfrak{p}^{-r_\mathfrak{p}(XV^{j_\mathfrak{p}})}xv^{j_\mathfrak{p}} & \text{otherwise} \end{cases}$$

Suppose first that $\mathfrak{p} \nmid 2XV\mathfrak{O}_K$. Then $h_\mathfrak{p} = 1$ and so

$$h_\mathfrak{p}\Gamma = \frac{1}{4}\left(1 + v + x\right),$$

whereas

$$\gamma_\mathfrak{p} = 1 + v + x.$$

We note that $\mathfrak{p} \nmid 2\mathfrak{O}_K$ and so $4 \in \mathfrak{O}_{K,\mathfrak{p}}^\times$. Therefore we have that $h_\mathfrak{p}\Gamma$ and $\gamma_\mathfrak{p}$ differ only by an element of $\mathfrak{O}_{K,\mathfrak{p}}^\times$, and so $h_\mathfrak{p}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. Next suppose that $\mathfrak{p} \mid XV\mathfrak{O}_K$. Then

$$\begin{aligned} h_\mathfrak{p}\Gamma &= E_0\Gamma + \pi_\mathfrak{p}^{-r_\mathfrak{p}(V)}E_1\Gamma + \pi_\mathfrak{p}^{-r_\mathfrak{p}(XV^{j_\mathfrak{p}})}e_1(a_v\eta)^{j_\mathfrak{p}}\Gamma \\ &= \frac{1}{4}\left(1 + \pi_\mathfrak{p}^{-r_\mathfrak{p}(V)}v + \pi_\mathfrak{p}^{-r_\mathfrak{p}(XV^{j_\mathfrak{p}})}xv^{j_\mathfrak{p}}\right) \end{aligned}$$

whereas

$$\gamma_\mathfrak{p} = 1 + \pi_\mathfrak{p}^{-r_\mathfrak{p}(V)}v + \pi_\mathfrak{p}^{-r_\mathfrak{p}(XV^{j_\mathfrak{p}})}xv^{j_\mathfrak{p}}.$$

Again, since $\mathfrak{p} \nmid 2\mathfrak{O}_K$ we have that $4 \in \mathfrak{O}_{K,\mathfrak{p}}^\times$. Therefore $h_\mathfrak{p}\Gamma$ and $\gamma_\mathfrak{p}$ differ only by an element of $\mathfrak{O}_{K,\mathfrak{p}}^\times$, and so $h_\mathfrak{p}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. Finally suppose

that $\mathfrak{p} \mid 2\mathfrak{O}_K$. Then

$$\begin{aligned} h_{\mathfrak{p}}\Gamma &= E_0\Gamma + E_1\Gamma + e_1\Gamma + e_1(a_v\eta)\Gamma \\ &= \frac{1}{4}(1 + v + x + xv) \\ &= \gamma_{\mathfrak{p}} \end{aligned}$$

So in this case $h_{\mathfrak{p}}\Gamma$ coincides with the generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ given in (6.1.7). This completes the proof. □

Remark 7.2.2. By (5.2.1), a nonclassical Hopf-Galois structure on L/K is determined by a choice of subgroup T of $G = \mathrm{Gal}(L/K)$ of order 2. This choice also determines the field $K(w)$ appearing in the isomorphism of K-algebras $H \cong K^2 \times K(w)$. In (5.2.1) we chose an element $\tau \in G$ such that $T = \langle\tau\rangle$ and an element $\sigma \in G$ such that $G = \langle\sigma, \tau\rangle$. Making a different choice of this element σ will result in a different description of the field L and Hopf algebra H, but it will not affect the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$ because this does not depend on the descriptions of the objects involved. In this case, if we denote by σ' a different group element satisfying $\langle\sigma', \tau\rangle = G$, then since $|G| = 4$ we must have that $\sigma' = \sigma\tau$. Making this choice would lead to a change of K-basis of L:

$$\begin{aligned} v &\mapsto v \\ x &\mapsto x' = xv \end{aligned}$$

and a change of K-basis of H:

$$\begin{aligned} E_r &\mapsto E_r && \text{for } r = 0, 1 \\ e_1(a_v\eta)^t &\mapsto (-1)^t e_1(a_v\eta)^t && \text{for } t = 0, 1. \end{aligned}$$

Definition 7.2.3. For $y \in K$, define the fractional ideal

$$I_y = \prod_{\mathfrak{p} | y\mathfrak{O}_K} \mathfrak{p}^{r_\mathfrak{p}(y)}.$$

Proposition 7.2.4. Under the composition of maps

$$\mathbb{J}(H) \to \mathbb{J}(K)^2 \times \mathbb{J}(K(w)) \to \mathrm{Cl}\left(\mathfrak{O}_K\right)^2 \times \mathrm{Cl}\left(\mathfrak{O}_{K(w)}\right),$$

the idèle $(h_\mathfrak{p})_\mathfrak{p}$ is mapped to the triple of classes of fractional ideals

$$\left(\mathfrak{O}_K, I_W^{-1}, \left(I_X^{-1} \prod_{\substack{\mathfrak{P} | (1+w) \\ \mathfrak{P} \nmid 2\mathfrak{O}_{K(w)}}} \mathfrak{P}^{-v_\mathfrak{P}(1+w)} \prod_{\substack{v_\mathfrak{p}(W) \equiv 1 \pmod 2 \\ v_\mathfrak{p}(X) \equiv 1 \pmod 2}} \mathfrak{P}^{-1}\right)\right).$$

Proof. Under the isomorphism

$$\mathbb{J}(H) \cong \mathbb{J}(K)^2 \times \mathbb{J}(K(w))$$

the idèle $(h_\mathfrak{p})_\mathfrak{p}$ is mapped to the triple of idèles

$$\left((1)_\mathfrak{p}, \left(\pi_\mathfrak{p}^{-r_\mathfrak{p}(W)}\right)_\mathfrak{p}, (y_\mathfrak{p})_\mathfrak{p}\right),$$

where

$$y_\mathfrak{p} = \begin{cases} 1 + w & \mathfrak{p} \mid 2\mathfrak{O}_K \\ \pi_\mathfrak{p}^{-r_\mathfrak{p}(XW)} w & v_\mathfrak{p}(X) \equiv v_\mathfrak{p}(W) \equiv 1 \pmod 2 \\ \pi_\mathfrak{p}^{-r_\mathfrak{p}(X)} & \text{otherwise.} \end{cases}$$

since by (6.1.3) we have $j_\mathfrak{p} = 1$ if $v_\mathfrak{p}(X) \equiv v_\mathfrak{p}(W) \equiv 1 \pmod 2$ and $j_\mathfrak{p} = 0$ otherwise. If $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ then we use the isomorphism in (2.1.17) to obtain from $y_\mathfrak{p}$ elements $y_\mathfrak{P} \in K(w)_\mathfrak{P}$ for each prime $\mathfrak{P}$ of $\mathfrak{O}_{K(w)}$ lying above $\mathfrak{p}$ as follows: If $\mathfrak{P}$ is the only prime of $\mathfrak{O}_{K(w)}$ lying above $\mathfrak{p}$ then $y_\mathfrak{P} = y_\mathfrak{p}$. If two primes of $\mathfrak{O}_{K(w)}$

lie above $\mathfrak{p}$ then $y_{\mathfrak{P}} = y_{\mathfrak{p}}$ and $y_{\sigma\mathfrak{P}} = \sigma y_{\mathfrak{p}}$, where σ is a generator for the Galois group of $K(w)/K$. Thus the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ corresponds to the triple of idèles

$$\left((1)_{\mathfrak{p}}, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(W)}\right)_{\mathfrak{p}}, \left((1+w)y'_{\mathfrak{P}}\right)_{\mathfrak{P}}\right),$$

where

$$y'_{\mathfrak{P}} = \begin{cases} 1 & \mathfrak{P} \mid 2\mathfrak{O}_{K(w)} \\ (1+w)^{-1}\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X)} & \mathfrak{P} \mid (1+w)\mathfrak{O}_{K(w)}, \mathfrak{P} \nmid 2\mathfrak{O}_{K(w)} \\ \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(XW)} w & v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(W) \equiv 1 \pmod 2 \text{ and } \mathfrak{P} \mid \mathfrak{p} \\ \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X)} & \text{otherwise} \end{cases}$$

Since $(1+w) \in K(w)^{\times}$, this triple of idèles has the same class in the product $\mathrm{Cl}(\mathfrak{O}_K)^2 \times \mathrm{Cl}\left(\mathfrak{O}_{K(w)}\right)$ as the triple of idèles

$$\left((1)_{\mathfrak{p}}, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(W)}\right)_{\mathfrak{p}}, \left(y'_{\mathfrak{P}}\right)_{\mathfrak{P}}\right).$$

We use the homomorphism defined in (2.1.19), applied to each component, to map this triple of idèles to a triple of fractional ideals. We see immediately that the first component corresponds to the trivial ideal, and that the second component corresponds to the fractional ideal I_W^{-1}. In the third component we calculate:

$$v_{\mathfrak{P}}\left(y'_{\mathfrak{P}}\right) = \begin{cases} 0 & \mathfrak{P} \mid 2\mathfrak{O}_{K(w)} \\ -v_{\mathfrak{P}}(1+w) - v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X)}\right) & \mathfrak{P} \mid (1+w)\mathfrak{O}_{K(w)}, \mathfrak{P} \nmid 2\mathfrak{O}_{K(w)} \\ -v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X)}\right) - 1 & v_{\mathfrak{p}}(X) \equiv v_{\mathfrak{p}}(W) \equiv 1 \pmod 2 \text{ and } \mathfrak{B} \mid \mathfrak{p} \\ -v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X)}\right) & \text{otherwise} \end{cases}$$

and so this component corresponds to the fractional ideal

$$\left(I_X^{-1} \prod_{\substack{\mathfrak{P} | (1+w)\mathfrak{O}_{K(w)} \\ \mathfrak{P} \nmid 2\mathfrak{O}_{K(w)}}} \mathfrak{P}^{-v_{\mathfrak{P}}(1+w)} \prod_{\substack{v_{\mathfrak{p}}(W) \equiv 1 \pmod 2 \\ v_{\mathfrak{p}}(X) \equiv 1 \pmod 2}} \mathfrak{P}^{-1} \right).$$

□

7.3 Conditions for Global Freeness

Proposition 7.3.1. A sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$ is that the triple of fractional ideals given in (7.2.4) has trival class in the product of ray class groups

$$\mathrm{Cl}\,(\mathfrak{O}_K) \times \mathrm{Cl}_4(\mathfrak{O}_K) \times \mathrm{Cl}_4(\mathfrak{O}_{K(w)}).$$

A necessary condition is that the same triple has trivial class in the product of ray class groups

$$\mathrm{Cl}\,(\mathfrak{O}_K) \times \mathrm{Cl}_2(\mathfrak{O}_K) \times \mathrm{Cl}_{\mathfrak{e}}(\mathfrak{O}_{K(w)}).$$

Proof. By (7.2.1), the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$ corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ in $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$. Recalling the surjections of (7.1.5), the result follows. □

Proposition 7.3.2. Let K be a number field such that $h_4(K)$ is odd. Define an ideal $\mathfrak{t}$ of $\mathfrak{O}_K$ by

$$\mathfrak{t} = \prod_{\mathfrak{p} | 2\mathfrak{O}_K} \mathfrak{p}.$$

Then

$$\mathrm{Cl}_4(\mathfrak{O}_K) \cong \mathrm{Cl}_{\mathfrak{t}}(\mathfrak{O}_K).$$

Proof. This proposition differs only slightly from [BS05, Lemma 4.1]. There is a natural surjection

$$\phi : \mathrm{Cl}_4(\mathfrak{O}_K) \to \mathrm{Cl}_{\mathfrak{t}}(\mathfrak{O}_K).$$

with kernel

$$\ker \phi = \frac{K^\times \mathbb{U}_\mathfrak{t}(\mathfrak{O}_K)}{K^\times \mathbb{U}_4(\mathfrak{O}_K)}.$$

Let

$$E_\mathfrak{t}(\mathfrak{O}_K) = K^\times \cap \mathbb{U}_\mathfrak{t}(\mathfrak{O}_K).$$

Then

$$\ker \phi \cong \frac{\mathbb{U}_\mathfrak{t}(\mathfrak{O}_K)}{E_\mathfrak{t}(\mathfrak{O}_K)\mathbb{U}_4(\mathfrak{O}_K)},$$

so $\ker \phi$ is isomorphic to a quotient of $\mathbb{U}_\mathfrak{t}(\mathfrak{O}_K)/\mathbb{U}_4(\mathfrak{O}_K)$, a group of 2-power order. But also $\ker \phi$ is a subgroup of $\mathrm{Cl}_4(\mathfrak{O}_K)$, which has odd order by hypothesis. Therefore $\ker \phi$ is trivial and ϕ is an isomorphism. □

Proposition 7.3.3. Suppose that $h_4(K)$ and $h_4(K(w))$ are both odd. Then

$$\mathrm{Cl}\,(\mathfrak{A}_H) \cong \mathrm{Cl}\,(\mathfrak{O}_K) \times \mathrm{Cl}_2(\mathfrak{O}_K) \times \mathrm{Cl}_\mathfrak{e}(\mathfrak{O}_{K(w)}),$$

and so $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ if and only if the triple of fractional ideals given in (7.2.4) has trival class in this product of ray class groups.

Proof. By (7.3.2), we have both

$$\mathrm{Cl}_4(\mathfrak{O}_K) \cong \mathrm{Cl}_\mathfrak{t}(\mathfrak{O}_K)$$

and

$$\mathrm{Cl}_4(\mathfrak{O}_{K(w)}) \cong \mathrm{Cl}_\mathfrak{t}(\mathfrak{O}_{K(w)}).$$

Therefore the surjections given in (7.1.5) are in fact isomorphisms, and the result follows. □

7.4 Tame Biquadratic Extensions of $\mathbb{Q}$

In this section we take $K = \mathbb{Q}$. By (4.2.4), a tame biquadratic extension L of $\mathbb{Q}$ has the form $L = \mathbb{Q}(\alpha, \beta)$, where $\alpha^2 = a, \beta^2 = b$ and a, b are squarefree integers both congruent to 1 modulo 4. By (5.1.3), such an extension admits precisely 3 nonclassical Hopf-Galois structures, and by (5.2.1), each structure is determined by a choice of subgroup T of $G = \mathrm{Gal}(L/\mathbb{Q})$ of order 2. We have fixed a generator τ of T and an element $\sigma \in G$ such that $G = \langle \sigma, \tau \rangle$. We have also fixed elements $x \in \mathfrak{O}_L^S$ and $v \in \mathfrak{O}_L^T$ satisfying $\tau(x) = -x$, $\sigma(v) = -v$ and $L = K(x, v)$. We are free to replace the element x by $xv/\gcd(X, V)$ (corresponding to replacing the element $\sigma \in G$ by $\sigma\tau$); by (7.2.2) this does not affect the class of $\mathfrak{O}_L$ in $\mathrm{Cl}(\mathfrak{A}_H)$. We may assume without loss of generality that $x^2 = X$ and $v^2 = V$ are squarefree integers.

By (5.3.2) we have the following isomorphism of $\mathbb{Q}$-algebras:

$$H \cong \mathbb{Q}^2 \times \mathbb{Q}(w),$$

where $w^2 = W = -V$. We shall write $F = \mathbb{Q}(w)$. Since $V \equiv 1 \pmod 4$, we have $W \equiv -1 \pmod 4$. Thus $\mathrm{Disc}(F) = 4W$, and so $F/\mathbb{Q}$ is wildly ramified at 2. Also $\mathfrak{O}_F = \mathbb{Z}[w]$.

Proposition 7.4.1. The ring of integers $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ if and only if there exist integers m_0, m_1 satisfying

$$m_0^2 + Vm_1^2 = \pm 2\gcd(X, V) \tag{7.1}$$

Proof. Recall from (7.2.3) that for $y \in \mathbb{Q}$ we define the fractional ideal I_y by

$$I_y = \prod_{p|y} p^{r_p(y)}.$$

Since X, V are squarefree integers we have $v_p(X) \equiv v_p(V) \equiv 1 \pmod 2$ if and only if $p \mid \gcd(X, V)$, and so by (7.3.1), a sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$ is that the triple of fractional ideals

$$\left(\mathbb{Z}, I_W^{-1}, \left(I_X^{-1} \prod_{\substack{\mathfrak{P} \mid (1+w)\mathfrak{O}_F \\ \mathfrak{P} \nmid 2\mathfrak{O}_F}} \mathfrak{P}^{-v_{\mathfrak{P}}(1+w)} \prod_{\substack{p \mid \gcd(X,V) \\ \mathfrak{P} \mid p\mathfrak{O}_F}} \mathfrak{P}^{-1} \right) \right)$$

has trivial class in the product of ray class groups

$$\mathrm{Cl}(\mathbb{Z}) \times \mathrm{Cl}_4(\mathbb{Z}) \times \mathrm{Cl}_4(\mathfrak{O}_F).$$

We show first that this is equivalent to the fractional ideal

$$J = \prod_{\substack{\mathfrak{P} \mid (1+w)\mathfrak{O}_F \\ \mathfrak{P} \nmid 2\mathfrak{O}_F}} \mathfrak{P}^{-v_{\mathfrak{P}}(1+w)} \prod_{\substack{p \mid \gcd(X,V) \\ \mathfrak{P} \mid p\mathfrak{O}_F}} \mathfrak{P}^{-1}$$

having trivial class in the ray class group $\mathrm{Cl}_4(\mathfrak{O}_F)$. We note that since X and W are squarefree, we have $r_p(W) = r_p(X) = 0$ for all prime numbers p. So $I_W = I_X = \mathbb{Z}$, and therefore the first two terms of the triple of ideals above automatically have trivial class in $\mathrm{Cl}(\mathbb{Z}) \times \mathrm{Cl}_4(\mathbb{Z})$, and the third term has trivial class in $\mathrm{Cl}_4(\mathfrak{O}_F)$ if and only if the ideal J has trivial class in $\mathrm{Cl}_4(\mathfrak{O}_F)$. Next we show that J is a principal fractional ideal if and only if the equation (7.1) has a solution in integers. We recall from above that 2 is ramified in F, and write $2\mathfrak{O}_F = \mathfrak{P}_2^2$. Then $\mathfrak{P}_2 \mid\mid (1+w)\mathfrak{O}_F$, since $2 \mid\mid N_{F/\mathbb{Q}}(1+w)$ in $\mathbb{Z}$. Also we have

$$\gcd(X, V)\mathfrak{O}_F = \left(\prod_{\substack{p \mid \gcd(X,V) \\ \mathfrak{P} \mid p\mathfrak{O}_F}} \mathfrak{P} \right)^2,$$

and so we have

$$(1+w)\gcd(X,V)J\mathfrak{O}_F = \mathfrak{P}_2 \prod_{\substack{\mathfrak{P}\mid p\mathfrak{O}_F \\ p\mid \gcd(X,V)}} \mathfrak{P}.$$

Therefore $J = \lambda F$ for some $\lambda \in F$ if and only if there exists some element $\mu = (1+w)\gcd(X,V)\lambda \in \mathfrak{O}_F$ such that

$$2\gcd(X,V)\mathfrak{O}_F = (\mu\mathfrak{O}_F)^2.$$

Taking norms, this is equivalent to the existence of an element $\mu = m_0 + m_1 w \in \mathfrak{O}_F$ satisfying

$$N_{F/\mathbb{Q}}(\mu)^2 = (2\gcd(X,V))^2$$

i.e.

$$m_0^2 + Vm_1^2 = \pm 2\gcd(X,V)$$

Finally we show that if J is a principal fractional ideal, then it has trivial class in $\mathrm{Cl}_4(\mathfrak{O}_F)$, i.e. it has a generator congruent to 1 $(\mathrm{mod}^*\ 4\mathfrak{O}_F)$. Suppose J is principal and let λ, μ be as above. Then certainly m_0, m_1 are odd integers, and replacing m_i by $-m_i$ if necessary we may assume that $m_i \equiv 1 \pmod 4$ for $i = 0, 1$. So $\mu \equiv (1+w) \pmod{4\mathfrak{O}_F}$. Recall that $\mathfrak{P}_2$ is the unique prime of $\mathfrak{O}_F$ lying above 2 and that $v_{\mathfrak{P}_2}(2) = 2$. Then

$$\begin{aligned}
\mu = (1+w)\gcd(X,V)\lambda \quad &\Rightarrow \quad v_{\mathfrak{P}_2}\left((1+w)\gcd(X,V)\lambda - (1+w)\right) \geq 4 \\
&\Rightarrow \quad v_{\mathfrak{P}_2}(1+w) + v_{\mathfrak{P}_2}\left(\gcd(X,V)\lambda - 1\right) \geq 4 \\
&\Rightarrow \quad v_{\mathfrak{P}_2}\left(\gcd(X,V)\lambda - 1\right) \geq 3 \\
&\Rightarrow \quad \gcd(X,V)\lambda \equiv 1 \ (\mathrm{mod}^*\ 2\mathfrak{O}_F) \\
&\Rightarrow \quad \pm\lambda \equiv 1 \ (\mathrm{mod}^*\ 4\mathfrak{O}_F)
\end{aligned}$$

So, since λ is a generator for J, there exists a generator of J congruent to 1 $(\mathrm{mod}^*\ 4\mathfrak{O}_F)$.

□

7.5 Examples

If $L/\mathbb{Q}$ is a tame biquadratic extension, then by Leopoldt's theorem ([Leo59]) $\mathfrak{O}_L$ is free over the associated order $\mathfrak{A}_{\mathbb{Q}[G]} = \mathbb{Z}[G]$ in the classical Hopf-Galois structure $\mathbb{Q}[G]$. In this section we show that the analogous result does not hold for the 3 nonclassical Hopf-Galois structure admitted by the extension. We give examples of classes of extension where $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in $0, 1$ and 2 of the nonclassical structures, and show that $\mathfrak{O}_L$ cannot be free over $\mathfrak{A}_H$ in all 3 nonclassical structures simultaneously.

Example 7.5.1. Let p, q be prime numbers satisfiying $p \equiv q \equiv 1 \pmod 4$. Let $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Then $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in any of the three nonclassical Hopf-Galois structures admitted by the extension.

Proof. Each of the three nonclassical strutures admitted by $L/\mathbb{Q}$ corresponds to a choice of element $v \in \mathfrak{O}_L$, which appears in equation (7.1). By (7.2.2) we have some freedom in each case to make a convenient choice of the element x without affecting the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$. We consider the following 3 cases, each corresponding to the freeness of $\mathfrak{O}_L$ over $\mathfrak{A}_H$ in one of the nonclassical Hopf-Galois structures admitted by $L/\mathbb{Q}$:

i) The choices $v = \sqrt{p}, x = \sqrt{q}$ lead us to consider the equation $m_0^2 + pm_1^2 = \pm 2$. This has no solutions in integers since a solution (m_0, m_1) would satisfy $|m_0^2 + pm_1^2| = 2$, which is impossible.

ii) The choices $v = \sqrt{q}, x = \sqrt{p}$ lead us to consider the equation $m_0^2 + qm_1^2 = \pm 2$. This has no solutions in integers for similar reasons as equation (i).

iii) The choices $v = \sqrt{pq}, x = \sqrt{p}$ lead us to consider the equation $m_0^2 + pqm_1^2 = \pm 2p$. Suppose that (m_0, m_1) is an integer solution of this equation. Then

$m_0^2 = \pm 2p - pqm_1^2$, which implies that $p \mid m_0^2$, and so $p \mid m_0$. Write $m_0 = pm_2$. Then (m_1, m_2) is an integer solution of the equation $pm_2^2 + qm_1^2 = \pm 2$. This implies that $|pm_2^2 + qm_1^2| = 2$ which is impossible.

Thus $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in any of the Hopf-Galois structures admitted by the extension. □

Example 7.5.2. Let p, q be prime numbers satisfying $p \equiv q \equiv -1 \pmod 4$. Let $L = \mathbb{Q}(\sqrt{-p}, \sqrt{-q})$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in precisely two of the three nonclassical Hopf-Galois structures admitted by the extension.

Proof. Each of the three nonclassical strutures admitted by $L/\mathbb{Q}$ corresponds to a choice of element $v \in \mathfrak{O}_L$, which appears in equation (7.1). By (7.2.2) we have some freedom in each case to make a convenient choice of the element x without affecting the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$. We show first that $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{pq}, x = \sqrt{-p}$. For this would imply that there exist integers m_0, m_1 satisfying

$$m_0^2 + pqm_1^2 = \pm 2p,$$

which would imply that there exist integers m_1, m_2 satisfying

$$|pm_2^2 + qm_1^2| = 2,$$

which is impossible. We now show that $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{-p}, x = \sqrt{-q}$. The argument for the choices $v = \sqrt{-q}, x = \sqrt{-p}$ is analogous. Let $F = \mathbb{Q}(\sqrt{p})$. By (7.4.1) freeness is equivalent to the existence of a principal ideal of $\mathfrak{O}_F$ of norm ± 2. Since $\mathrm{Disc}\,(\mathfrak{O}_F) = 4p$ we have that 2 is ramified, and in fact $2\mathfrak{O}_F = I^2$, where $I = 2\mathfrak{O}_F + (1 + \sqrt{p})\mathfrak{O}_F$. So I is an ideal of norm 2, and it will suffice to show that I is principal. To do this, it suffices to show that $|\mathrm{Cl}\,(\mathfrak{O}_F)|$ is odd. We use [FT91, Theorem 39, Corollary 1].

Since F is real, we need to establish whether the fundamental unit η has norm 1 or -1. We write $\eta = x + y\sqrt{p}$ and consider

$$\mathrm{N}_{F/\mathbb{Q}}(\eta) = x^2 - py^2.$$

Since $p \equiv -1 \pmod 4$ we have that -1 is not a quadratic residue mod p, so $\mathrm{N}_{F/\mathbb{Q}}(\eta) = -1$ is impossible, and so the fundamental unit must have norm 1. Now by [FT91, Theorem 39, Corollary 1] the 2-part of $\mathrm{Cl}\,(\mathfrak{O}_F)$ has order 2^{g-2}, where g is the number of distinct prime divisors of $\mathrm{Disc}\,(\mathfrak{O}_F)$. Since $\mathrm{Disc}\,(\mathfrak{O}_F) = 4p$, we have $g = 2$ and so conclude that $|\mathrm{Cl}\,(\mathfrak{O}_F)|$ is odd. Therefore I is a principal ideal of norm ± 2 and $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choice $v = \sqrt{-p}$. Thus $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in precisely two of the three nonclassical Hopf-Galois strcture admitted by the extension. □

Example 7.5.3. Let p, q be prime numbers satisfying $p \equiv q \equiv -1 \pmod 4$ and let r be a prime number satisfying $r \equiv 1 \pmod 8$. Let $L = \mathbb{Q}(\sqrt{-p}, \sqrt{-qr})$. Then $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in precisely one of the three nonclassical Hopf-Galois structures admitted by the extension.

Proof. Each of the three nonclassical structures admitted by $L/\mathbb{Q}$ corresponds to a choice of element $v \in \mathfrak{O}_L$, which appears in equation (7.1). By (7.2.2) we have some freedom in each case to make a convenient choice of the element x without affecting the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$. By the argument presented above, $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{-p}, x = \sqrt{-qr}$. If $\mathfrak{O}_L$ were free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{pqr}, x = \sqrt{-p}$ then there would exist integers m_0, m_1 satisfying

$$m_0^2 + pqrm_1^2 = \pm 2p,$$

which would imply that there exist integers m_1, m_2 satisfying

$$pm_2^2 + qrm_1^2 = \pm 2,$$

which is impossible. Finally we show that $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{-qr}, x = \sqrt{-p}$. This would imply that there exist integers m_0, m_1 satisfying

$$m_0^2 - qrm_1^2 = \pm 2.$$

If we reduce this equation modulo r then we have a solution to

$$m_0^2 \equiv \pm 2 \pmod{r}.$$

But $r \equiv 1 \pmod 8$, so neither of ± 2 is a quadratic residue modulo r, and so this is impossible. Thus $\mathfrak{O}_L$ is free over $\mathfrak{A}_H$ in precisely one of the three nonclassical Hopf-Galois structures admitted by the extension. □

Example 7.5.4. Let $L/\mathbb{Q}$ be a tame biquadratic extension. Then $\mathfrak{O}_L$ is not simultaneously free over $\mathfrak{A}_H$ in all three of the nonclassical Hopf-Galois structures admitted by the extension.

Proof. Write $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \in \mathbb{Z}/\mathbb{Z}^2$ and $a \equiv b \equiv 1 \pmod 4$. By (7.2.2) we have some freedom in each case to make a convenient choice of the element x without affecting the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$. If $a > 0$ then $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{a}, x = \sqrt{b}$, and if $b > 0$ then $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{b}, x = \sqrt{a}$. But if $a < 0$ and $b < 0$ then $ab > 0$ and $\mathfrak{O}_L$ is not free over $\mathfrak{A}_H$ in the Hopf-Galois structure corresponding to the choices $v = \sqrt{ab}, x = \sqrt{a}$. □

Chapter 8

Hopf-Galois Module Structure: Odd p

For an odd prime number p we have from (5.3.2) the following isomorphism of K-algebras:

$$H \cong K^p \times K(v)^{(p-1)},$$

and so the following description of the unique maximal $\mathfrak{O}_K$-order:

$$\mathfrak{M}_H \cong \mathfrak{O}_K^p \times \mathfrak{O}_{K(v)}^{(p-1)}.$$

We also have from (5.3.6) and (5.3.7) that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$, then an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{M}_{H,\mathfrak{p}}$ is given by

$$\begin{cases} \{E_r \mid 0 \leq r \leq p-1\} \cup \left\{ \left(\frac{e_s(a_v\eta)-e_s}{\pi_{\mathfrak{p}}^{e'}} \right)^t \mid 1 \leq s \leq p-1, 0 \leq t \leq p-1 \right\} & \text{if } \mathfrak{p} \mid p\mathfrak{O}_K \\ \{E_r \mid 0 \leq r \leq p-1\} \cup \left\{ \frac{e_s(a_v\eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{st})}} \mid 1 \leq s \leq p-1, 0 \leq t \leq p-1 \right\} & \text{otherwise.} \end{cases}$$

8.1 Sandwiching $\mathbf{Cl}\left(\mathfrak{A}_H\right)$

Proposition 8.1.1. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p. Let $z \in \mathfrak{M}_{H,\mathfrak{p}}$ and write

$$z = \sum_{r=0}^{p-1} a_r E_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} a_{s,t}\left(\frac{e_s(a_v\eta)-e_s}{\pi_{\mathfrak{p}}^{e'}}\right)^t e_s$$

with $a_r, a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$ for $r,t = 0,\ldots,p-1$ and $s = 1,\ldots,p-1$. Then $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$ if and only if

i) $\displaystyle\sum_{s=i}^{p-1}\sum_{t=j}^{p-1}\binom{s}{i}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p\pi_{\mathfrak{p}}^{-ie'}}$ for $1 \le i,j \le p-1$,

ii) $\displaystyle\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{s=1}^{p-1}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p^2}$ for $1 \le j \le p-1$,

iii) $\displaystyle\sum_{r=0}^{p-1}a_r + p\sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{-ks}(-1)^{t}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p^2}$ for $0 \le k \le p-1$,

iv) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^\times$.

Proof. We rewrite z in terms of the basis elements of $\mathfrak{O}_{L,\mathfrak{p}}[N]^G$ given in (6.2.1). By (6.2.4), we then have that $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$ if and only if the coefficients of these basis elements lie in $\mathfrak{O}_{K,\mathfrak{p}}$ and $\varepsilon(z) \in \mathfrak{O}_{K,\mathfrak{p}}^\times$. Using the binomial expansion, we have

$$\begin{aligned}
z &= \sum_{r=0}^{p-1}a_rE_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\sum_{j=0}^{t}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}e_s(a_v\eta)^j \\
&= \sum_{r=0}^{p-1}a_rE_r + \sum_{s=1}^{p-1}a_{s,0}e_s + \sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\sum_{j=0}^{t}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}e_s(a_v\eta)^j \\
&= \sum_{r=0}^{p-1}a_rE_r + \sum_{s=1}^{p-1}a_{s,0}e_s + \sum_{s=1}^{p-1}\sum_{t=1}^{p-1}(-1)^{t}\pi_{\mathfrak{p}}^{-te'}a_{s,t}e_s \\
&\qquad + \sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\sum_{j=1}^{t}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}e_s(a_v\eta)^j \\
&= \sum_{r=0}^{p-1}a_rE_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}(-1)^{t}\pi_{\mathfrak{p}}^{-te'}a_{s,t}e_s + \sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\sum_{j=1}^{t}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}e_s(a_v\eta)^j.
\end{aligned} \tag{8.1}$$

We consider the final term first, and use (6.2.2)

$$\begin{aligned}
&\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\sum_{j=1}^{t}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}e_s(a_v\eta)^j \\
&= \sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\sum_{j=1}^{t}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}\frac{1}{p}\sum_{i=0}^{s}\binom{s}{i}\pi_{\mathfrak{p}}^{ie'}\omega_{i,j} \\
&= \sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\pi_{\mathfrak{p}}^{-te'}a_{s,t}\sum_{j=1}^{t}\binom{t}{j}(-1)^{t-j}\frac{1}{p}\omega_{0,j} \\
&\quad + \sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\sum_{j=1}^{t}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}\frac{1}{p}\sum_{i=1}^{s}\binom{s}{i}\pi_{\mathfrak{p}}^{ie'}\omega_{i,j}
\end{aligned}$$

For $0 \leq i \leq p-1$ and $1 \leq j \leq p-1$, let $A_{i,j}$ denote the coefficient of $\omega_{i,j}$ in z. The from the above we see that for $1 \leq i, j \leq p-1$ we have

$$A_{i,j} = \frac{1}{p}\pi_{\mathfrak{p}}^{ie'}\sum_{s=i}^{p-1}\sum_{t=j}^{p-1}\binom{s}{i}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}.$$

We have that $A_{i,j} \in \mathfrak{O}_{K,\mathfrak{p}}$ if and only if the congruence condition in (i) holds.

Next we seek, for each $1 \leq j \leq p-1$, the coefficient of $\omega_{0,j}$ in z. We use again the formula given in (6.2.2).The final term of equation (8.1) contains a contribution:

$$\frac{1}{p}\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\pi_{\mathfrak{p}}^{-te'}a_{s,t}\sum_{j=1}^{t}\binom{t}{j}(-1)^{t-j}\omega_{0,j}.$$

The other terms involving $\omega_{0,j}$ are the idempotents E_r defined in (5.3.3). We calculate

$$\begin{aligned}
\sum_{r=0}^{p-1}a_rE_r &= \sum_{r=0}^{p-1}a_r\frac{1}{p}\sum_{j=0}^{p-1}\zeta^{jdr}e_0(a_v\eta)^j \\
&= \frac{1}{p}\sum_{r=0}^{p-1}a_re_0 + \frac{1}{p^2}\sum_{j=1}^{p-1}\sum_{r=0}^{p-1}\zeta^{jdr}a_r\omega_{0,j}
\end{aligned}$$

So the total coefficient of $\omega_{0,j}$ is

$$A_{0,j} = \frac{1}{p^2}\sum_{r=0}^{p-1}\zeta^{jdr}a_r + \frac{1}{p}\sum_{s=1}^{p-1}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}.$$

We have that $A_{0,j} \in \mathfrak{O}_{K,\mathfrak{p}}$ if and only if the congruence condition in (ii) holds.

Collecting the remaining terms together will allow us to examine the coefficients of the ρ^k for $0 \leq k \leq p-1$. We have

$$\begin{aligned}
&\frac{1}{p}\sum_{r=0}^{p-1}a_r e_0 + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t}e_s \\
&= \frac{1}{p}\sum_{r=0}^{p-1}a_r\frac{1}{p}\sum_{k=0}^{p-1}\rho^k + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t}\frac{1}{p}\sum_{k=0}^{p-1}\zeta^{-ks}\rho^k \\
&= \sum_{k=0}^{p-1}\left(\frac{1}{p^2}\sum_{r=0}^{p-1}a_r + \frac{1}{p}\sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{-ks}(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t}\right)\rho^k.
\end{aligned}$$

So for each $0 \leq k \leq p-1$, the coefficient of ρ^k is

$$\frac{1}{p^2}\sum_{r=0}^{p-1}a_r + \frac{1}{p}\sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{-ks}(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t},$$

and each of these lies in $\mathfrak{O}_{K,\mathfrak{p}}$ if and only if the corresponding congruence condition in (iii) holds.

Finally, we observe that

$$\varepsilon(z) = \sum_{r=0}^{p-1}a_r\varepsilon(E_r) + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\sum_{j=0}^{t}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}\varepsilon(e_s(a_v\eta)^j).$$

Now

$$\varepsilon(e_s(a_v\eta)^j) = \begin{cases} 1 & \text{if } s = 0 \\ 0 & \text{otherwise.} \end{cases}$$

and

$$\begin{aligned}\varepsilon(E_r) &= \frac{1}{p}\sum_{k=0}^{p-1}\zeta^{kdr}\varepsilon(e_0(a_v\eta)^k)\\ &= \begin{cases}1 & \text{if } r=0\\ 0 & \text{otherwise}\end{cases}\end{aligned}$$

So $\varepsilon(z)=a_0$ and, assuming $z\in\mathfrak{O}_{L,\mathfrak{p}}[N]^G$, we have $z\in\left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$ if and only if $a_0\in\mathfrak{O}_{K,\mathfrak{p}}^\times$. □

We now seek necessary and sufficient conditions for $z\in\left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^\times$. These will be in terms of higher unit groups of $\mathfrak{O}_{K,\mathfrak{p}}$ and $\mathfrak{O}_{K(v),\mathfrak{p}}$.

Definition 8.1.2. Define an isomorphism

$$\Theta : (K^\times)^p\times(K(v)^\times)^{(p-1)}\cong H^\times$$

by composing the automorphism of $(K^\times)^p\times(K(v)^\times)^{(p-1)}$ defined by

$$(z_0,z_1,\ldots,z_{p-1},y_1,\ldots y_{p-1})\mapsto(z_0,z_0z_1,\ldots,z_0z_{p-1},z_0y_1,\ldots,z_0y_{p-1})$$

with the isomorphism $K^p\times K(v)^{(p-1)}\cong H$ defined in (5.3.2). We shall also write Θ for the induced isomorphism $(K_\mathfrak{p}^\times)^p\times(K(v)_\mathfrak{p}^\times)^{(p-1)}\cong H_\mathfrak{p}^\times$, where $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, and the isomorphism $\mathbb{J}(K)^p\times\mathbb{J}(K(v))^{(p-1)}\cong\mathbb{J}(H)$.

Proposition 8.1.3. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p. Then

$$\Theta\left(\mathfrak{O}_{K,\mathfrak{p}}^\times\times(1+p^2\mathfrak{O}_{K,\mathfrak{p}})^{(p-1)}\times(1+p^2\mathfrak{O}_{K(v),\mathfrak{p}})^{(p-1)}\right)\subseteq\mathfrak{A}_{H,\mathfrak{p}}^\times.$$

Proof. The image under Θ of an element of

$$\mathfrak{O}_{K,\mathfrak{p}}^\times\times(1+p^2\mathfrak{O}_{K,\mathfrak{p}})^{(p-1)}\times(1+p^2\mathfrak{O}_{K(v),\mathfrak{p}})^{(p-1)}$$

has the form

$$z = \sum_{r=0}^{p-1} a_r E_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} a_{s,t}\left(\frac{e_s(a_v\eta) - e_s}{\pi_{\mathfrak{p}}^{e'}}\right)^t e_s$$

with $a_r, a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$ for $r, t = 0, \ldots, p-1$ and $s = 1, \ldots, p-1$, and

a) $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$.

b) $a_r \equiv a_0 \pmod{p^2}$ for $1 \leq r \leq p-1$.

c) $a_{s,0} \equiv a_0 \pmod{p^2}$ for $1 \leq s \leq p-1$.

d) $a_{s,t} \equiv 0 \pmod{p^2}$ for $1 \leq s, t \leq p-1$.

We show that z satisfies the conditions of (8.1.1).

i) By (d) we have $\pi_{\mathfrak{p}}^{-te'} a_{s,t} \equiv 0 \pmod{p}$ for $1 \leq s, t \leq p-1$. So

$$\sum_{s=i}^{p-1}\sum_{t=j}^{p-1}\binom{s}{i}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'} a_{s,t} \equiv 0 \pmod{p},$$

which is sufficient to ensure that condition (i) of (8.1.1) holds.

ii) By (b) and (d) we have, for $1 \leq j \leq p-1$, that

$$\begin{aligned}\sum_{r=0}^{p-1}\zeta^{jdr} a_r + p\sum_{s=1}^{p-1}\sum_{j=1}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'} a_{s,t} &\equiv \sum_{r=0}^{p-1}\zeta^{jdr} a_0 \pmod{p^2} \\ &\equiv a_0\sum_{r=0}^{p-1}\zeta^{jdr} \pmod{p^2} \\ &\equiv 0 \pmod{p^2}\end{aligned}$$

so condition (ii) of (8.1.1) holds.

iii) For $0 \leq k \leq p-1$ we have by (b),(c) and (d) that

$$\begin{aligned}\sum_{r=0}^{p-1} a_r + p\sum_{s=1}^{p-1}\sum_{t=0}^{p-1} \zeta^{-ks}(-1)^t \pi_{\mathfrak{p}}^{-te'} a_{s,t} &\equiv \sum_{r=0}^{p-1} a_0 + p\sum_{s=1}^{p-1} \zeta^{-ks} a_{s,0} \pmod{p^2} \\ &\equiv pa_0 + p\sum_{s=1}^{p-1} \zeta^{-ks} a_0 \pmod{p^2} \\ &\equiv pa_0 \sum_{s=0}^{p-1} \zeta^{-ks} \pmod{p^2} \\ &\equiv 0 \pmod{p^2}\end{aligned}$$

so condition (iii) of (8.1.1) holds.

iv) Condition (iv) of (8.1.1) holds by (a).

□

Proposition 8.1.4. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ lying above p. Then

$$\Theta^{-1}(\mathfrak{A}_{H,\mathfrak{p}}^{\times}) \subseteq \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times \left(1 + (\zeta - 1)\mathfrak{O}_{K,\mathfrak{p}}\right)^{(p-1)} \times \left(1 + (\zeta - 1)\mathfrak{O}_{K(v),\mathfrak{p}}\right)^{(p-1)}.$$

Proof. Let

$$z = \sum_{r=0}^{p-1} a_r E_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} a_{s,t} \left(\frac{e_s(a_v\eta) - e_s}{\pi_{\mathfrak{p}}^{e'}}\right)^t e_s \in \mathfrak{M}_{H,\mathfrak{p}}$$

with $a_r, a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$ for $r, t = 0, \ldots, p-1$ and $s = 1, \ldots, p-1$, and suppose that $z \in \left(\mathfrak{O}_{L,\mathfrak{p}}[N]^G\right)^{\times}$. Then the a_r and $a_{s,t}$ satisify the conditions of (8.1.1) and, in particular, $a_0 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. We shall show that this implies

$$\Theta^{-1}(z) \in \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times \left(1 + (\zeta - 1)\mathfrak{O}_{K,\mathfrak{p}}\right)^{(p-1)} \times \left(1 + (\zeta - 1)\mathfrak{O}_{K(v),\mathfrak{p}}\right)^{(p-1)}.$$

It is sufficient to prove that

i) $a_r \equiv a_0 \pmod{(\zeta - 1)}$ for $0 \leq r \leq p-1$.

ii) $a_{s,0} \equiv a_0 \pmod{(\zeta - 1)}$ for $1 \leq s \leq p-1$.

iii) $a_{s,t} \equiv 0 \pmod{(\zeta - 1)}$ for $1 \leq s, t \leq p-1$.

Recall from (8.1.1) that for $0 \leq i \leq p-1$ and $1 \leq j \leq p-1$ we denote by $A_{i,j}$ the coefficient of $\omega_{i,j}$ in z, and that for $1 \leq i, j \leq p-1$ we have

$$A_{i,j} = \frac{1}{p}\pi_{\mathfrak{p}}^{ie'} \sum_{s=i}^{p-1} \sum_{t=j}^{p-1} \binom{s}{i}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t}.$$

For $1 \leq i, t \leq p-1$ define

$$B_{i,t} = \sum_{s=i}^{p-1} \binom{s}{i} a_{s,t}.$$

Then for $1 \leq i, j \leq p-1$ we have

$$A_{i,j} = \frac{1}{p}\pi_{\mathfrak{p}}^{ie'} \sum_{t=j}^{p-1} \binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}B_{i,t}. \tag{8.2}$$

In particular, for $1 \leq i \leq p-1$ we have

$$A_{i,p-1} \sim \frac{1}{p^2}\pi_{\mathfrak{p}}^{ie'}B_{i,p-1},$$

and so

$$B_{i,p-1} \equiv 0 \pmod{p^2\pi_{\mathfrak{p}}^{-ie'}}.$$

Inducting backwards on j in (8.2), we find that for $1 \leq i, t \leq p-1$ we have

$$B_{i,t} \equiv 0 \pmod{p\pi_{\mathfrak{p}}^{(t-i)e'}},$$

and inducting backwards on i in the definition of $B_{i,t}$ we find that for $1 \leq s, t \leq p-1$ we have

$$a_{s,t} \equiv 0 \pmod{\pi_{\mathfrak{p}}^{te'}}.$$

This is sufficient to prove claim (iii) of the proposition.

Next recall the congruences in case (ii) of (8.1.1):

$$\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{s=1}^{p-1}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p^2} \text{ for } 1 \le j \le p-1$$

and the $k = 0$ case of the congruences in case (iii) of (8.1.1):

$$\sum_{r=0}^{p-1}a_r + p\sum_{s=1}^{p-1}\sum_{t=0}^{p-1}(-1)^{t}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \equiv 0 \pmod{p^2}$$

Summing these over j with appropriate coefficients yields, for each $0 \le l \le p-1$:

$$\begin{aligned}
&\sum_{j=0}^{p-1}\zeta^{-jdl}\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{j=0}^{p-1}\zeta^{-jdl}\sum_{s=1}^{p-1}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} &&\equiv 0 \pmod{p^2}\\
\Rightarrow\quad &\sum_{r=0}^{p-1}\left(\sum_{j=0}^{p-1}\zeta^{(r-l)jd}\right)a_r + p\sum_{s=1}^{p-1}\sum_{j=0}^{p-1}\zeta^{-jdl}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} &&\equiv 0 \pmod{p^2}\\
\Rightarrow\quad &pa_l + p\sum_{s=1}^{p-1}\sum_{j=0}^{p-1}\zeta^{-jdl}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} &&\equiv 0 \pmod{p^2}\\
\Rightarrow\quad &a_l + \sum_{s=1}^{p-1}\sum_{j=0}^{p-1}\zeta^{-jdl}\sum_{t=j}^{p-1}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} &&\equiv 0 \pmod{p}.
\end{aligned}$$

The coefficient of a given $\pi_{\mathfrak{p}}^{-te'}a_{s,t}$ in the second term is

$$\sum_{j=0}^{t}\binom{t}{j}\zeta^{-jdl}(-1)^{t-j} = (\zeta^{-dl}-1)^t,$$

so for $0 \le l \le p-1$ we have

$$a_l + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\left(\zeta^{-dl}-1\right)^t a_{s,t} \equiv 0 \pmod{p}.$$

This implies that

$$a_l \equiv -\sum_{s=1}^{p-1}a_{s,0} \pmod{\pi_{\mathfrak{p}}^{e'}},$$

and so $a_l \equiv a_0 \pmod{\pi_{\mathfrak{p}}^{e'}}$ for $1 \leq l \leq p-1$, as claimed in (i).

Finally, to show (ii), we recall from (8.1.1) part (i) that for $1 \leq i, j \leq p-1$ we have

$$A_{i,j} = \frac{1}{p}\pi_{\mathfrak{p}}^{ie'} \sum_{s=i}^{p-1}\sum_{t=j}^{p-1} \binom{s}{i}\binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$$

Therefore for $1 \leq i \leq p-1$ we have

$$\sum_{j=1}^{p-1} A_{i,j} = \frac{1}{p}\pi_{\mathfrak{p}}^{ie'} \sum_{s=i}^{p-1} \binom{s}{i} \sum_{j=1}^{p-1}\sum_{t=j}^{p-1} \binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}.$$

For each $1 \leq s, t \leq p-1$, we have $\pi_{\mathfrak{p}}^{-te'}a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$ by part (i) of this proposition. The coefficient of a given $\pi_{\mathfrak{p}}^{-te'}a_{s,t}$ in the above is

$$\begin{aligned} \frac{1}{p}\pi_{\mathfrak{p}}^{ie'} \sum_{j=1}^{t} \binom{t}{j}(-1)^{t-j} &= \frac{1}{p}\pi_{\mathfrak{p}}^{ie'} \sum_{j=0}^{t} \binom{t}{j}(-1)^{t-j} - (-1)^t \\ &= \frac{1}{p}\pi_{\mathfrak{p}}^{ie'}\left(0 + (-1)^{t-1}\right) \end{aligned}$$

so we have

$$\sum_{j=1}^{p-1} A_{i,j} = \frac{1}{p}\pi_{\mathfrak{p}}^{ie'} \sum_{s=i}^{p-1} \binom{s}{i} \sum_{t=1}^{p-1}(-1)^{t-1}\pi_{\mathfrak{p}}^{-te'}a_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}.$$

For $1 \leq s \leq p-1$ we define

$$\alpha_s = \sum_{t=1}^{p-1}(-1)^t \pi_{\mathfrak{p}}^{-te'}a_{s,t}.$$

Then we have

$$\frac{1}{p}\pi_{\mathfrak{p}}^{ie'} \sum_{s=i}^{p-1} \binom{s}{i}\alpha_s \in \mathfrak{O}_{K,\mathfrak{p}}.$$

Now fix some $1 \leq k \leq p-1$. Then $v_{\mathfrak{p}}\left(\zeta^{-k}-1\right) = e'$, so for $1 \leq i \leq p-1$ we have

$$\frac{1}{p}(\zeta^{-k}-1)^i \sum_{s=i}^{p-1} \binom{s}{i}\alpha_s \in \mathfrak{O}_{K,\mathfrak{p}},$$

and summing these over i we obtain

$$\sum_{i=1}^{p-1} \frac{1}{p} \sum_{s=i}^{p-1} \binom{s}{i} (\zeta^{-k} - 1)^i \alpha_s \in \mathfrak{O}_{K,\mathfrak{p}}.$$

The coefficient of a given α_s in this sum is

$$\begin{aligned} \frac{1}{p} \sum_{i=1}^{s} \binom{s}{i} (\zeta^{-k} - 1)^i &= \frac{1}{p} \left(\sum_{i=0}^{s} \binom{s}{i} (\zeta^{-k} - 1)^i - 1 \right) \\ &= \frac{1}{p} \left(((\zeta^{-k} - 1) + 1)^s - 1 \right) \\ &= \frac{1}{p} \left(\zeta^{-ks} - 1 \right). \end{aligned}$$

So for $1 \leq k \leq p-1$ we have

$$\frac{1}{p} \sum_{s=1}^{p-1} (\zeta^{-ks} - 1) \alpha_s \in \mathfrak{O}_{K,\mathfrak{p}}.$$

i.e.

$$\sum_{s=1}^{p-1} (\zeta^{-ks} - 1) \sum_{t=1}^{p-1} (-1)^t \pi_{\mathfrak{p}}^{-te'} a_{s,t} \equiv 0 \pmod{p}. \tag{8.3}$$

Next recall the congruences in part (ii) of (8.1.1):

$$\sum_{r=0}^{p-1} \zeta^{jdr} a_r + p \sum_{s=1}^{p-1} \sum_{t=j}^{p-1} \binom{t}{j} (-1)^{t-j} \pi_{\mathfrak{p}}^{-te'} a_{s,t} \equiv 0 \pmod{p^2} \text{ for } 1 \leq j \leq p-1.$$

Summing these over j, we obtain:

$$\sum_{j=1}^{p-1} \sum_{r=0}^{p-1} \zeta^{jdr} a_r + p \sum_{s=1}^{p-1} \sum_{j=1}^{p-1} \sum_{t=j}^{p-1} \binom{t}{j} (-1)^{t-j} \pi_{\mathfrak{p}}^{-te'} a_{s,t} \equiv 0 \pmod{p^2}.$$

The coefficient of a given $\pi_{\mathfrak{p}}^{-te'}a_{s,t}$ in this sum is

$$\begin{aligned} p\sum_{j=1}^{t}\binom{t}{j}(-1)^{t-j} &= p\left(\sum_{j=0}^{t}\binom{t}{j}(-1)^{t-j}-(-1)^t\right) \\ &= p\left(0-(-1)^t\right) \end{aligned}$$

So we have

$$\sum_{j=1}^{p-1}\sum_{r=0}^{p-1}\zeta^{jdr}a_r - p\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t}\equiv 0 \pmod{p^2}. \tag{8.4}$$

Now recall from (8.1.1)(iii) that for $0\leq k\leq p-1$ we have

$$\sum_{r=0}^{p-1}a_r + p\sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{-ks}(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t}\equiv 0 \pmod{p^2}. \tag{8.5}$$

Adding (8.4) to (8.5) yields:

$$\sum_{j=0}^{p-1}\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{s=1}^{p-1}\zeta^{-ks}a_{s,0} + p\sum_{s=1}^{p-1}\sum_{t=1}^{p-1}\left(\zeta^{-ks}-1\right)(-1)^t\pi_{\mathfrak{p}}^{-te'}a_{s,t}\equiv 0 \pmod{p^2}.$$

Using congruence (8.3) we then have

$$\begin{aligned} &\sum_{j=0}^{p-1}\sum_{r=0}^{p-1}\zeta^{jdr}a_r + p\sum_{s=1}^{p-1}\zeta^{-ks}a_{s,0}\equiv 0 \pmod{p^2} \\ &\quad\Rightarrow\quad pa_0 + p\sum_{s=1}^{p-1}\zeta^{-ks}a_{s,0}\equiv 0 \pmod{p^2} \\ &\quad\Rightarrow\quad a_0 + \sum_{s=1}^{p-1}\zeta^{-ks}a_{s,0}\equiv 0 \pmod{p} \end{aligned}$$

Now write $a_{0,0}=a_0$. Then for $0\leq k\leq p-1$ we have

$$\sum_{s=0}^{p-1}\zeta^{-ks}a_{s,0}\equiv 0 \pmod{p},$$

so for some $C_k \in \mathfrak{O}_{K,\mathfrak{p}}$ we have

$$\sum_{s=0}^{p-1} \zeta^{-ks} a_{s,0} = pC_k.$$

Then we have

$$a_{s,0} = \sum_{k=0}^{p-1} \zeta^{ks} C_k,$$

and for $s \neq s'$ we have

$$a_{s,0} - a_{s',0} = \sum_{k=0}^{p-1} \left(\zeta^{ks} - \zeta^{ks'}\right) C_k \equiv 0 \pmod{(\zeta - 1)}$$

So for each $1 \leq s \leq p-1$, we have $a_{s,0} \equiv a_0 \pmod{(\zeta - 1)}$, as claimed in (i). This completes the proof. □

Proposition 8.1.5. There are injections:

$$\begin{array}{c} \mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathbb{U}_{p^2}(\mathfrak{O}_{K(v)})^{(p-1)} \\ \downarrow \\ \mathbb{U}(\mathfrak{A}_H) \\ \downarrow \\ \mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_{(\zeta-1)}(\mathfrak{O}_K)^{(p-1)} \times \mathbb{U}_{(\zeta-1)}(\mathfrak{O}_{K(v)})^{(p-1)} \end{array}$$

and therefore surjections:

$$\begin{array}{c} \mathrm{Cl}\,(\mathfrak{O}_K) \times \mathrm{Cl}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{p^2}(\mathfrak{O}_{K(v)})^{(p-1)} \\ \downarrow \\ \mathrm{Cl}\,(\mathfrak{A}_H) \\ \downarrow \\ \mathrm{Cl}\,(\mathfrak{O}_K) \times \mathrm{Cl}_{(\zeta-1)}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{(\zeta-1)}(\mathfrak{O}_{K(v)})^{(p-1)}. \end{array}$$

Proof. Recall from (2.1.21) that

$$\mathbb{U}(\mathfrak{A}_H) = \prod_{\mathfrak{p} \lhd \mathfrak{O}_K} \mathfrak{A}_{H,\mathfrak{p}}^{\times} = \left\{ (a_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbb{J}(H) \mid a_{\mathfrak{p}} \in \mathfrak{A}_{H,\mathfrak{p}}^{\times} \text{ for all } \mathfrak{p} \right\}.$$

By (6.1.1) and (5.3.4) we have that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which does not lie above p then

$$\mathfrak{A}_{H,\mathfrak{p}}^{\times} = \mathfrak{M}_{H,\mathfrak{p}}^{\times} \cong \left(\mathfrak{O}_{K,\mathfrak{p}}^{\times}\right)^p \times \left(\mathfrak{O}_{K(w),\mathfrak{p}}^{\times}\right)^{p-1}.$$

From (8.1.4) and (8.1.3) we have that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ which lies above p then there are injections:

$$\begin{array}{c} \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times \left(1 + p^2 \mathfrak{O}_{K,\mathfrak{p}}\right)^{(p-1)} \times \left(1 + p^2 \mathfrak{O}_{K(v),\mathfrak{p}}\right)^{(p-1)} \\ \downarrow \\ \mathfrak{A}_{H,\mathfrak{p}}^{\times} \\ \downarrow \\ \mathfrak{O}_{K,\mathfrak{p}}^{\times} \times \left(1 + (\zeta - 1)\mathfrak{O}_{K,\mathfrak{p}}\right)^{(p-1)} \times \left(1 + (\zeta - 1)\mathfrak{O}_{K(w),\mathfrak{p}}\right)^{(p-1)} \end{array}$$

Recalling definition (2.1.20), this implies that there are injections

$$\begin{array}{c} \mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathbb{U}_{p^2}(\mathfrak{O}_{K(w)})^{(p-1)} \\ \downarrow \\ \mathbb{U}(\mathfrak{A}_H) \\ \downarrow \\ \mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_{(\zeta-1)}(\mathfrak{O}_K)^{(p-1)} \times \mathbb{U}_{(\zeta-1)}(\mathfrak{O}_{K(w)})^{(p-1)}. \end{array}$$

The existence of the surjections asserted by the proposition then follows from the isomorphism (see (2.1.25))

$$\mathrm{Cl}\left(\mathfrak{A}_H\right) \cong \frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathfrak{A}_H)}.$$

□

8.2 The Class Representing $\mathfrak{O}_L$

Proposition 8.2.1. The class of $\mathfrak{O}_L$ in the locally free class group

$$\mathrm{Cl}\,(\mathfrak{A}) \cong \frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathfrak{A}_H)},$$

corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$, where

$$h_{\mathfrak{p}} = \begin{cases} \displaystyle\sum_{r=0}^{p-1} E_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} \zeta^{std(t-1)/2} \upsilon^{-pq_{s,t}} e_s (a_v \eta)^t & \mathfrak{p} | p\mathfrak{O}_K \\ \displaystyle\sum_{r=0}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^r)} E_r + \sum_{s=1}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} e_s (a_v \eta)^{j_{\mathfrak{p}}} & \mathfrak{p} | XV\mathfrak{O}_K \\ 1 & \text{otherwise.} \end{cases}$$

Here $q_{s,t} = \left\lfloor \frac{st}{p} \right\rfloor$ and (see (6.1.2)) $0 \leq j_{\mathfrak{p}} \leq p-1$ is defined as follows:

$$\begin{cases} j_{\mathfrak{p}} = 0 & \text{if } v_{\mathfrak{p}}(X) \equiv 0 \pmod{p} \text{ or } v_{\mathfrak{p}}(V) \equiv 0 \pmod{p} \\ v_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}}) \equiv 0 \pmod{p} & \text{otherwise.} \end{cases}$$

Proof. Define

$$\Gamma = \frac{1}{p^2} \left(\sum_{j=0}^{p-1} v^j + \sum_{s=1}^{p-1} x^s \right) \in L^{\times}$$

Using the formulae for the action of the K-basis elements of H on those of L in (5.4.3) and (5.4.4), we see that Γ is a generator of L over H. By (2.1.25), to show that the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$ corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ in $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$ we must show that for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$, the element $h_{\mathfrak{p}}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. We recall the local generators $\gamma_{\mathfrak{p}}$ given in (6.1.2) and

(6.1.7):

$$\gamma_{\mathfrak{p}} = \begin{cases} \dfrac{1}{p^2}\displaystyle\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} x^i v^j & \text{if } \mathfrak{p} \mid p\mathfrak{O}_K \\ \displaystyle\sum_{j=0}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^j)} v^j + \sum_{s=1}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} x^s v^{sj_{\mathfrak{p}}} & \text{otherwise} \end{cases}$$

Suppose first that $\mathfrak{p} \nmid pXV\mathfrak{O}_K$. Then $j_{\mathfrak{p}} = 0$ and so

$$h_{\mathfrak{p}}\Gamma = \frac{1}{p^2}\left(\sum_{j=0}^{p-1} v^j + \sum_{s=1}^{p-1} x^s\right)$$

whereas

$$\gamma_{\mathfrak{p}} = \sum_{j=0}^{p-1} v^j + \sum_{s=1}^{p-1} x^s.$$

We note that $\mathfrak{p} \nmid p\mathfrak{O}_K$ and so $p^2 \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. Therefore $h_{\mathfrak{p}}\Gamma$ and $\gamma_{\mathfrak{p}}$ differ only by an element of $\mathfrak{O}_{K,\mathfrak{p}}^{\times}$, and so $h_{\mathfrak{p}}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$. Next suppose that $\mathfrak{p} \mid XV\mathfrak{O}_K$. Then

$$\begin{aligned} h_{\mathfrak{p}}\Gamma &= \sum_{r=0}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^r)} E_r\Gamma + \sum_{s=1}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} e_s (a_v\eta)^{j_{\mathfrak{p}}}\Gamma \\ &= \frac{1}{p^2}\sum_{r=0}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^r)} v^r + \frac{1}{p^2}\sum_{s=1}^{p-1} \zeta^{sj_{\mathfrak{p}}d(j_{\mathfrak{p}}-1)/2} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} x^s v^{sj_{\mathfrak{p}}} \end{aligned}$$

whereas

$$\gamma_{\mathfrak{p}} = \sum_{j=0}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^j)} v^j + \sum_{s=1}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} x^s v^{sj_{\mathfrak{p}}}.$$

Comparing these two, we see that

$$p^2\left(\sum_{r=0}^{p-1} E_r + \sum_{s=1}^{p-1} \zeta^{-sj_{\mathfrak{p}}d(j_{\mathfrak{p}}-1)/2} e_s\right)(h_{\mathfrak{p}}\Gamma) = \gamma_{\mathfrak{p}}.$$

Since the first factor lies in $\mathfrak{A}_{H,\mathfrak{p}}^{\times}$, we have that $h_{\mathfrak{p}}\Gamma$ is a generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$.

Finally suppose that $\mathfrak{p} \mid p\mathfrak{O}_K$. Let $^-$ denote reduction to least positive residue mod p. Then

$$\begin{aligned} h_{\mathfrak{p}}\Gamma &= \sum_{r=0}^{p-1} E_r\Gamma + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} \zeta^{std(t-1)/2} v^{-pq_{s,t}} e_s(a_v\eta)^t\Gamma \\ &= \frac{1}{p^2}\left(\sum_{r=0}^{p-1} v^r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} \zeta^{std(t-1)/2} v^{-pq_{s,t}} e_s(a_v\eta)^t x^s\right) \\ &= \frac{1}{p^2}\left(\sum_{r=0}^{p-1} v^r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} \zeta^{std(t-1)/2} v^{-pq_{s,t}} \zeta^{-std(t-1)/2} v^{st} x^s\right) \\ &= \frac{1}{p^2}\left(\sum_{r=0}^{p-1} v^r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} v^{\overline{st}} x^s\right) \\ &= \gamma_{\mathfrak{p}} \end{aligned}$$

So in this case $h_{\mathfrak{p}}\Gamma$ coincides with the generator of $\mathfrak{O}_{L,\mathfrak{p}}$ over $\mathfrak{A}_{H,\mathfrak{p}}$ given in (6.1.7). This completes the proof. □

Remark 8.2.2. By (5.2.1), a nonclassical Hopf-Galois structure on L/K is determined by a choice of subgroup T of $G = \mathrm{Gal}(L/K)$ of order p and a choice of $d \in \{1, \ldots, p-1\}$. These choices also determine the field $K(v)$ appearing in the isomorphism of K-algebras $H \cong K^p \times K(v)^{p-1}$. We chose in (5.2.1) an element $\tau \in G$ such that $T = \langle\tau\rangle$ and an element $\sigma \in G$ such that $G = \langle\sigma, \tau\rangle$. Making a different choice of these elements τ, σ will result in a different description of the field L and Hopf algebra H, but it will not affect the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_H)$ because this does not depend on the descriptions of the objects involved. If we denote by τ' a different choice of generator for the subgroup T and by σ' a different choice of group element satisfying $\langle\sigma', \tau'\rangle = G$ then we have three possibilities. Throughout, let $^-$ denote reduction to least positive residue modulo p.

i) If $\tau' = \tau^m$ for some $1 \leq m \leq p-1$ then let $0 \leq n \leq p-1$ satisfy $mn \equiv 1$

(mod p). We have the following change of K-basis of L:

$$\begin{aligned} v &\mapsto v \\ x &\mapsto x' = x^n \end{aligned}$$

and the following change of K-basis of H:

$$\begin{aligned} E_r &\mapsto E_r && \text{for } r = 0, \ldots, p-1 \\ e_s(a_v\eta)^t &\mapsto e_{\overline{ns}}(a_v\eta)^t && \text{for } s = 1, \ldots, p-1 \text{ and } t = 0, \ldots, p-1. \end{aligned}$$

ii) If $\sigma' = \sigma^m$ for some $1 \leq m \leq p-1$ then let $0 \leq n \leq p-1$ satisfy $mn \equiv 1$ (mod p). We have the following change of K-basis of L:

$$\begin{aligned} v &\mapsto v' = v^n \\ x &\mapsto x \end{aligned}$$

and the following change of K-basis of H:

$$\begin{aligned} E_r &\mapsto E_{\overline{nr}} && \text{for } r = 0, \ldots, p-1 \\ e_s(a_v\eta)^t &\mapsto e_s(a_v\eta)^{\overline{nt}} && \text{for } s = 1, \ldots, p-1 \text{ and } t = 0, \ldots, p-1. \end{aligned}$$

iii) If $\sigma' = \sigma\tau^m$ for some $1 \leq m \leq p-1$ then let $0 \leq n \leq p-1$ satisfy $m - dn \equiv 1$ (mod p). We have the following change of K-basis of L:

$$\begin{aligned} v &\mapsto v \\ x &\mapsto x' = xv^n \end{aligned}$$

and the following change of K-basis of H:

$$\begin{aligned} E_r &\mapsto E_r && \text{for } r = 0, \dots, p-1 \\ e_s(a_v\eta)^t &\mapsto \zeta^{-dnst} e_s(a_v\eta)^t && \text{for } s = 1, \dots, p-1 \text{ and } t = 0, \dots, p-1. \end{aligned}$$

Definition 8.2.3. For each $s = 1, \dots, p-1$ define $U_s \in K(v)^\times$ by

$$U_s = \sum_{t=0}^{p-1} \zeta^{std(t-1)/2} V^{-q_{s,t}} v^{st} \in K(v)^\times.$$

Proposition 8.2.4. Under the composition of maps

$$\mathbb{J}(H) \to \mathbb{J}(K)^p \times \mathbb{J}(K(v))^{(p-1)} \to \mathrm{Cl}\left(\mathfrak{O}_K\right)^p \times \mathrm{Cl}\left(\mathfrak{O}_{K(v)}\right)^{(p-1)},$$

the idèle $(h_\mathfrak{p})_\mathfrak{p}$ defined in (8.2.1) corresponds to the class of the tuple of fractional ideals

$$\left(\mathfrak{O}_K, I_V^{-1}, \dots, I_{V^{(p-1)}}^{-1}, J_1, \dots, J_{(p-1)}\right),$$

where for $s = 1, \dots, (p-1)$ the fractional ideal J_s is defined by

$$J_s = \left(I_{X^s}^{-1} \prod_{\mathfrak{P} \mid p\mathfrak{O}_{K(v)}} \mathfrak{P}^{-v_\mathfrak{P}(U_s)} \prod_{\mathfrak{P} \mid V\mathfrak{O}_{K(v)}} \mathfrak{P}^{v_\mathfrak{P}\left(V^{sj_\mathfrak{p}}\right) - pr_\mathfrak{p}(V^{sj_\mathfrak{p}}) - p} \right)$$

Proof. Under the isomorphism

$$\mathbb{J}(H) \to \mathbb{J}(K)^p \times \mathbb{J}(K(v))^{(p-1)}$$

the idèle $(h_\mathfrak{p})_\mathfrak{p}$ is mapped to the tuple of idèles

$$\left((1)_\mathfrak{p}, \left(\pi_\mathfrak{p}^{-r_\mathfrak{p}(V)}\right)_\mathfrak{p}, \dots, \left(\pi_\mathfrak{p}^{-r_\mathfrak{p}(V^{(p-1)})}\right)_\mathfrak{p}, (y_{1,\mathfrak{P}})_\mathfrak{P}, \dots, (y_{(p-1),\mathfrak{P}})_\mathfrak{P}\right)$$

where for $s = 1, \ldots, p-1$, the element $y_{s,\mathfrak{P}} \in K(v)_{\mathfrak{P}}$ is defined by

$$y_{s,\mathfrak{P}} = \begin{cases} \sum_{t=0}^{p-1} \zeta^{std(t-1)/2} v^{-pq_{s,t}} v^{st} & \mathfrak{P} \mid p\mathfrak{O}_{K(v)} \\ \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} v^{sj_{\mathfrak{p}}} & \mathfrak{P} \mid XV\mathfrak{O}_{K(v)} \\ 1 & \text{otherwise} \end{cases}$$

Now for each $s = 1, \ldots, p-1$ we define an idèle $(y'_{s,\mathfrak{P}})_{\mathfrak{P}} \in \mathbb{J}(K(v))$ by

$$y'_{s,\mathfrak{P}} = U_s^{-1} y_{s,\mathfrak{P}} = \begin{cases} 1 & \mathfrak{P} \mid p\mathfrak{O}_{K(v)} \\ U_s^{-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s V^{sj_{\mathfrak{p}}})} v^{sj_{\mathfrak{p}}} & \text{otherwise} \end{cases}$$

Then the tuple of idèles

$$\left((1)_{\mathfrak{p}}, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)}\right)_{\mathfrak{p}}, \ldots, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^{(p-1)})}\right)_{\mathfrak{p}}, (y_{1,\mathfrak{P}})_{\mathfrak{P}}, \ldots, (y_{(p-1),\mathfrak{P}})_{\mathfrak{P}} \right)$$

has the same class in the product $\mathrm{Cl}\,(\mathfrak{O}_K)^p \times \mathrm{Cl}\left(\mathfrak{O}_{K(v)}\right)^{(p-1)}$ as the tuple of idèles

$$\left((1)_{\mathfrak{p}}, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)}\right)_{\mathfrak{p}}, \ldots, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^{(p-1)})}\right)_{\mathfrak{p}}, (y'_{1,\mathfrak{P}})_{\mathfrak{P}}, \ldots, (y'_{(p-1),\mathfrak{P}})_{\mathfrak{P}} \right).$$

We use the homomorphism defined in (2.1.19), applied to each component, to map this tuple of idèles to a tuple of fractional ideals. We see immediately that the first component is mapped to the trivial ideal, and that for $r = 2, \ldots, p$, the r^{th} component is mapped to the fractional ideal

$$I_{V^{r-1}}^{-1} = \prod_{\mathfrak{p} \mid V} \mathfrak{p}^{-r_{\mathfrak{p}}(V^{r-1})}.$$

To determine the images of the remaining components we calculate, for each $s \neq 0$

and $\mathfrak{P}$ a prime of $\mathfrak{O}_{K(v)}$, the valuation $v_{\mathfrak{P}}\left(y'_{s,\mathfrak{P}}\right)$. We have:

$$v_{\mathfrak{P}}\left(y'_{s,\mathfrak{P}}\right) = \begin{cases} 0 & \mathfrak{P} \mid p\mathfrak{O}_{K(v)} \\ -v_{\mathfrak{P}}\left(U_s\right) - v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}})}v^{sj_{\mathfrak{p}}}\right) & \text{otherwise.} \end{cases}$$

We now make the following observations regarding $j_{\mathfrak{p}}$:

i) By (6.1.3) we have $j_{\mathfrak{p}} \neq 0$ only if the prime $\mathfrak{p}$ of $\mathfrak{O}_K$ is ramified in the extension $K(v)/K$.

ii) If $j_{\mathfrak{p}} \neq 0$ then by the definition of $j_{\mathfrak{p}}$ in (6.1.2) we have

$$r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}}) = r_{\mathfrak{p}}(X^s) + r_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}}) + 1.$$

iii) If $j_{\mathfrak{p}} \neq 0$ then since $\mathfrak{p}$ is ramified in $K(v)/K$ we have

$$pv_{\mathfrak{p}}\left(V\right) = v_{\mathfrak{P}}\left(V\right) = v_{\mathfrak{P}}\left(v^p\right) = pv_{\mathfrak{P}}\left(v\right),$$

and so $v_{\mathfrak{P}}\left(v\right) = v_{\mathfrak{p}}\left(V\right)$.

Using these observations we see that if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ such that $j_{\mathfrak{p}} \neq 0$ and $\mathfrak{P}$ is a prime of $\mathfrak{O}_{K(v)}$ lying above $\mathfrak{p}$ then we have

$$\begin{aligned} v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}})}v^{sj_{\mathfrak{p}}}\right) &= -v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s)}\right) - v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}})+1}\right) + v_{\mathfrak{P}}\left(v^{sj_{\mathfrak{p}}}\right) \\ &= -v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(X^s)}\right) - pr_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}}) - p + v_{\mathfrak{p}}\left(V^{sj_{\mathfrak{p}}}\right). \end{aligned}$$

On the other hand, if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ such that $j_{\mathfrak{p}} = 0$ and $\mathfrak{P}$ is a prime of $\mathfrak{O}_{K(v)}$ lying above $\mathfrak{p}$ then we have

$$v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}})}v^{sj_{\mathfrak{p}}}\right) = v_{\mathfrak{P}}\left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^s)}\right)$$

So we see that the idèle $(y'_{s,\mathfrak{P}})_{\mathfrak{P}}$ corresponds to the fractional ideal

$$J_s = \left(I_{X^s}^{-1} \prod_{\mathfrak{P} \nmid p\mathfrak{O}_{K(v)}} \mathfrak{P}^{-v_{\mathfrak{P}}(U_s)} \prod_{\mathfrak{P} \mid V\mathfrak{O}_{K(v)}} \mathfrak{P}^{v_{\mathfrak{P}}\left(V^{sj_{\mathfrak{p}}}\right) - pr_{\mathfrak{p}}(V^{sj_{\mathfrak{p}}}) - p} \right),$$

and so the tuple of idèles

$$\left((1)_{\mathfrak{p}}, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V)}\right)_{\mathfrak{p}}, \ldots, \left(\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^{(p-1)})}\right)_{\mathfrak{p}}, (y'_{1,\mathfrak{P}})_{\mathfrak{P}}, \ldots, (y'_{(p-1),\mathfrak{P}})_{\mathfrak{P}} \right)$$

corresponds to the tuple of fractional ideals

$$\left(\mathfrak{O}_K, I_V^{-1}, \ldots, I_{V^{(p-1)}}^{-1}, J_1, \ldots, J_{(p-1)}\right).$$

□

8.3 Conditions for Global Freeness

Proposition 8.3.1. A sufficient condition for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$ is that the tuple of ideals given in (8.2.4) has trival class in the product of ray class groups

$$\mathrm{Cl}\left(\mathfrak{O}_K\right) \times \mathrm{Cl}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{p^2}(\mathfrak{O}_{K(v)})^{(p-1)}.$$

A necessary condition is that the same triple has trivial class in the product of ray class groups

$$\mathrm{Cl}\left(\mathfrak{O}_K\right) \times \mathrm{Cl}_{(\zeta-1)}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{(\zeta-1)}(\mathfrak{O}_{K(v)})^{(p-1)}.$$

Proof. By (8.2.1), the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\left(\mathfrak{A}_H\right)$ corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ in $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$. Recalling the surjections of (8.1.5), the result follows. □

8.4 Comparing Structures

By (5.2.1), a Hopf algebra giving a nonclassical Hopf-Galois structure on L/K is determined by a choice of subgroup T of $\mathrm{Gal}(L/K)$ of order p and a choice of the integer $d \in \{1, \ldots, p-1\}$. In this section we prove a partial result relating the structure of $\mathfrak{O}_L$ over the associated order in the Hopf algebra $H = H_{T,d}$ and its structure over the associated order in the Hopf algebra $H' = H_{T,d'}$. Throughout, let $^-$ denote reduction to least positive residue modulo p.

Let $d, d' \in \{1, \ldots, p-1\}$ and suppose that $d \neq d'$. Let $c \in \{1, \ldots, p-1\}$ satisfy $cd \equiv d' \pmod{p}$. In section (5.3) we associated with H elements $v \in \mathfrak{O}_L^T, x \in \mathfrak{O}_L^S$ satisfying $\sigma(v) = \zeta^{-d}v, \tau(x) = \zeta x$. Let v', x' denote the analogous elements associated with H'. We have

$$\begin{aligned} \sigma(v^c) &= \zeta^{-cd}v^c \\ &= \zeta^{-d'}v^c \end{aligned}$$

and so we may take $v' = v^c$. We shall also take $x' = x^c$; by (8.2.2) this choice does not affect the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\,(\mathfrak{A}_{H'})$. We fix the following K-basis for H, as in (5.3.2)

$$\{E_r \mid 0 \leq r \leq p-1\} \cup \left\{e_s(a_v\eta)^t \mid 1 \leq s \leq p-1, 0 \leq t \leq p-1\right\}$$

and the following analogous K-basis for H':

$$\{E'_r \mid 0 \leq r \leq p-1\} \cup \left\{e'_s(a_{v'}\eta')^t \mid 1 \leq s \leq p-1, 0 \leq t \leq p-1\right\}.$$

Proposition 8.4.1. Define a K-linear map $\Phi : H' \to H$ by

$$\begin{aligned} \Phi(E'_r) &= E_{\overline{cr}} \quad \text{for } r = 0, \ldots, p-1 \\ \Phi(e'_s(a_{v'}\eta')^t) &= V^{\lfloor \frac{cs}{p} \rfloor t} e_{\overline{cs}}(a_v\eta)^t \quad \text{for } s = 1, \ldots, p-1 \text{ and } t = 0, \ldots, p-1. \end{aligned}$$

Then Φ is an isomorphism of K-algebras.

Proof. For $r = 0, \ldots, p-1$ the elements E_r and E'_r are idempotents, and so we have:

$$\Phi((E'_r)^2) = \Phi(E'_r) = E_{\overline{cr}} = E^2_{\overline{cr}} = \Phi(E'_r)^2.$$

For $s = 1, \ldots, p-1$ we have on the one hand:

$$\begin{aligned} \Phi(e'_s(a_{v'}\eta')^p) &= \Phi((v')^{sp}e'_s) \\ &= V^{cs}\Phi(e'_s) \\ &= V^{cs}e_{\overline{cs}} \end{aligned}$$

and on the other:

$$\begin{aligned} \Phi(e'_s(a_{v'}\eta'))^p &= V^{\lfloor \frac{cs}{p} \rfloor p} e_{\overline{cs}}(a_v\eta)^p \\ &= V^{\lfloor \frac{cs}{p} \rfloor p} V^{\overline{cs}} e_{\overline{cs}} \\ &= V^{cs} e_{\overline{cs}} \end{aligned}$$

the final equality holding since $cs = p\left\lfloor \frac{cs}{p} \right\rfloor + \overline{cs}$. Since these two calculations agree, the result follows. □

Remark 8.4.2. As with the isomorphism Θ defined in (8.1.2), we shall also write Φ for the induced isomorphism $H'_{\mathfrak{p}} \cong H_{\mathfrak{p}}$, where $\mathfrak{p}$ a prime of $\mathfrak{O}_K$, and the isomorphism $\mathbb{J}(H') \cong \mathbb{J}(H)$.

Definition 8.4.3. Recall from (8.1.2) the isomorphism

$$\Theta : \mathbb{J}(K)^p \times \mathbb{J}(K(v))^{(p-1)} \cong \mathbb{J}(H).$$

Let Θ' denote the corresponding isomorphism

$$\Theta' : \mathbb{J}(K)^p \times \mathbb{J}(K(v))^{(p-1)} \cong \mathbb{J}(H').$$

Define a subgroup $\mathfrak{B}'$ of $\mathbb{J}(H')$ as follows:

$$\mathfrak{B}' \;=\; \Theta'\left(\mathbb{U}(\mathfrak{O}_K) \times \mathbb{U}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathbb{U}_{p^2}(\mathfrak{O}_{K(v)})^{(p-1)}\right) \leq \mathbb{J}(H')$$

Proposition 8.4.4. Suppose that $V \equiv 1 \pmod{p^2(\zeta - 1)}$. Then under the isomorphism $\Phi : \mathbb{J}(H') \cong \mathbb{J}(H)$ we have

$$\Phi\left((H')^\times\right) = H^\times$$

and

$$\Phi\left(\mathfrak{B}'\right) \subseteq \mathbb{U}(\mathfrak{A}_H).$$

Proof. Since the isomorphism $\Phi : \mathbb{J}(H') \cong \mathbb{J}(H)$ is induced from an isomorphism $H' \cong H$ we have that

$$\Phi\left((h)_{\mathfrak{p}}\right) = \left(\Phi(h)\right)_{\mathfrak{p}} \text{ for } h \in H',$$

which establishes the first part of the proposition. For the second part, let $(z'_{\mathfrak{p}})_{\mathfrak{p}} \in \mathfrak{B}'$. Then

a) $z'_{\mathfrak{p}} \in (\mathfrak{M}'_{H,\mathfrak{p}})^\times$ for all $\mathfrak{p} \nmid p\mathfrak{O}_K$.

b) $z'_{\mathfrak{p}} \in \Theta'\left(\mathfrak{O}_{K,\mathfrak{p}}^\times \times (1 + p^2\mathfrak{O}_{K,\mathfrak{p}})^{(p-1)} \times (1 + p^2\mathfrak{O}_{K(v),\mathfrak{p}})^{(p-1)}\right)$ for all $\mathfrak{p} \mid p\mathfrak{O}_K$.

By (5.3.6) and (8.1.3), sufficient conditions for an idèle $(z_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbb{J}(H)$ to lie in $\mathbb{U}(\mathfrak{A}_H)$ are

i) $z_{\mathfrak{p}} \in (\mathfrak{M}_{H,\mathfrak{p}}^{\times})$ for all $\mathfrak{p} \nmid p\mathfrak{O}_K$.

ii) $z_{\mathfrak{p}} \in \Theta\left(\mathfrak{O}_{K,\mathfrak{p}}^{\times} \times (1+p^2\mathfrak{O}_{K,\mathfrak{p}})^{(p-1)} \times (1+p^2\mathfrak{O}_{K(v),\mathfrak{p}})^{(p-1)}\right)$ for all $\mathfrak{p} \mid p\mathfrak{O}_K$.

Suppose first that $\mathfrak{p} \nmid p\mathfrak{O}_K$. Then by (5.3.6) we may write

$$z'_{\mathfrak{p}} = \sum_{r=0}^{p-1} a'_r E'_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} a'_{s,t} \frac{e'_s (a_{v'}\eta')^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{cst})}},$$

with $a'_r \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}, a'_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$ and $e'_s z_{\mathfrak{p}} \in \left(e'_s \mathfrak{M}'_{H,\mathfrak{p}}\right)^{\times} \cong \mathfrak{O}_{K(v),\mathfrak{p}}^{\times}$. We calculate:

$$\Phi(z'_{\mathfrak{p}}) = \sum_{r=0}^{p-1} a'_r E_{\overline{cr}} + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} a'_{s,t} V^{\lfloor \frac{cs}{p} \rfloor t} \frac{e_{\overline{cs}} (a_v \eta)^t}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(V^{cst})}}.$$

This implies that $\Phi(z_{\mathfrak{p}}) \in \mathfrak{M}_{H,\mathfrak{p}}^{\times}$ since for each $s = 1, \ldots, p-1$ the following diagram commutes:

$$\begin{array}{ccc} e'_s H'_{\mathfrak{p}} & \xrightarrow{\quad\Phi\quad} & e_{\overline{cs}} H_{\mathfrak{p}} \\ \downarrow & & \downarrow \\ K(v)_{\mathfrak{p}} & = & K(v)_{\mathfrak{p}}. \end{array}$$

Now suppose that $\mathfrak{p} \mid p\mathfrak{O}_K$. Then by (5.3.7) we may write

$$z'_{\mathfrak{p}} = \sum_{r=0}^{p-1} a'_r E'_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} a'_{s,t} \left(\frac{e'_s (a_{v'}\eta') - e'_s}{\pi_{\mathfrak{p}}^{e'}}\right)^t e'_s,$$

with $a'_r, a'_{s,t} \in \mathfrak{O}_{K,\mathfrak{p}}$. Using the binomial expansion we have

$$z'_{\mathfrak{p}} = \sum_{r=0}^{p-1} a'_r E'_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\sum_{j=0}^{t} \binom{t}{j} (-1)^{t-j} \pi_{\mathfrak{p}}^{-je'} a'_{s,t} e'_s (a_{v'}\eta')^j,$$

and so

$$\Phi\left(z'_{\mathfrak{p}}\right) = \sum_{r=0}^{p-1} a'_r E_{\overline{cr}} + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\sum_{j=0}^{t} \binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-je'} a'_{s,t} V^{\left\lfloor \frac{cs}{p} \right\rfloor j} e_{\overline{cs}}(a_v\eta)^j.$$

From (6.2.1) we see that $p^2\mathfrak{M}_{H,\mathfrak{p}} \subseteq \mathfrak{A}_{H,\mathfrak{p}}$, so using the assumption that $V \equiv 1 \pmod{p^2(\zeta-1)}$ we have

$$\begin{aligned}\Phi\left(z'_{\mathfrak{p}}\right) &\equiv \sum_{r=0}^{p-1} a'_r E_{\overline{cr}} + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\sum_{j=0}^{t} \binom{t}{j}(-1)^{t-j}\pi_{\mathfrak{p}}^{-je'} a'_{s,t} e_{\overline{cs}}(a_v\eta)^j \pmod{\pi_{\mathfrak{p}}^{e'}\mathfrak{A}_{H,\mathfrak{p}}} \\ &\equiv \sum_{r=0}^{p-1} a'_r E_{\overline{cr}} + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} a'_{s,t}\left(\frac{e_{\overline{cs}}(a_v\eta) - e_{\overline{cs}}}{\pi_{\mathfrak{p}}^{e'}}\right)^t \pmod{\pi_{\mathfrak{p}}^{e'}\mathfrak{A}_{H,\mathfrak{p}}}.\end{aligned}$$

This satisfies (ii) since z'_p satisfies (b). So $\Phi\left(z'_{\mathfrak{p}}\right) \in \mathfrak{A}_{H,\mathfrak{p}}^{\times}$. This completes the proof. □

Corollary 8.4.5. Suppose that $V \equiv 1 \pmod{p^2(\zeta-1)}$, and that the idèle $(z'_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbb{J}(H')$ has trivial class in the quotient group

$$\frac{\mathbb{J}(H')}{(H')^{\times}\,\mathfrak{B}'}.$$

Then the idèle $\Phi\left((z'_{\mathfrak{p}})_{\mathfrak{p}}\right) \in \mathbb{J}(H)$ has trivial class in the quotient group

$$\frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathfrak{A}_H)}$$

Proposition 8.4.6. Suppose $V \equiv 1 \pmod{p^2(\zeta-1)}$. Let $(h'_{\mathfrak{p}})_{\mathfrak{p}}, (h_{\mathfrak{p}})_{\mathfrak{p}}$ be the idèles in $\mathbb{J}(H'), \mathbb{J}(H)$ respectively which correspond to the class of $\mathfrak{O}_L$ in $\mathrm{Cl}\left(\mathfrak{A}_{H'}\right), \mathrm{Cl}\left(\mathfrak{A}_H\right)$ according to (8.2.1). Then $\Phi((h'_{\mathfrak{p}})_{\mathfrak{p}})$ has the same class in the quotient group $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$ as $(h_{\mathfrak{p}})_{\mathfrak{p}}$.

Proof. We shall show that the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbb{J}(H)$ and the idèle $\Phi\left(h'_{\mathfrak{p}}\right)_{\mathfrak{p}} \in \mathbb{J}(H)$

differ only by an element of $H^{\times}\mathbb{U}(\mathfrak{A}_H)$. Recall that $q_{s,t} = \left\lfloor \frac{st}{p} \right\rfloor$. We have:

$$h_{\mathfrak{p}} = \begin{cases} \displaystyle\sum_{r=0}^{p-1} E_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} \zeta^{std(t-1)/2} v^{-pq_{s,t}} e_s(a_v\eta)^t & \mathfrak{p}|p\mathfrak{O}_K \\ \displaystyle\sum_{r=0}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^r)} E_r + \sum_{s=1}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^sV^{sj_{\mathfrak{p}}})} e_s(a_v\eta)^{j_{\mathfrak{p}}} & \mathfrak{p}|XV\mathfrak{O}_K \\ 1 & \text{otherwise} \end{cases}$$

where $0 \leq j_{\mathfrak{p}} \leq p-1$ is defined by

$$\begin{cases} j_{\mathfrak{p}} = 0 & \text{if } v_{\mathfrak{p}}(X) \equiv 0 \pmod{p} \text{ or } v_{\mathfrak{p}}(V) \equiv 0 \pmod{p} \\ v_{\mathfrak{p}}(XV^{j_{\mathfrak{p}}}) \equiv 0 \pmod{p} & \text{otherwise} \end{cases}$$

and

$$h'_{\mathfrak{p}} = \begin{cases} \displaystyle\sum_{r=0}^{p-1} E'_r + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1} \zeta^{std'(t-1)/2} (v')^{-pq_{s,t}} e'_s(a_{v'}\eta')^t & \mathfrak{p}|p\mathfrak{O}_K \\ \displaystyle\sum_{r=0}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}((V')^r)} E'_r + \sum_{s=1}^{p-1} \pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}((X')^s(V')^{sj'_{\mathfrak{p}}})} e'_s(a_{v'}\eta')^{j'_{\mathfrak{p}}} & \mathfrak{p}|XV\mathfrak{O}_K \\ 1 & \text{otherwise} \end{cases}$$

where $0 \leq j'_{\mathfrak{p}} \leq p-1$ is defined by

$$\begin{cases} j'_{\mathfrak{p}} = 0 & \text{if } v_{\mathfrak{p}}(X^c) \equiv 0 \pmod{p} \text{ or } v_{\mathfrak{p}}(V^c) \equiv 0 \pmod{p} \\ v_{\mathfrak{p}}\left(X^cV^{cj'_{\mathfrak{p}}}\right) \equiv 0 \pmod{p} & \text{otherwise} \end{cases}$$

We note that we have $j'_{\mathfrak{p}} = j_{\mathfrak{p}}$ for all primes $\mathfrak{p} \nmid p\mathfrak{O}_K$. If $\mathfrak{p} \nmid pXV\mathfrak{O}_K$ then we have $\Phi(h'_{\mathfrak{p}}) = h_{\mathfrak{p}}$ and there is nothing to prove. Suppose that $\mathfrak{p} \mid XV\mathfrak{O}_K$, and write

$X = u_x\pi_{\mathfrak{p}}^{v_{\mathfrak{p}}(X)}, V = u_v\pi_{\mathfrak{p}}^{v_{\mathfrak{p}}(V)}$ with $u_x, u_v \in \mathfrak{O}_{K,\mathfrak{p}}^{\times}$. Then

$$\begin{aligned}\Phi(h'_{\mathfrak{p}}) &= \sum_{r=0}^{p-1}\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^{cr})}E_{\overline{cr}} + \sum_{s=1}^{p-1}\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^{cs}V^{csj_{\mathfrak{p}}})}V^{\left\lfloor\frac{cs}{p}\right\rfloor j_{\mathfrak{p}}}e_{\overline{cs}}(a_v\eta)^{j_{\mathfrak{p}}} \\ &= \sum_{r=0}^{p-1}\pi_{\mathfrak{p}}^{-v_{\mathfrak{p}}\left(V^{\left\lfloor\frac{cr}{p}\right\rfloor}\right)}\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(V^{\overline{cr}})}E_{\overline{cr}} \\ &\quad + \sum_{s=1}^{p-1}\pi_{\mathfrak{p}}^{-v_{\mathfrak{p}}\left(X^{\left\lfloor\frac{cs}{p}\right\rfloor}\right)}\pi_{\mathfrak{p}}^{-v_{\mathfrak{p}}\left(V^{\left\lfloor\frac{cs}{p}\right\rfloor j_{\mathfrak{p}}}\right)}V^{\left\lfloor\frac{cs}{p}\right\rfloor j_{\mathfrak{p}}}\pi_{\mathfrak{p}}^{-r_{\mathfrak{p}}(X^{\overline{cs}}V^{\overline{cs}j_{\mathfrak{p}}})}e_{\overline{cs}}(a_v\eta)^{j_{\mathfrak{p}}},\end{aligned}$$

and so we have

$$\begin{aligned}\Phi(h'_{\mathfrak{p}}) &= \left(\sum_{r=0}^{p-1}u_v^{\left\lfloor\frac{cr}{p}\right\rfloor}V^{-\left\lfloor\frac{cr}{p}\right\rfloor}E_{\overline{cr}} + \sum_{s=1}^{p-1}u_x^{\left\lfloor\frac{cs}{p}\right\rfloor}X^{-\left\lfloor\frac{cs}{p}\right\rfloor}u_v^{\left\lfloor\frac{cs}{p}\right\rfloor j_{\mathfrak{p}}}e_{\overline{cs}}\right)h_{\mathfrak{p}} \\ &= \left(\sum_{r=0}^{p-1}u_v^{\left\lfloor\frac{cr}{p}\right\rfloor}E_{\overline{cr}} + \sum_{s=1}^{p-1}u_x^{\left\lfloor\frac{cs}{p}\right\rfloor}u_v^{\left\lfloor\frac{cs}{p}\right\rfloor j_{\mathfrak{p}}}e_{\overline{cs}}\right)\left(\sum_{r=0}^{p-1}V^{-\left\lfloor\frac{cr}{p}\right\rfloor}E_{\overline{cr}} + \sum_{s=1}^{p-1}X^{-\left\lfloor\frac{cs}{p}\right\rfloor}e_{\overline{cs}}\right)h_{\mathfrak{p}}.\end{aligned}$$

The first term of this lies in $\mathfrak{M}_{H,\mathfrak{p}}^{\times}$ and the second term lies in $H^{\times}$. Finally suppose that $\mathfrak{p} \mid p\mathfrak{O}_K$. Then

$$\Phi(h'_{\mathfrak{p}}) = \sum_{r=0}^{p-1}E_{\overline{cr}} + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{cstd(t-1)/2}v^{-pcq_{s,t}}V^{\left\lfloor\frac{cs}{p}\right\rfloor t}e_{\overline{cs}}(a_v\eta)^t.$$

We may write

$$h_{\mathfrak{p}} = \sum_{r=0}^{p-1}E_{\overline{cr}} + \sum_{s=1}^{p-1}\sum_{t=0}^{p-1}\zeta^{cstd(t-1)/2}v^{-pq_{\overline{cs},t}}e_{\overline{cs}}(a_v\eta)^t.$$

We shall show that

$$\frac{h_{\mathfrak{p}}}{\Phi(h'_{\mathfrak{p}})} \in \mathfrak{A}_{H,\mathfrak{p}}^{\times}.$$

By (8.1.3) it is sufficient to show that for each $s = 1, \ldots, p-1$ we have

$$\frac{e_{\overline{cs}} h_{\mathfrak{p}}}{e_{\overline{cs}} \Phi(h'_{\mathfrak{p}})} \in (1 + p^2 \mathfrak{M}_{H,\mathfrak{p}}).$$

For each $s = 1, \ldots, p-1$ we have

$$e_{\overline{cs}} h_{\mathfrak{p}} = e_{\overline{cs}} \Phi(h'_{\mathfrak{p}}) + \sum_{t=0}^{p-1} \left(v^{-pq_{\overline{cs},t}} - v^{-pcq_{s,t}} V^{\lfloor \frac{cs}{p} \rfloor t} \right) e_{\overline{cs}} (a_v \eta)^t$$

and so

$$\frac{e_{\overline{cs}} h_{\mathfrak{p}}}{e_{\overline{cs}} \Phi(h'_{\mathfrak{p}})} = 1 + \sum_{t=0}^{p-1} \frac{\left(v^{-pq_{\overline{cs},t}} - v^{-pcq_{s,t}} V^{\lfloor \frac{cs}{p} \rfloor t} \right) e_{\overline{cs}} (a_v \eta)^t}{e_{\overline{cs}} \Phi(h'_{\mathfrak{p}})}.$$

Since we are assuming that $V \equiv 1 \pmod{p^2(\zeta - 1)}$, it now suffices to show that $e_{\overline{cs}} \Phi(h'_{\mathfrak{p}}) \in (\zeta - 1) \mathfrak{M}_{H,\mathfrak{p}}^{\times}$. Let

$$\mu_{\overline{cs}} = \frac{e_{\overline{cs}} (a_v \eta) - e_{\overline{cs}}}{\pi_{\mathfrak{p}}^{e'}}.$$

Then

$$e_{\overline{cs}} (a_v \eta) = \pi_{\mathfrak{p}}^{e'} \mu_{\overline{cs}} + e_{\overline{cs}},$$

and using the binomial expansion we have

$$e_{\overline{cs}} \Phi(h'_{\mathfrak{p}}) = \sum_{t=0}^{p-1} \zeta^{cstd(t-1)/2} v^{-pq_{\overline{cs},t}} V^{\lfloor \frac{cs}{p} \rfloor t} \sum_{j=0}^{t} \binom{t}{j} \pi_{\mathfrak{p}}^{je'} \mu_{\overline{cs}}^{j}.$$

The coefficient C_j of a given $\mu_{\overline{cs}}^{j}$ is given by

$$\begin{aligned} C_j &= \sum_{t=j}^{p-1} \zeta^{cstd(t-1)/2} \binom{t}{j} v^{-pq_{\overline{cs},t}} V^{\lfloor \frac{cs}{p} \rfloor t} \pi_{\mathfrak{p}}^{je'} \\ &\equiv \pi_{\mathfrak{p}}^{je'} \sum_{t=j}^{p-1} \zeta^{cstd(t-1)/2} \binom{t}{j} \pmod{p^2(\zeta - 1)\mathfrak{M}_{H,\mathfrak{p}}} \end{aligned}$$

So

$$\begin{aligned}\pi_{\mathfrak{p}}^{-je'}C_j &\equiv \sum_{t=k}^{p-1}\binom{t}{j} \pmod{(\zeta-1)\mathfrak{M}_{H,\mathfrak{p}}}\\ &\equiv \binom{p}{j+1} \pmod{(\zeta-1)\mathfrak{M}_{H,\mathfrak{p}}}\\ &\equiv 0 \pmod{(\zeta-1)\mathfrak{M}_{H,\mathfrak{p}}}\end{aligned}$$

and so, by considering C_0, we see that

$$e_{\overline{cs}}\Phi(h'_{\mathfrak{p}}) \in (\zeta-1)\mathfrak{M}_{H,\mathfrak{p}}^{\times}.$$

This completes the proof. □

Proposition 8.4.7. Suppose that $V \equiv 1 \pmod{p^2(\zeta-1)}$. If the idèle $(h'_{\mathfrak{p}})$ has trivial class in the quotient group $\mathbb{J}(H')/(H')^{\times}\mathfrak{B}'$ then the idèle $h_{\mathfrak{p}}$ has trivial class in the quotient group $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$.

Proof. By (8.4.5) $\Phi((h'_{\mathfrak{p}})_{\mathfrak{p}})$ has trivial class in $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$ if $(h'_{\mathfrak{p}})_{\mathfrak{p}}$ has trivial class in $\mathbb{J}(H')/(H')^{\times}\mathfrak{B}'$, and by (8.4.6) $\Phi((h'_{\mathfrak{p}})_{\mathfrak{p}})$ has the same class in $\mathbb{J}(H)/H^{\times}\mathbb{U}(\mathfrak{A}_H)$ as $(h_{\mathfrak{p}})_{\mathfrak{p}}$. □

Corollary 8.4.8. Suppose that $V \equiv 1 \pmod{p^2(\zeta-1)}$. Fix a choice of subgroup T of $\mathrm{Gal}(L/K)$ of order p. If for some choice of $d \in \{1,\dots,p-1\}$ the tuple of fractional ideals defined in (8.2.4) has trivial class in the product of ray class groups

$$\mathrm{Cl}\,(\mathfrak{O}_K) \times \mathrm{Cl}_{p^2}(\mathfrak{O}_K)^{(p-1)} \times \mathrm{Cl}_{p^2}(\mathfrak{O}_{K(v)})^{(p-1)}$$

then $\mathfrak{O}_L$ is free over $\mathfrak{A}_{H_{T,d}}$ for all choices of $d \in \{1,\dots,p-1\}$.

Bibliography

[BS05] N. P. Byott and B. Sodaïgui. Galois module structure for dihedral extensions of degree 8: Realizable classes over the group ring. *Journal of Number Theory*, 112:1–19, 2005.

[Byo96] N. P. Byott. Uniqueness of Hopf-Galois structure for separable field extensions. *Communications in Algebra*, 24(10):3217 – 3228, 3705, 1996.

[Byo97] N. P. Byott. Tame realisable classes over Hopf orders. *Journal of Algebra*, 201:284–316, 1997.

[Byo00] N. P. Byott. Galois module theory and Kummer theory for Lubin-Tate formal groups. *Proc. Conf. on Algebraic Number Theory and Diophantine Analysis (Graz, 1998)*, pages 55–67, 2000.

[Byo02] N. P. Byott. Integral Hopf-Galois structures on degree p^2 extensions of $p-$adic fields. *Journal of Algebra*, 248:334–365, 2002.

[Chi00] L. N. Childs. *Taming Wild Extensions: Hopf Algebras and local Galois module theory.* American Mathematical Society, 2000.

[CR81a] C. W. Curtis and I. Reiner. *Methods of Representation Theory with Applications to Finite Groups and Orders*, volume 1. Wiley, 1981.

[CR81b] C. W. Curtis and I. Reiner. *Methods of Representation Theory with Applications to Finite Groups and Orders*, volume 2. Wiley, 1981.

[Frö83] A. Fröhlich. *Galois Module Structure of Algebraic Integers*. Springer, 1983.

[FT91] A. Fröhlich and M. J. Taylor. *Algebraic Number Theory*. Cambridge University Press, 1991.

[Lan99] S. Lang. *Algebra, Third Edition*. Addison Wesley, 1999.

[Leo59] H. W. Leopoldt. Uber die Hauptordnung der ganzen Elemente eines abelschen Zahlkorpers. *J. reine angew. Math.*, 201:119–149, 1959.

[Let98] G. Lettl. Relative Galois module structure of integers of local abelian fields. *Acta Arithmetica*, 3:235–248, 1998.

[Mol99] R. A. Mollin. *Algebraic Number Theory*. Chapman and Hall, 1999.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[Wat97] W.C. Waterhouse. *Introduction to Affine Group Schemes*. Springer, 1997.