Hopf-Galois module structure of some non-normal extensions

Submitted by

George Thomas Prestidge

to the University of Keele as a thesis for the degree of Doctor of Philosophy in Mathematics, June 2024.

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.

.....

George Thomas Prestidge

Abstract

We use Hopf-Galois theory to study the structure of rings of algebraic integers in some non-normal extensions of number fields which are tamely ramified, generalising results of Del Corso and Rossi for tamely ramified Kummer extensions.

Firstly we study tamely ramified non-normal extensions of number fields of the form $L = K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_r})$ for some prime number p and a_1, ..., $a_r \in \mathcal{O}_K$. We show that extensions of this form admit a unique almost classical Hopf-Galois structure and that if $r = 2$ then this is the only Hopf-Galois structure on the extension. We then obtain explicit $\mathcal{O}_{K,\mathfrak{p}}$-bases of $\mathcal{O}_{L,\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Using these, we show that $\mathcal{O}_L$ is locally free over its associated order in the unique almost classical Hopf-Galois structure on the extension. To obtain criteria for $\mathcal{O}_L$ to be free over this associated order we use an idèlic description of the locally free class group of the maximal order.

Secondly we conduct an analogous study of tamely ramified non-normal extensions of number fields of the form $L = K(\sqrt[m]{a})$ for some odd square-free number $m = p_1...p_r$ and $a \in \mathcal{O}_K$. Once again, we find that extensions of this form admit a unique almost classical Hopf-Galois structure. Once again we show that if $r = 2$ then this is the only Hopf-Galois structure on the extension. We again use explicit $\mathcal{O}_{K,\mathfrak{p}}$-bases of $\mathcal{O}_{L,\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ to show that $\mathcal{O}_L$ is locally free over its associated order in the almost classical Hopf-Galois structure on the extension. Once again, to obtain criteria for $\mathcal{O}_L$ to be free over this associated order we use an idèlic description of the locally free class group of the maximal order.

In both cases, the criteria we obtain are identical to those obtained by Del Corso and Rossi in the Galois case.

Acknowledgements

I would like to thank my advisor, Dr. Paul Truman, for the invaluable advice and guidance he has given me whilst completing this thesis. I would also like to thank Dr. Griff Elder for giving me the opportunity to present my research at the Hopf algebras and Galois module theory conference.

Contents

Chapter 1

Introduction

The module theoretic result perspective on Galois theory began with the normal basis theorem (see Theorem 2.3.9): if L/K is a Galois extension of fields with Galois group G then L is a free $K[G]$-module of rank one. (Equivalently: L has a K-basis of the form $\{g(x)|g \in G\}$ for some $x \in L$.) If L/K is a Galois extension of local or global fields then it is natural to ask an analogous question at integral level: is $\mathcal{O}_L$ a free module (necessarily of rank one) over the integral group ring $\mathcal{O}_K[G]$? (Equivalently: does $\mathcal{O}_L$ have an $\mathcal{O}_K$-basis of the form $\{g(x)|g \in G\}$ for some $x \in \mathcal{O}_L$?) The study of questions of this form is part of Galois module theory. The answer to this question is connected to the ramification of prime ideals in the extension.

The Hilbert-Speiser theorem gives a criterion for freeness in the particular case that the base field is $\mathbb{Q}$: if $K = \mathbb{Q}$, the group G is abelian and $L/\mathbb{Q}$ is tamely ramified, then $\mathcal{O}_L$ is a free $\mathbb{Z}G$-module of rank one (see Theorem 132 of [Hil13]). In general working directly with rings of integers in number fields is difficult: if the class number of K is not equal to one then $\mathcal{O}_K$ is not a principal ideal domain, so $\mathcal{O}_L$ might not have an $\mathcal{O}_K$-basis at all.

One way to address this problem is to work with completions. For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we can form the completion of K at $\mathfrak{p}$, by completing K with respect to the absolute value arising from $\mathfrak{p}$, denoted $K_\mathfrak{p}$ which is a local field. If L/K is a Galois extension of number fields with Galois group G, then the $K_\mathfrak{p}$-algebra

$L_{\mathfrak{p}} = K_{\mathfrak{p}} \otimes_K L$ is a free $K_{\mathfrak{p}}[G]$-module of rank one. To see this, since L is a module over $K[G]$ the $K_{\mathfrak{p}}$ algebra $L_{\mathfrak{p}}$ is a module over $K_{\mathfrak{p}} \otimes K[G]$ which identifies naturally with the group algebra $K_{\mathfrak{p}}[G]$. Since L is a free $K[G]$-module of rank one there exists $x \in L$ such that the set $\{\sigma(x) | \sigma \in G\}$ is a K-basis of L which implies that the set $\{1 \otimes \sigma(x) | \sigma \in G\}$ is a $K_{\mathfrak{p}}$-basis of $L_{\mathfrak{p}}$ which implies that $L_{\mathfrak{p}}$ is a free $K_{\mathfrak{p}}[G]$-module of rank one. In general $L_{\mathfrak{p}}$ is isomorphic to a product of local fields.

Inside $K_{\mathfrak{p}}$ we have the completed ring of integers $\mathcal{O}_{K,\mathfrak{p}}$ which is a principal ideal domain. Since $\mathcal{O}_{K,\mathfrak{p}}$ is a principal ideal domain, this means that the $\mathcal{O}_{K,\mathfrak{p}}$-algebra $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{O}_L$ has an $\mathcal{O}_{K,\mathfrak{p}}$-basis and we can study the structure of $\mathcal{O}_{L,\mathfrak{p}}$ as a module over $\mathcal{O}_{K,\mathfrak{p}}[G]$. We say that $\mathcal{O}_L$ is a locally free $\mathcal{O}_K[G]$-module to mean that $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{O}_{K,\mathfrak{p}}[G]$-module for each $\mathfrak{p}$. This is a weaker condition than $\mathcal{O}_L$ being a free $\mathcal{O}_K[G]$-module.

Noether's theorem gives a criterion for local freeness: $\mathcal{O}_L$ is a locally free $\mathcal{O}_K[G]$-module if and only if L/K is at most tamely ramified (see Theorem 2.3.15). Since Noether's theorem provides a necessary and sufficient condition for $\mathcal{O}_L$ to be locally free over $\mathcal{O}_K[G]$, other techniques are required to study extensions that are wildly ramified. One of these is to replace the integral group ring $\mathcal{O}_K[G]$ with a larger subring of $K[G]$, called the associated order of $\mathcal{O}_L$ in $K[G]$:

$$\mathcal{A}_{K[G]} = \{z \in K[G] | z \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

As before, we say that $\mathcal{O}_L$ is a locally free $\mathcal{A}_{K[G]}$-module to mean that $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{K[G],\mathfrak{p}}$-module for each $\mathfrak{p}$. If $\mathcal{O}_L$ is a locally free $\mathcal{A}_{K[G]}$-module then we can obtain criteria for it to be free by using idèles, which allow us to collect together detailed information about the structure of $\mathcal{O}_{L,\mathfrak{p}}$ for each $\mathfrak{p}$.

Returning to tamely ramified extensions, a natural class of extensions to study are tamely ramified Kummer extensions L/K. Various authors have studied certain families of these and obtained criteria for $\mathcal{O}_L$ to be a free $\mathcal{O}_K[G]$-module. These results all revolve around certain ideals of $\mathcal{O}_K$, defined as follows: If L/K is a Kummer extension of degree N and exponent m and α_1, ..., α_r are a set of integral Kummer generators for L/K then we write $a_i = \alpha_i^m \in \mathcal{O}_K$ for each i. To ease notation we denote a list of indices j_1, ..., $j_r \in \mathbb{N}^r$ by $\boldsymbol{j}$ (where $\mathbb{N}$ denotes the

natural numbers including zero) and write $\boldsymbol{a^j}$ as a shorthand for $a_1^{j_1}...a_r^{j_r}$. We then define the ideals associated to $\boldsymbol{a}\mathcal{O}_K$ to be the ideals

$$\mathfrak{b}_{\boldsymbol{j}} = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(\boldsymbol{a^j})}{m} \rfloor}.$$

Gómez-Ayala studies tamely ramified Kummer extensions L/K of prime degree p in [GA94]. He shows that $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module if and only if there exists an integral Kummer generator α for L/K such that the ideals $\mathfrak{b}_j$ associated to $a\mathcal{O}_K$ are principal with generators b_j such that

$$\sum_{j=0}^{p-1} \frac{\alpha^j}{b_j} \equiv 0 \pmod{p\mathcal{O}_L}.$$

Furthermore, in this case the element

$$\frac{1}{p} \sum_{j=0}^{p-1} \frac{\alpha^j}{b_j}$$

is a free generator of $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module.

Ichimura studies the case in which L/K is a tamely ramified cyclic Kummer extension of arbitrary degree in [Ich04] and a criterion for the freeness of $\mathcal{O}_L$ over $\mathcal{O}_K[G]$ in this case is given by Del Corso and Rossi in [DCR10].

The most general result in this area is also due to Del Corso and Rossi (see Theorem 11 of [DCR13]). They show that if L/K is a tamely ramified Kummer extension of degree N and exponent m then $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module if and only if there exists a set of integral Kummer generators α_1, ..., α_r for L/K such that the ideals $\mathfrak{b}_{\boldsymbol{j}}$ associated to $\boldsymbol{a}\mathcal{O}_K$ are principal with generators $b_{\boldsymbol{j}}$ such that

$$\sum_{\boldsymbol{j}} \frac{\boldsymbol{\alpha^j}}{b_{\boldsymbol{j}}} \equiv 0 \pmod{N\mathcal{O}_L}.$$

Furthermore, in this case the element

$$\frac{1}{N} \sum_{\boldsymbol{j}} \frac{\boldsymbol{\alpha^j}}{b_{\boldsymbol{j}}}$$

is a free generator of $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module.

Hopf-Galois theory generalises the situation described above. The group algebra $K[G]$ is an example of a K-Hopf algebra and the action of $K[G]$ on L is

an example of a Hopf-Galois structure on the extension. In general, a Hopf-Galois structure on a finite extension of fields consists of a K-Hopf algebra H of dimension $[L : K]$ as a K-vector space and an action of H on L satisfying certain technical conditions (see Definition 2.6.6). Hopf-Galois structures can be used to generalise the concepts from Galois theory, such as the Galois correspondence, to extensions that are inseparable or non-normal. A given extension may admit a number of different Hopf-Galois structures which raises the possibility of making comparisons between them. If H gives a Hopf-Galois structure on a finite (potentially non-normal) extension of number fields L/K then we may define the associated order of $\mathcal{O}_L$ inside H

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

and study the structure of $\mathcal{O}_L$ as an $\mathcal{A}_H$-module.

This approach has been fruitfully applied to wildly ramified extensions of local fields (see for example [Byo00], [Byo02] and [BCE18]). The application of these ideas to global fields is less well developed. In [Tru11], Truman uses Hopf-Galois theory to study the structure of rings of algebraic integers in tamely ramified Kummer extensions of number fields and in [GMR22] Gil-Muñoz and Rio do the same for both tamely and wildly ramified quartic extension of $\mathbb{Q}$.

In [Tru20], Truman studies tamely ramified radical extensions of number fields L/K of prime degree p in which K does not contain a primitive p^{th} root of unity. This is a non-normal analogue of the situation considered by Gómez-Ayala. Extensions of this form admit exactly one Hopf-Galois structure. Under the assumption that the prime number p is unramified in K, Truman shows that $\mathcal{O}_L$ is locally free over its associated order in this Hopf-Galois structure and determines criteria for it to be free. Interestingly, these criteria are identical to those obtained by Gómez-Ayala for the Galois case.

In this thesis we generalise Truman's results to two large families of non-normal tamely ramified extensions of number fields: those of the form $L = K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_r})$ for some prime number p and $a_1, ..., a_r \in \mathcal{O}_K$ and those of the form $L = K(\sqrt[m]{a})$ for some odd square-free number m and $a \in \mathcal{O}_K$. Extensions of these forms potentially

admit many Hopf-Galois structures, but we show that they admit a unique Hopf-Galois structure with the additional property of being so-called almost classical. We show that in both cases $\mathcal{O}_L$ is locally free over its associated order in this Hopf-Galois structure and determine criteria for it to be free. In the same way that the criteria in Truman's paper are identical to those obtained by Gómez-Ayala for the Galois case, our criteria are identical to those obtained by Del Corso and Rossi in the Galois case.

In Chapter 2 we give formal statements of the definitions and results that we shall use in what follows including ramification theory, completions, idèles and locally free class groups and Hopf algebras and Hopf-Galois theory. As a worked example of the theory in action we provide a new proof of a special case of the result of Del Corso and Rossi, based upon a theorem of Bley and Johnston, that makes use of the unique maximal order in $K[G]$ in place of the associated order. We also give an outline of the proof of Truman's result for tamely ramified radical extensions of prime degree which is based on many of the same ideas.

In Chapters 3 and 4 we study tamely ramified non-normal extensions of number fields of the form $L = K(\sqrt[p]{a_1}, ..., \sqrt[p]{a_r})$ for some prime number p and a_1, ..., $a_r \in \mathcal{O}_K$. We show that extensions of this form admit a unique almost classical Hopf-Galois structure and that if $r = 2$ then this is the only Hopf-Galois structure on the extension. We then obtain explicit $\mathcal{O}_{K,\mathfrak{p}}$-bases of $\mathcal{O}_{L,\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Using these, we show that $\mathcal{O}_L$ is locally free over its associated order in the unique almost classical Hopf-Galois structure on the extension. To obtain criteria for $\mathcal{O}_L$ to be free over this associated order we use a result of Bley and Johnston, which allows us to work with the maximal order in place of the associated order and then use an idèlic description of the locally free class group of this maximal order. The criteria we obtain are identical to those obtained by Del Corso and Rossi in the Galois case.

In Chapters 5 and 6 we conduct an analogous study of tamely ramified non-normal extensions of number fields of the form $L = K(\sqrt[m]{a})$ for some odd square-free number m and $a \in \mathcal{O}_K$. Once again, we find that extensions of this form

admit a unique almost classical Hopf-Galois structure. Our approach is essentially the same: using explicit $\mathcal{O}_{K,\mathfrak{p}}$-bases of $\mathcal{O}_{L,\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we show that $\mathcal{O}_L$ is locally free over its associated order in the almost classical Hopf-Galois structure on the extension. Once again, we combine the result of Bley and Johnston with idèlic machinery to obtain criteria for $\mathcal{O}_L$ to be free over this associated order and once again we find that these criteria are identical to those obtained by Del Corso and Rossi in the Galois case.

Chapter 2

Background material

2.1 Algebraic number theory and ramification

Throughout this section we suppose that L/K is a finite extension of number fields with rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$ respectively.

Definition 2.1.1. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$. We say* $\mathfrak{P}$ lies above $\mathfrak{p}$ *if $\mathfrak{P}|\mathfrak{p}\mathcal{O}_L$.*

Remark 2.1.2. *Since $\mathcal{O}_L$ is a Dedekind domain $\mathfrak{p}\mathcal{O}_L$ factorises uniquely into prime ideals of $\mathcal{O}_L$.*

A reference for the following is page 110 of [FT91].

Definition 2.1.3. *Suppose the unique prime factorisation of $\mathfrak{p}\mathcal{O}_L$ is $\mathfrak{P}_1^{e_1}...\mathfrak{P}_g^{e_g}$ where each $\mathfrak{P}_i$ is distinct. The integer e_i denotes the* ramification index *of $\mathfrak{P}_i$ over $\mathfrak{p}$.*

For each i, $\mathcal{O}_L/\mathfrak{P}_i$ is an extension of $\mathcal{O}_K/\mathfrak{p}$, f_i denotes the degree of this extension which is called the residue class degree.

Theorem 2.1.4. $\sum_{i=1}^{g} e_i f_i = [L : K]$.

Proof. See pages 46 and 47 of [Neu13]. □

Corollary 2.1.5. *In the case of Galois extensions we have $e_1 = ... = e_g = e$ and $f_1 = ... = f_g = f$ hence the previous result simplifies to $efg = n$.*

Definition 2.1.6. *A prime ideal* $\mathfrak{p}$ *is* unramified *in* L *if* $e_i = 1$. *If* $g > 1$, $\mathfrak{p}$ splits *in* L. *If* $g = 1$ *and* $e_1 = 1$, $\mathfrak{p}$ *is* inert *in* L.

A prime ideal $\mathfrak{p}$ *is* ramified *in* L *if* $e_i > 1$ *for some* i. *Let* p *denote the residue characteristic of* $\mathfrak{p}$. *The extension* L/K *is* tamely ramified *if* $gcd(e_i, p) = 1$ *for all* i. *The extension* L/K *is* wildly ramified *if* $gcd(e_i, p) > 1$ *for some* i.

Remark 2.1.7. *Henceforth we will say simply "*tame*" to mean at most tamely ramified.*

Proposition 2.1.8. *Let* $K \subseteq F \subseteq L$ *be field extensions. The extension* L/K *is tame if and only if the extensions* L/F *and* F/K *are both tame.*

Proof. See Corollary 7.8 of [Neu13]. □

Proposition 2.1.9. *Let* F_1/K *and* F_2/K *be field extensions and let* L *be the compositum i.e.* $L = F_1F_2$. *The extension* L/K *is tame if and only if the extensions* F_1/K *and* F_2/K *are both tame.*

Proof. See Corollary 7.9 of [Neu13]. □

Proposition 2.1.10. *Let* L/K *be a Galois extension. The extension* L/K *is tame if and only if the trace map* $\mathrm{Tr} : \mathcal{O}_L \to \mathcal{O}_K$ *is surjective.*

Proof. See Chapter I, Section 3, Corollary 2 of [Frö83]. □

Proposition 2.1.11. *Let* $F = K(\zeta)$ *for* ζ *some primitive* p^{th} *root of unity. We have an equality of ideals* $(\zeta - 1)^{p-1}\mathcal{O}_F = p\mathcal{O}_F$ *and* F/K *is tame.*

Proof. See 1.15 in Section VI.1 on page 210 of [FT91]. □

2.2 Completions

For a general extension of number fields L/K, the ring of integers $\mathcal{O}_K$ need not be a principal ideal domain, so $\mathcal{O}_L$ won't necessarily have an integral basis over $\mathcal{O}_K$. When we complete at a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the ring $\mathcal{O}_{K,\mathfrak{p}}$ is a principal ideal domain, and $\mathcal{O}_{L,\mathfrak{p}}$ is a finitely generated torsion free $\mathcal{O}_{K,\mathfrak{p}}$-module, so it does

have an integral basis over $\mathcal{O}_{K,\mathfrak{p}}$ (see 4.1 in Section II.4 on page 88 of [FT91]). For $a \in \mathcal{O}_K$ we get an ideal $a\mathcal{O}_K = \langle a \rangle$. For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, set $v_\mathfrak{p}(a)$ to be the exact power of $\mathfrak{p}$ in the factorisation of $a\mathcal{O}_K$. A typical element of K is $x = \frac{a}{b}$ where a, $b \in \mathcal{O}_K$.

Definition 2.2.1. *Define the* valuation $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ *by* $v_\mathfrak{p}(x) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b)$ *with* x, a *and* b *as defined above.*

Remark 2.2.2. *The valuation has the following properties.*

1. $v_\mathfrak{p}(xy) = v_\mathfrak{p}(x) + v_\mathfrak{p}(y)$.

2. $v_\mathfrak{p}(x + y) \geq min(v_\mathfrak{p}(x), v_\mathfrak{p}(y))$.

Using this valuation, we define an absolute value on K as follows.

Definition 2.2.3. *We can now define the* $\mathfrak{p}$-adic absolute value $|\cdot|_\mathfrak{p} : K \to \mathbb{Q}_{\geq 0}$ *by* $|x|_\mathfrak{p} = p^{-f v_\mathfrak{p}(x)}$ *for* $x \in K$ *with* f *defined as in Definition 2.1.3.*

If we complete K with respect to the $\mathfrak{p}$-adic absolute value, we get a *local field* $K_\mathfrak{p}$. If V is a K-vector space we write $V_\mathfrak{p}$ for the $K_\mathfrak{p}$-vector space $K_\mathfrak{p} \otimes_K V$. In particular, we write $L_\mathfrak{p} = K_\mathfrak{p} \otimes_K L$. Note, however, that $L_\mathfrak{p}$ will not be a field in general. We have an isomorphism of $K_\mathfrak{p}$-algebras $L_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$ where the product is taken over the prime ideals of $\mathcal{O}_L$ lying above $\mathfrak{p}$, and each $L_\mathfrak{P}$ is a local field (see [FT91]). Inside $K_\mathfrak{p}$ we have its ring of integers $\mathcal{O}_{K,\mathfrak{p}}$ which is a *valuation ring* defined as

Definition 2.2.4. $\mathcal{O}_{K,\mathfrak{p}} = \{x \in K_\mathfrak{p} \mid v_\mathfrak{p}(x) \geq 0\} = \{x \in K_\mathfrak{p} \mid |x|_\mathfrak{p} \leq 1\}$.

$\mathcal{O}_{K,\mathfrak{p}}$ is a *local ring*, it has a unique maximal ideal $\mathfrak{p} = \{x \in \mathcal{O}_{K,\mathfrak{p}} | v_\mathfrak{p}(x) \geq 1\}$. $\mathcal{O}_{K,\mathfrak{p}}$ is a principal ideal domain since $\mathfrak{p} = \langle \pi_\mathfrak{p} \rangle$ with $v_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. Just like for number fields, $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}$ is a finite field of characteristic p, called the *residue field* $k_\mathfrak{p}$ and p is called the *residue characteristic*.

Let K be a number field such that its ring of algebraic integers $\mathcal{O}_K$ is a Dedekind domain and let V be a finite dimensional vector space over K. An $\mathcal{O}_K$*-lattice* in V is a finitely generated $\mathcal{O}_K$-submodule M of V that contains a K-basis of V. Let

M and N be $\mathcal{O}_K$-lattices in an n dimensional vector space V. For each prime $\mathfrak{p}$, $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are free $\mathcal{O}_{K,\mathfrak{p}}$-modules of rank n. Let x_1, ..., x_n be an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $M_\mathfrak{p}$ and let y_1, ..., y_n be an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $N_\mathfrak{p}$. Let $V_\mathfrak{p}$ denote the ambient vector space $V_\mathfrak{p} := V \otimes_K K_\mathfrak{p}$. In this space, we can write $y_j = \sum_{i=1}^{n} c_{ij}x_i$ with $c_{ij} \in K_\mathfrak{p}$ and let $C = [c_{ij}]$. Then $[M_\mathfrak{p} : N_\mathfrak{p}] = det(C) \in K_\mathfrak{p}$ and in particular, if $M_\mathfrak{p} = N_\mathfrak{p}$, then $[M_\mathfrak{p} : N_\mathfrak{p}] \in \mathcal{O}_{K,\mathfrak{p}}^\times$.

Theorem 2.2.5. *There exists a unique fractional ideal I of K such that $I_\mathfrak{p} = [M_\mathfrak{p} : N_\mathfrak{p}]$ for all $\mathfrak{p}$. Also note that $v_\mathfrak{p}(I) = v_\mathfrak{p}([M_\mathfrak{p} : N_\mathfrak{p}])$ for all $\mathfrak{p}$.*

Proof. See Chapter 2, Section 4 of [FT91]. □

Definition 2.2.6. *We define the* index $[M : N]$ *to be this fractional ideal I.*

We now define the discriminant. Suppose V has a symmetric non-degenerate bilinear form $b : V \times V \to K$. For example, if V is a number field, we can take the bilinear form to be the trace pairing $b(x, y) = \mathrm{Tr}(xy)$. Let M be an $\mathcal{O}_K$-lattice in V. For each $\mathfrak{p}$, $M_\mathfrak{p}$ is a free $\mathcal{O}_{K,\mathfrak{p}}$-module of rank n. Define the *discriminant of $M_\mathfrak{p}$* (with respect to b) to be $\mathfrak{d}(M_\mathfrak{p}) = det(b(x_i, x_j)) \in K_\mathfrak{p}$ where the elements x_i and x_j come from a basis of V. Note that the discriminant does not depend on the choice of basis.

Theorem 2.2.7. *There exists a unique fractional ideal $\mathfrak{d}(M)$ of K with the property that $v_\mathfrak{p}(\mathfrak{d}(M)) = v_\mathfrak{p}(\mathfrak{d}(M_\mathfrak{p}))$ for all $\mathfrak{p}$.*

Proof. See Chapter 3, Section 2 of [FT91].. □

Definition 2.2.8. *We define the* discriminant $\mathfrak{d}(M)$ *to be this fractional ideal.*

Lemma 2.2.9. *If M and N are lattices, then $\mathfrak{d}(N) = \mathfrak{d}(M)[M : N]^2$.*

Proof. See Chapter 3, Section 2, result 2.4 of [FT91]. □

We now focus on the $\mathcal{O}_K$-lattice $\mathcal{O}_L$, and record some tools for finding local integral bases of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{O}_{K,\mathfrak{p}}$.

Theorem 2.2.10. *Let L/K denote a finite separable extension, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ that lies above $\mathfrak{p}$ (then $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is an extension of local fields).*

- *The following conditions are equivalent*
  - *$L_{\mathfrak{P}} = K_{\mathfrak{p}}(\lambda)$ for λ a root of some Eisenstein polynomial $g(X)$.*
  - *$L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is totally ramified.*
  - *$\mathcal{O}_{L,\mathfrak{P}} = \mathcal{O}_{K,\mathfrak{p}}[\lambda]$ for a uniformising parameter λ of L.*
- *If the first condition above is satisfied, then λ is a uniformising parameter and $deg(g) = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ and so g is irreducible in $K_{\mathfrak{p}}$.*
- *the minimal polynomial over $K_{\mathfrak{p}}$ of a uniformising parameter of a totally ramified separable extension $L_{\mathfrak{P}}$ of $K_{\mathfrak{p}}$ is an Eisenstein polynomial over $K_{\mathfrak{p}}$.*

Proof. See Theorem 24 in Section III.3 of [FT91]. □

Definition 2.2.11. *Let L/K be a finite extension with intermediate fields F_1 and F_2. We say that F_1 and F_2 are* linearly disjoint *if any K-basis of F_1 remains linearly independent over F_2.*

Lemma 2.2.12. *If F_1 and F_2 are linearly disjoint, then $F_1 \cap F_2 = K$. If at least one of the extensions F_1/K and F_2/K is Galois, then the converse holds.*

Proof. See 2.13 in Section III.2 on page 125 of [FT91]. □

Definition 2.2.13. *Let L/K be a finite extension of number fields with intermediate fields F_1 and F_2. We say that F_1 and F_2 are* arithmetically disjoint *if they are linearly disjoint and $\mathfrak{d}(\mathcal{O}_{F_1})$ and $\mathfrak{d}(\mathcal{O}_{F_2})$ are coprime. Note that in general, these discriminants are ideals, as defined in Definition 2.2.8 and in this case the bilinear form is given by the trace.*

Theorem 2.2.14. *Let L/K be a finite extension of number fields with intermediate fields F_1 and F_2. If F_1 and F_2 are arithmetically disjoint and L is equal to their compositum F_1F_2, then $\{xy | x \in \mathcal{O}_{F_1}, y \in \mathcal{O}_{F_2}\} = \mathcal{O}_L$.*

Proof. See 2.13 in Section III.2 on page 125 of [FT91]. □

Remark 2.2.15. *The previous theorem also applies* locally.

Remark 2.2.16. *If the extensions aren't arithmetically disjoint, then* $\{xy|x \in \mathcal{O}_{F_1}, y \in \mathcal{O}_{F_2}\} \subsetneqq \mathcal{O}_L$.

2.3 Galois module theory

Definition 2.3.1. *Let* R *be a commutative ring with unity. An* R-algebra *is an* R*-module* A *with a multiplication map* $\mu : A \otimes A \to A$ *which is associative i.e. the following diagram commutes*

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

and a unit map $\iota : R \to A$ *which is unitary i.e. the following diagrams commute.*

$$\begin{array}{ccc} A \otimes R & \xrightarrow{1 \otimes \iota} & A \otimes A \\ & \searrow^{\textit{scalar multiplication}} & \downarrow{\scriptstyle \mu} \\ & & A \end{array}$$

$$\begin{array}{ccc} R \otimes A & \xrightarrow{\iota \otimes 1} & A \otimes A \\ & \searrow^{\textit{scalar multiplication}} & \downarrow{\scriptstyle \mu} \\ & & A \end{array}$$

Remark 2.3.2. *In this thesis we will mainly consider the specific case of* K*-algebras where* K *is a field. All of the* K*-algebras that we will consider have finite dimension as* K*-vector spaces.*

Example 2.3.3. *Let* K *be a field and* G *be a finite group. The* group algebra $K[G]$ *is an example of a* K*-algebra.*

Definition 2.3.4. *Let* K *be a number field and let* A *be a* K*-algebra. An* $\mathcal{O}_K$-order *in* A *is a subring* Λ *of* A *containing* $\mathcal{O}_K$ *such that* Λ *is finitely generated over* $\mathcal{O}_K$ *and* $K \otimes \Lambda \cong A$ *i.e.* Λ *contains a* K*-basis of* A.

Example 2.3.5. *$\mathcal{O}_K[G]$ is an $\mathcal{O}_K$-order in $K[G]$.*

Definition 2.3.6. *An order is said to be* maximal *if it is not properly contained in another order.*

Theorem 2.3.7. *Let K be a number field with ring of integers $\mathcal{O}_K$ and let A be a K-algebra. $\mathcal{O}_K$-orders have the following properties.*

1. *Every order in A is contained in some maximal order.*
2. *The K-algebra A has at least one maximal order.*
3. *If A is commutative, then A has a unique maximal order $\mathcal{M}$. Also, $\mathcal{M}$ is the integral closure of $\mathcal{O}_K$ in A.*

Proof. See Theorem 26.5, Corollary 26.6 and Proposition 26.10 of [CR81a]. □

We will now discuss the normal basis theorem which can be viewed as a module theoretic interpretation of Galois theory.

Definition 2.3.8. *Let L/K be a finite Galois extension of number fields with Galois group G. A* normal basis *of L/K is a basis of the form $\{\sigma(x)|\sigma \in G\}$.*

Theorem 2.3.9 (Normal Basis Theorem)**.** *For Galois extensions, it is always possible to find a normal basis.*

Proof. See Chapter VI, Section 13 of [Lan04]. □

Remark 2.3.10. *The existence of a normal basis is equivalent to saying that L is a free $K[G]$-module of rank one and the Normal Basis Theorem says that for Galois extensions, this is always the case.*

Given an extension L/K of number fields a common problem in Galois module theory is to attempt to determine an integral analogue of the normal basis theorem i.e. whether $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module. A problem here is that $\mathcal{O}_K[G]$ often isn't large enough for this to be the case. This motivates the definition of the associated order. The following definition and remark are based on Definition 24.3 of [CR81a].

Definition 2.3.11. *The largest subring of $K[G]$ for which $\mathcal{O}_L$ is a module is*

$$\mathcal{A}_{K[G]} = \{z \in K[G] | z \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

This is called the associated order of $\mathcal{O}_L$ in $K[G]$.

Remark 2.3.12. *$\mathcal{A}_{K[G]}$ is an order in $K[G]$ because it is finitely generated and projective as an $\mathcal{O}_K$-module and it contains a basis of $K[G]$ i.e. $K \otimes_{\mathcal{O}_K} \mathcal{A}_{K[G]} = K[G]$.*

Lemma 2.3.13. *The associated order is the only order in $K[G]$ over which $\mathcal{O}_L$ can possibly be free.*

Proof. See Chapter 3 of [Chi00]. □

Proposition 2.3.14. $\mathcal{O}_K[G] \subseteq \mathcal{A}_{K[G]}$.

Proof. Let $x \in \mathcal{O}_L$, then $g(x) \in \mathcal{O}_L$ for all $g \in G$, since $g(x)$ is a root of the minimal polynomial of x over K. Hence if $z = \sum_{g \in G} c_g g \in \mathcal{O}_K[G]$ (with $c_g \in \mathcal{O}_K$ for each $g \in G$) then

$$z \cdot x = \sum_{g \in G} c_g g(x) \in \mathcal{O}_L,$$

and so $z \in \mathcal{A}_{K[G]}$. Thus $\mathcal{O}_K[G] \subseteq \mathcal{A}_{K[G]}$. □

Theorem 2.3.15 (Noether)**.** *If L/K is a tame Galois extension with Galois group G, then $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{O}_{K,\mathfrak{p}}[G]$-module (of rank one) for each $\mathfrak{p}$.*

Proof. See Theorem 1.2 of [Tho10]. □

Definition 2.3.16. *In this case, we say that $\mathcal{O}_L$ is* locally free *over $\mathcal{O}_K[G]$.*

2.4 Idèles and Class Groups

Let K be a number field, A be a commutative K-algebra and Λ be an $\mathcal{O}_K$-order in A. Recall (from Section 2.2) that if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ we write $A_\mathfrak{p} = K_\mathfrak{p} \otimes_K A$ and $\Lambda_\mathfrak{p} = \mathcal{O}_{K,\mathfrak{p}} \otimes_{\mathcal{O}_K} \Lambda$; then $\Lambda_\mathfrak{p}$ is an $\mathcal{O}_{K,\mathfrak{p}}$-order in $A_\mathfrak{p}$. Also we define a Λ-*lattice* to be a finitely generated projective $\mathcal{O}_K$-module which is also a Λ-module. If X is a Λ-lattice then for each prime $\mathfrak{p}$ of $\mathcal{O}_K$ we write $X_\mathfrak{p} = \mathcal{O}_{K,\mathfrak{p}} \otimes_{\mathcal{O}_K} X$, and then $X_\mathfrak{p}$ is a $\Lambda_\mathfrak{p}$-lattice.

Definition 2.4.1. *We say that X is a* locally free Λ*-lattice if $X_{\mathfrak{p}}$ is a free $\Lambda_{\mathfrak{p}}$-module for each $\mathfrak{p}$.*

We say that two locally free Λ-lattices of rank one are *stably isomorphic* if $X \oplus \Lambda^k \cong Y \oplus \Lambda^k$ for some $k \geq 0$. Let $[X]$ denote the stable isomorphism class of X and let $\mathrm{Cl}(\Lambda)$ denote the set of these classes. It can be shown (see Section 51 of [CR81b]) that $X \oplus Y \cong \Lambda \oplus Z$ for some locally free Λ-lattice Z of rank one; using this we define a binary operation on $\mathrm{Cl}(\Lambda)$ by $[X] + [Y] = [Z]$ whenever $X \oplus Y \cong \Lambda \oplus Z$. this binary operation gives a group structure on $\mathrm{Cl}(\Lambda)$.

Definition 2.4.2. *The set* $\mathrm{Cl}(\Lambda)$ *with the binary operation described above is called the* locally free class group of Λ.

Theorem 2.4.3. *Since A is commutative, a Λ-lattice X has trivial class in* $\mathrm{Cl}(\Lambda)$ *if and only if it is a free Λ-module.*

Proof. See Theorem 24 in Section 51 of [CR81b]. □

Remark 2.4.4. *In full generality X having trivial class is only a necessary condition for it to be a free Λ-module (see Section 51 of [CR81b]). Since we are specialising to cases where A is a* commutative *algebra, in our case this condition is also sufficient.*

Next, we obtain a more concrete description of $\mathrm{Cl}(\Lambda)$ and a method for describing the class of a locally free Λ-lattice in $\mathrm{Cl}(\Lambda)$. This material is based on Section 49A of [CR81a].

Definition 2.4.5. *For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $a_{\mathfrak{p}} \in A_{\mathfrak{p}}^{\times}$. An* idèle *is an infinite sequence of these elements $a_{\mathfrak{p}}$ indexed by the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, written as $(a_{\mathfrak{p}})_{\mathfrak{p}}$.*

Definition 2.4.6. *The* idèle group of A *is a subgroup of the direct product $\prod_{\mathfrak{p}} A_{\mathfrak{p}}^{\times}$, defined as*

$$\mathbb{J}(A) := \left\{ (a_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} A_{\mathfrak{p}}^{\times} \,|\, a_{\mathfrak{p}} \in \Lambda_{\mathfrak{p}}^{\times} \text{ for all but finitely many } \mathfrak{p} \right\}.$$

Remark 2.4.7. *This definition appears to depend on the choice of order Λ, but it can be shown to be independent of this choice.*

Definition 2.4.8. *The subgroup of* unit idèles of Λ *is defined as*

$$\mathbb{U}(\Lambda) = \prod_{\mathfrak{p}} \Lambda_{\mathfrak{p}}^{\times} = \left\{ (a_{\mathfrak{p}})_{\mathfrak{p}} | a_{\mathfrak{p}} \in \Lambda_{\mathfrak{p}}^{\times} \text{ for all } \mathfrak{p} \right\}.$$

Definition 2.4.9. *A* principal idèle of A *is an idèle of the form $(a)_{\mathfrak{p}}$ where $a \in A^{\times}$. The principal idèles of A form a* subgroup *of $\mathbb{J}(A)$ denoted by $A^{\times}$.*

Theorem 2.4.10. *With the notation established above, we have*

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

Proof. See Theorem 22 in Section 49 of [CR81a]. □

Remark 2.4.11. *Note that in Theorem 2.4.10 since all groups involved are abelian, all the subgroups are normal so the product of subgroups in the denominator is again a subgroup and is normal, so the quotient is well defined.*

In order to describe the class of a locally free Λ-lattice in $\mathrm{Cl}(\Lambda)$, we make an additional assumption. Since X is a Λ-module, $K \otimes_{\mathcal{O}_K} X$ is a module over $K \otimes_{\mathcal{O}_K} \Lambda$ which is equal to A. We assume that $K \otimes_{\mathcal{O}_K} X$ is actually a *free* A-module of rank one.

For example we can take A to be $K[G]$, X to be $\mathcal{O}_L$ and $K \otimes_{\mathcal{O}_K} \mathcal{O}_L = L$ which is a free $K[G]$-module of rank one by the normal basis theorem.

Let x be a free generator of $K \otimes_{\mathcal{O}_K} X$ as an A-module and for each $\mathfrak{p}$ let $x_{\mathfrak{p}}$ be a generator of $X_{\mathfrak{p}}$ as a $\Lambda_{\mathfrak{p}}$-module. Then for each $\mathfrak{p}$, there exists a unique element $a_{\mathfrak{p}} \in A_{\mathfrak{p}}$ such that $a_{\mathfrak{p}} \cdot x = x_{\mathfrak{p}}$.

Proposition 2.4.12. *With the notation established above, the class of X in* $\mathrm{Cl}(\Lambda)$ *corresponds to the class of the idèle $(a_{\mathfrak{p}})_{\mathfrak{p}}$ in the quotient group*

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

Proof. See Theorem 49.22 of [CR81b]. □

Definition 2.4.13. *Let A be a commutative algebra. Then we denote its unique* maximal order *by $\mathcal{M}$.*

Proposition 2.4.14. *The class group of the maximal order is isomorphic to a product of class groups of finite extensions of the field K.*

Proof. Suppose that $A \cong \prod_{i=1}^{r} F_i$, where each F_i is a finite extension of K. Then the unique maximal order in A is $\mathcal{M} \cong \prod_{i=1}^{r} \mathcal{O}_{F_i}$. We have

$$A^\times \cong \prod_{i=1}^{r} F_i^\times,$$

$$\mathbb{J}(A) \cong \prod_{i=1}^{r} \mathbb{J}(F_i)$$

and

$$\mathbb{U}(\mathcal{M}) \cong \prod_{i=1}^{r} \mathbb{U}(\mathcal{O}_{F_i})$$

so

$$\begin{aligned} \mathrm{Cl}(\mathcal{M}) &\cong \frac{\mathbb{J}(A)}{A^\times \mathbb{U}(\mathcal{M})} \\ &\cong \prod_{i=1}^{r} \frac{\mathbb{J}(F_i)}{F_i^\times \mathbb{U}(\mathcal{O}_{F_i})} \\ &\cong \prod_{i=1}^{r} \mathrm{Cl}(F_i) \end{aligned}$$

where $\mathrm{Cl}(F_i)$ denotes the ideal class group of F_i. See also pages 359 and 360 of [Neu13]. □

Corollary 2.4.15. *Applying the isomorphism in the previous proposition, the idèle $(a_\mathfrak{p})_\mathfrak{p}$ gets mapped to $\prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}$. This allows us to obtain a tuple of ideals from an idèle.*

We can often obtain criteria for an $\mathcal{M}$-module to be free in terms of certain ideals of the rings of integers $\mathcal{O}_{F_i}$ being principal. In general the locally free class group of an order Λ in A will not admit a decomposition of this form, but we have the following result of Bley and Johnston.

Theorem 2.4.16. *Let X be a Λ-lattice and let*

$$\mathcal{M}X = \left\{ \sum_{finite} z \cdot x | z \in \mathcal{M}, x \in X \right\} \subset KX.$$

Then X is a free Λ-module of rank one if and only if

- *X is a locally free Λ-module of rank one*
- *$\mathcal{M}X$ is a free $\mathcal{M}$-module with a generator lying in X*

Proof. See Theorem 2.1 of [BJ08]. □

Thus we can obtain criteria for a Λ-module X to be free by first obtaining criteria for X to be a locally free Λ-module and then obtaining criteria for $\mathcal{M}X$ to be a free $\mathcal{M}$-module with a generator lying in X. As noted above, this second task is facilitated by the decomposition of $\mathrm{Cl}(\mathcal{M})$ as a product of ideal class groups.

2.5 An example of Galois module theory - Tamely ramified Kummer extensions of prime power degree

The aim of this section will be to reprove a particular case of the result of Del Corso and Rossi using the result of Bley and Johnston (Theorem 2.4.16). We will focus on certain tame Kummer extensions of prime-power degree. We first recall the result of Del Corso and Rossi. If L/K is a tamely ramified Kummer extension of degree N and exponent m then $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module if and only if there exists a set of integral Kummer generators α_1, ..., α_r for L/K such that the ideals $\mathfrak{b}_{\boldsymbol{j}}$ associated to $\boldsymbol{a}\mathcal{O}_K$ are principal with generators $b_{\boldsymbol{j}}$ such that

$$\sum_{\boldsymbol{j}} \frac{\boldsymbol{\alpha^j}}{b_{\boldsymbol{j}}} \equiv 0 \pmod{N\mathcal{O}_L}.$$

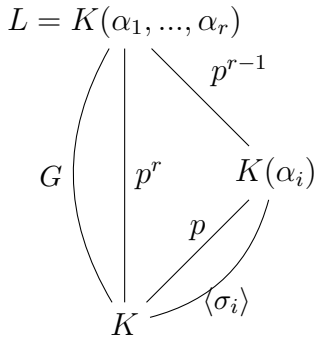
Furthermore, in this case the element

$$\frac{1}{N} \sum_{\boldsymbol{j}} \frac{\boldsymbol{\alpha^j}}{b_{\boldsymbol{j}}}$$

is a free generator of $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module.

2.5.1 Setup

Let p be an odd prime number and let K be a number field containing a primitive p^{th} root of unity ζ. Let L/K be a Galois extension with $G = \mathrm{Gal}(L/K) \cong C_p^r$. By Kummer theory $L = K(\alpha_1, ..., \alpha_r)$ with $\alpha_i^p \in K$ for each i, and $G = \langle \sigma_1, ..., \sigma_r \rangle$ where $\sigma_i(\alpha_i) = \zeta\alpha_i$ and $\sigma_i(\alpha_j) = \alpha_j$ for $i \neq j$. For more details on Kummer theory see [Rom05].



Definition 2.5.1 (Bold notation)**.** *If $i_1, ..., i_r \in \{0, ..., p-1\}$ write $\boldsymbol{i}$ for the vector of exponents $(i_1, ..., i_r) \in \mathbb{Z}^r$. Then the notation $\boldsymbol{\alpha^i}$ denotes $\alpha_1^{i_1}...\alpha_r^{i_r} \in L$ and $\boldsymbol{a^i}$ denotes $a_1^{i_1}...a_r^{i_r} \in K$.*

Remark 2.5.2. *This notation is compatible with componentwise multiplication in $\mathbb{Z}^r$: if $\boldsymbol{i}, \boldsymbol{j} \in \mathbb{Z}^r$ then*

$$(\boldsymbol{\alpha^i})^{\boldsymbol{j}} = (\alpha_1^{i_1}...\alpha_r^{i_r})^{j_1 \cdots j_r} = \boldsymbol{\alpha^{ij}}.$$

We can write sums of the form $\sum_{\boldsymbol{i}} \cdot$ where we again assume $0 \leq i_k \leq p-1$ for each k. We can also use this notation in subscripts e.g. for orthogonal idempotents $e_{\boldsymbol{i}}$.

Remark 2.5.3. *This notation will also be valid when we study extensions of square free degree in Chapters 5 and 6, but in that case the natural ranges for the exponents will be $0 \leq i_k \leq p_k - 1$ for each $1 \leq k \leq r$.*

2.5.2 Properties of the group algebra

Proposition 2.5.4. *We have $K[G] \cong K^{p^r}$ via orthogonal idempotents.*

Proof. First fix $k \in \{1, ..., r\}$ and for each $i = 0, ..., p-1$ define

$$e_{k,i} = \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-ij} \sigma_k^j \in K\langle \sigma_k \rangle.$$

Then the $e_{k,i}$ are a basis of mutually orthogonal idempotents in $K\langle \sigma_k \rangle$ so $K\langle \sigma_k \rangle \cong K^p$. Now given $i_1, ..., i_r \in \{0, ..., p-1\}$ define

$$e_{\boldsymbol{i}} = \prod_{k=1}^{r} e_{k,i_k} = \prod_{k=0}^{p-1} \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-i_k j} \sigma_k^j \in K[G].$$

Then the $e_{\boldsymbol{i}}$ are a basis of mutually orthogonal idempotents in $K[G]$, so $K[G] \cong K^{p^r}$. □

Corollary 2.5.5. *The unique maximal order in $K[G]$ is*

$$\mathcal{M} = \mathcal{O}_K\langle e_{\boldsymbol{i}} \rangle \cong \mathcal{O}_K^{p^r}.$$

Proposition 2.5.6. *The action of the $e_{\boldsymbol{i}}$ on L is given by*

$$e_{\boldsymbol{i}}(\boldsymbol{\alpha^j}) = \begin{cases} \boldsymbol{\alpha^j} & \text{if } \boldsymbol{i} = \boldsymbol{j} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We have

$$\begin{aligned} e_{\boldsymbol{i}}(\boldsymbol{\alpha^j}) &= \prod_{k=0}^{p-1} \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-i_k j} \sigma_k^j(\boldsymbol{\alpha^j}) \\ &= \prod_{k=0}^{p-1} \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{j(i_k - j_k)} \boldsymbol{\alpha^j} \\ &= \delta_{\boldsymbol{i},\boldsymbol{j}} \boldsymbol{\alpha^j}. \end{aligned}$$

□

2.5.3 Ramification

We ensure that the extension is tame in two steps. Firstly we determine conditions for a degree p subextension to be tame and secondly we apply Proposition 2.1.9 to ensure that the full extension is tame.

Lemma 2.5.7. *An extension of the form $K(\alpha)/K$ with $\alpha \notin K$ and $\alpha^p = a \in K$ is tame if and only if a can be chosen to satisfy $a \equiv 1 \pmod{(\zeta-1)^p\mathcal{O}_K}$.*

Proof. Since $\zeta \in K$ and $\alpha \notin K$, the polynomial $x^p - a$ is irreducible over K and is therefore the minimal polynomial of α over K. Hence $K(\alpha)/K$ has degree p. Since $K(\alpha)/K$ is Galois, each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ factorises in $K(\alpha)$ as $(\mathfrak{P}_1...\mathfrak{P}_g)^e$ with $e|p$. Therefore $K(\alpha)/K$ is tame if and only if each prime ideal $\mathfrak{p}$ lying above p is unramified in $K(\alpha)$. By Theorem 119 of [HGK81] this occurs if a can be chosen to satisfy $a \equiv 1 \pmod{\mathfrak{p}^{pv_\mathfrak{p}(\zeta-1)}}$ for each $\mathfrak{p}$ lying above p. By the Chinese remainder theorem, this is equivalent to requiring $a \equiv 1 \pmod{(\zeta-1)^p\mathcal{O}_K}$. □

Lemma 2.5.8. *The extension L/K is tame if and only if all a_i can be chosen to satisfy $a_i \equiv 1 \pmod{(\zeta-1)^p\mathcal{O}_K}$.*

Proof. The field L is the compositum of the fields $K(\alpha_i)$ for each i. Hence applying Proposition 2.1.9, L/K is tame if and only if $K(\alpha_i)/K$ is tame for each i. By the previous lemma this occurs if and only if all a_i can be chosen to satisfy $a_i \equiv 1 \pmod{(\zeta-1)^p\mathcal{O}_K}$. □

Henceforth we will assume that these congruences hold.

2.5.4 Local integral bases for $\mathfrak{p} \nmid p\mathcal{O}_K$

Definition 2.5.9. *For $x \in K^\times$ and $\mathfrak{p}$ a prime of $\mathcal{O}_K$ define $r_\mathfrak{p}(x)$ by*

$$r_\mathfrak{p}(x) = \lfloor \frac{v_\mathfrak{p}(x)}{p} \rfloor.$$

Remark 2.5.10. *This notation will also be valid when we study extensions of square free degree m in Chapters 5 and 6, but in that case the denominator in the above definition will be m.*

Proposition 2.5.11. *Suppose $\mathfrak{p} \nmid p\mathcal{O}_K$. Then an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{K(\alpha),\mathfrak{p}}$ is given by*

$$B = \left\{ \frac{\alpha^i}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^i)}} | i = 0, ..., p-1 \right\}.$$

Proof. By Theorem 118 of [HGK81], $\mathfrak{p}$ is unramified in $K(\alpha)$ if $p|v_{\mathfrak{p}}(a)$ and totally ramified in $K(\alpha)$ if $p \nmid v_{\mathfrak{p}}(a)$. Note that each element of B is integral over $\mathcal{O}_{K,\mathfrak{p}}$ since $(\frac{\alpha^i}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^i)}})^p = \frac{a^i}{\pi_{\mathfrak{p}}^{pr_{\mathfrak{p}}(a^i)}}$ and $pr_{\mathfrak{p}}(a^i) \leq v_{\mathfrak{p}}(a^i)$. First suppose that $p|v_{\mathfrak{p}}(a)$. Then $v_{\mathfrak{p}}(a) = pr_{\mathfrak{p}}(a)$ and $r_{\mathfrak{p}}(a^i) = ir_{\mathfrak{p}}(a)$ for each i. Using the trace formulation of the discriminant we find that

$$\begin{aligned}\mathfrak{d}(B) &= \pi_{\mathfrak{p}}^{-p(p-1)r_{\mathfrak{p}}(a)} \begin{vmatrix} p & 0 & ... & 0 \\ 0 & 0 & ... & ap \\ ... & ... & ... & ... \\ 0 & ap & ... & 0 \end{vmatrix} \\ &= p^p a^{p-1} \pi_{\mathfrak{p}}^{-p(p-1)r_{\mathfrak{p}}(a)} \\ &= p^p\end{aligned}$$

which is a unit of $\mathcal{O}_{K,\mathfrak{p}}$. Therefore B is an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{K(\alpha),\mathfrak{p}}$ in this case. Now suppose that $p \nmid v_{\mathfrak{p}}(a)$. Then $\mathfrak{p}$ is totally ramified in $K(\alpha)$, say $\mathfrak{p}\mathcal{O}_{K(\alpha)} = \mathfrak{P}^p$. We have $v_{\mathfrak{P}}(\alpha^p) = pv_{\mathfrak{P}}(\alpha)$ and also $v_{\mathfrak{P}}(\alpha^p) = v_{\mathfrak{P}}(a) = pv_{\mathfrak{p}}(a)$, so $v_{\mathfrak{P}}(\alpha) = v_{\mathfrak{p}}(a)$. Hence for each $i = 0, ..., p-1$ we have

$$\begin{aligned} v_{\mathfrak{P}}(\frac{\alpha^i}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^i)}}) &= v_{\mathfrak{P}}(\alpha^i) = v_{\mathfrak{P}}(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a^i)}) \\ &= v_{\mathfrak{p}}(a^i) - pr_{\mathfrak{p}}(a^i)\end{aligned}$$

This expression is the principal remainder in the division of $v_{\mathfrak{p}}(a^i)$ by p. Since $p \nmid v_{\mathfrak{p}}(a^i)$ these remainders cover all residues modulo p as i varies. Hence B contains an element of each $\mathfrak{P}$-valuation 0, ..., $p-1$ and so by Theorem 2.2.10 B is an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{K(\alpha),\mathfrak{p}}$. □

Proposition 2.5.12. *Suppose that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ that does not lie above p. Then an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by*

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}} | 0 \leq i_k \leq p-1 \text{ for all } k \right\}.$$

Proof. If $p|v_{\mathfrak{p}}(a_k)$ for all k then $\mathfrak{p}$ is unramified in $K(\alpha_k)$ for each k, so the extensions $K(\alpha_k)/K$ are pairwise arithmetically disjoint. Therefore in this case (applying the

previous proposition and Theorem 2.2.14) an $\mathcal{O}_{K,\mathfrak{p}}$ basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by

$$\left\{ \frac{\alpha_1^{i_1}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_1^{i_1})}} ... \frac{\alpha_r^{i_r}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_r^{i_r})}} | 0 \leq i_k \leq p-1 \text{ for all } k \right\}.$$

Since $r_{\mathfrak{p}}(a_k^{i_k}) = \frac{v_{\mathfrak{p}}(a_k^{i_k})}{p}$ for each k, we see that $r_{\mathfrak{p}}(a_1^{i_1}) + ... + r_{\mathfrak{p}}(a_r^{i_r}) = r_{\mathfrak{p}}(a_1^{i_1}...a_r^{i_r})$ giving the description in the statement of the proposition. If $p \nmid v_{\mathfrak{p}}(a_k)$ for some k then without loss of generality suppose that $p \nmid v_{\mathfrak{p}}(a_1)$. For each $k = 2, ..., r$ choose $n_k \in \{0, ..., p-1\}$ such that $v_{\mathfrak{p}}(a_1^{n_k} a_k) \equiv 0 \pmod{p}$. Then L is the compositum of the fields $K(\alpha_1)$, $K(\alpha_1^{n_2}\alpha_2)$, ..., $K(\alpha_1^{n_r}\alpha_r)$ and these are pairwise arithmetically disjoint as extensions of K. By the first part of the proof an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by

$$\begin{aligned}
&\left\{ \frac{\alpha_1^{i_1}(\alpha_1^{n_2}\alpha_2)^{i_2}...(\alpha_1^{n_r}\alpha_r)^{i_r}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_1^{i_1}(a_1^{n_2}a_2)^{i_2}...(a_1^{n_r}a_r)^{i_r})}} | 0 \leq i_k \leq p-1 \text{ for all } k \right\} \\
=&\left\{ \frac{\alpha_1^{i_1+n_2i_2+...+n_ri_r}\alpha_2^{i_2}...\alpha_r^{i_r}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_1^{i_1+n_2i_2+...+n_ri_r}a_2^{i_2}...a_r^{i_r})}} | 0 \leq i_k \leq p-1 \text{ for all } k \right\} \\
=&\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}} | 0 \leq i_k \leq p-1 \text{ for all } k \right\}
\end{aligned}$$

To explain the last equality above in more detail, we first note that since $v_{\mathfrak{p}}(a_1)$ is the only term which is not congruent to 0 modulo p, we do not get a "carry" in the floor function and we can combine the exponents of $\pi_{\mathfrak{p}}$ as expected. Now we must be able to reach a typical element,

$$\left\{ \frac{\alpha_1^{s_1}...\alpha_r^{s_r}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_1^{s_1}...a_r^{s_r})}} | 0 \leq i_k \leq p-1 \text{ for all } 1 \leq k \leq r \right\}$$

We can do this by first choosing each i_k to be the unique element in $\{0, ..., p-1\}$ such that $n_k i_k \equiv s_k \pmod{p}$ for $2 \leq k \leq r$ and finally choosing i_1 to be the unique element in $\{0, ..., p-1\}$ such that $\sum_{k=1}^{r} i_k \equiv s_1 \pmod{p}$. By doing this, we extract a unit power of each a_i but since these are in K already, this does not affect the extension. We can relabel the indices to rewrite the integral basis in terms of the

original elements and get a basis of the following form.

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{\alpha^i})}} | 0 \leq i_k \leq p-1 \text{ for all } 1 \leq k \leq r \right\}$$

This completes the proof. □

2.5.5 Local integral bases for $\mathfrak{p}|p\mathcal{O}_K$

Proposition 2.5.13. *Suppose that $\mathfrak{p}|p\mathcal{O}_K$. Then an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{K(\alpha),\mathfrak{p}}$ is given by*

$$B = \left\{ \left(\frac{\alpha - 1}{\zeta - 1} \right)^i | i = 0, ..., p-1 \right\}.$$

Proof. First note that $\mathfrak{p}$ is unramified in $K(\alpha)$ since $K(\alpha)/K$ is tamely ramified. Next we show that $\frac{\alpha-1}{\zeta-1}$ is integral. If $x = \frac{\alpha-1}{\zeta-1}$ then

$$\begin{aligned}
&(\zeta-1)x + 1 = \alpha \\
\Rightarrow &((\zeta-1)x+1)^p = a \\
\Rightarrow &\sum_{j=0}^{p-1} \binom{p}{j} (\zeta-1)^j x^j = a \\
\Rightarrow &\sum_{j=1}^{p-1} \binom{p}{j} (\zeta-1)^j x^j + (1-a) = 0 \\
\Rightarrow &\sum_{j=1}^{p-1} \binom{p}{j} (\zeta-1)^{j-p} x^j + \frac{1-a}{(\zeta-1)^p} = 0
\end{aligned}$$

Since $a \equiv 1 \pmod{(\zeta-1)^p}$, this is a monic polynomial in x with coeffcients in $\mathcal{O}_{K,\mathfrak{p}}$. Therefore x is integral and it follows that the elements of B are integral. We have $\mathfrak{d}(B) = (\prod_{i=0}^{p-1}(\zeta-1)^{-i})^2 \mathfrak{d}(B')$ where $B' = \{(\alpha-1)^i | i = 0, ..., p-1\}$ and $\mathfrak{d}(B') = \mathfrak{d}(1, \alpha, ..., \alpha^{p-1}) = (-1)^{\frac{p-1}{2}} p^p a^{p-1}$. Hence up to units of $\mathcal{O}_{K,\mathfrak{p}}$ we have $\mathfrak{d}(B) = (\zeta-1)^{-2\sum_{i=0}^{p-1} i} p^p = (\zeta-1)^{p(p-1)} p^p$ and since $(\zeta-1)^p$ and p differ by a unit of $\mathcal{O}_{K,\mathfrak{p}}$ this discriminant is trivial. Therefore B is an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{K(\alpha),\mathfrak{p}}$. □

Proposition 2.5.14. *Suppose that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ that lies above p. Then an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by*

$$\left\{ \prod_{k=1}^{r} \left(\frac{\alpha_k - 1}{\zeta - 1} \right)^{i_k} | 0 \leq i_k \leq p-1 \text{ for all } k \right\}.$$

Proof. In this case $\mathfrak{p}$ is unramified in $K(\alpha_k)/K$ for each k, so these extensions are pairwise arithmetically disjoint at $\mathfrak{p}$. The result now follows from the previous proposition and Theorem 2.2.14. □

2.5.6 Local generators

By Noether's theorem, $\mathcal{O}_L$ is a locally free $\mathcal{O}_K[G]$-module. We seek explicit generators of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{O}_{K,\mathfrak{p}}G$ for each $\mathfrak{p}$.

Proposition 2.5.15. *Suppose that $\mathfrak{p} \nmid p\mathcal{O}_K$. Then a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{O}_{K,\mathfrak{p}}G$-module is*

$$x_{\mathfrak{p}} = \frac{1}{p^r} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}}.$$

Proof. In this case we have $p \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$, so each idempotent $e_{\boldsymbol{i}}$ lies in $\mathcal{O}_{K,\mathfrak{p}}G$, so $\mathcal{O}_{K,\mathfrak{p}}G = \mathcal{M}_{\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}\langle e_{\boldsymbol{i}} \rangle$. For each $\boldsymbol{i}$ we have

$$e_{\boldsymbol{i}} \cdot x_{\mathfrak{p}} = \frac{1}{p^r} \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}}$$

so the set $\{e_{\boldsymbol{i}} \cdot x_{\mathfrak{p}} | 0 \leq i_k \leq p-1 \text{ for all } k\}$ forms an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ (note that $p^r \in \mathcal{O}_{K,\mathfrak{p}}$ and compare wth the basis from Proposition 2.5.12). Hence $x_{\mathfrak{p}}$ is a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{O}_{K,\mathfrak{p}}$-module. □

Proposition 2.5.16. *Suppose that $\mathfrak{p} | p\mathcal{O}_K$. Then a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{O}_{K,\mathfrak{p}}G$-module is*

$$x_{\mathfrak{p}} = \frac{1}{p^r} \prod_{k=1}^{r} (1 + \alpha_k + ... + \alpha_k^{p-1}).$$

We will discuss some preliminary p-group theory before proving this proposition. We note that the theory we will now discuss only requires the assumption that G is a p-group. For prime ideals $\mathfrak{p} | p\mathcal{O}_K$, the orthogonal idempotents are not available ($\frac{1}{p} \notin \mathcal{O}_{K,\mathfrak{p}}^{\times}$ so $e_{\boldsymbol{i}} \notin \mathcal{O}_{K,\mathfrak{p}}[G]$), so the argument we used to prove the previous proposition

cannot be applied. Since the Galois group of this extension is a p-group, this gives the group ring $\mathcal{O}_{K,\mathfrak{p}}G$ some special properties which can be used as an alternative method to obtain a local generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{O}_{K,\mathfrak{p}}$-module. Since $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_{K,\mathfrak{p}}$, the quotient $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}$ is a finite field of characteristic p. In fact $\mathfrak{p}$ is the *unique* maximal ideal of $\mathcal{O}_{K,\mathfrak{p}}$ so $\mathcal{O}_{K,\mathfrak{p}}$ is a *local ring*. This allows us to use *Nakayama's Lemma*.

Lemma 2.5.17 (Nakayama's Lemma)**.** *If M is a finitely generated $\mathcal{O}_{K,\mathfrak{p}}$-module and m_1, ..., m_k generate $M/\pi M$ (where π is a uniformiser) as an $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}$-module, then they generate M over $\mathcal{O}_{K,\mathfrak{p}}$.*

Proof. See Lemma 4.3 on page 425 of [Lan04]. □

Here $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}$ is a field, so $M/\pi M$ is a vector space. In our case, $M = \mathcal{O}_{L,\mathfrak{p}}$ and $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}\langle x_1, ..., x_n\rangle$ for some $\mathcal{O}_{K,\mathfrak{p}}$ basis $x_1, ..., x_n$.

$$M = \{\sum_{i=1}^{n} c_i x_i | c_i \in \mathcal{O}_{K,\mathfrak{p}}\}$$

and

$$\pi M = \{\sum_{i=1}^{n} c_i x_i | c_i \in \mathfrak{p} = \pi\mathcal{O}_{K,\mathfrak{p}}\}$$

so

$$M/\pi M = \{\sum_{i=1}^{n} c_i x_i | c_i \in \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\}.$$

Hence an integral basis of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{O}_{K,\mathfrak{p}}$ becomes a basis of $\mathcal{O}_{L,\mathfrak{p}}/\pi\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}$ which is a field. Similarly, $\mathcal{O}_{K,\mathfrak{p}}[G]/\pi\mathcal{O}_{K,\mathfrak{p}}[G]$ is the set

$$\mathcal{O}_{K,\mathfrak{p}}[G]/\pi\mathcal{O}_{K,\mathfrak{p}}[G] = \{\sum_{i=1}^{n} c_i\sigma_i | c_i \in \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\} = \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}[G] = k_{\mathfrak{p}}[G]$$

and since $k_{\mathfrak{p}}$ is a field, this set $(\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p})[G]$ is a *group algebra*. For this particular extension, $k_{\mathfrak{p}}[G]$ is a group algebra of a group of order p^r over a field of characteristic p. This gives the group algebra some nice properties, one of which is the following.

Proposition 2.5.18. *The group algebra $k_{\mathfrak{p}}[G]$ has a unique minimal (left) ideal, generated by $\theta = \sum_{i=1}^{n} \sigma_i$.*

Proof. See Proposition 6 on page 3816 of [Tho08]. □

Another property of the group algebra is the following, taken from Proposition 5.1 on page 7 of [Joh15].

Proposition 2.5.19. *If $x \in \mathcal{O}_{L,\mathfrak{p}}/\pi\mathcal{O}_{L,\mathfrak{p}}$ is such that $\theta \cdot x \neq 0$ in $k_{\mathfrak{p}}$ (i.e. $\theta \cdot x \notin \pi\mathcal{O}_{K,\mathfrak{p}}$) i.e. $Tr(x) \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$, then x is a free generator of $\mathcal{O}_{L,\mathfrak{p}}/\pi\mathcal{O}_{L,\mathfrak{p}}$ as a $k_{\mathfrak{p}}[G]$-module. And hence by Nakayama's lemma x is a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{O}_{K,\mathfrak{p}}[G]$.*

Proof. We are looking for $x \in \mathcal{O}_{L,\mathfrak{p}}/\pi\mathcal{O}_{L,\mathfrak{p}}$ such that $\mathcal{O}_{L,\mathfrak{p}}/\pi\mathcal{O}_{L,\mathfrak{p}} = k_{\mathfrak{p}}[G] \cdot x$. Given x, we get a linear map $f : k_{\mathfrak{p}}[G] \cdot x \to \mathcal{O}_{L,\mathfrak{p}}/\pi\mathcal{O}_{L,\mathfrak{p}}$ given by $f(z) = z \cdot x$. We want to choose x such that f is bijective. Since the domain and codomain are vector spaces of the same dimension, f is bijective if and only if it is injective if and only if $\ker(f) = \{0\}$. In addition, note that $\ker(f)$ is a (left) ideal since if $f(z) = 0$ and $y \in k_{\mathfrak{p}}[G]$, then $f(yz) = yz \cdot x = y \cdot (z \cdot x) = 0$. So $\ker(f) \neq \{0\}$ if and only if $\theta \in \ker(f)$ if and only if $\theta \cdot x = 0$ in $k_{\mathfrak{p}}$. Therefore if we choose $x \in \mathcal{O}_{L,\mathfrak{p}}$ such that $\theta \cdot x \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$ then $\theta \cdot x \neq 0$ in $k_{\mathfrak{p}}$ and so x is a free generator of $\mathcal{O}_{L,\mathfrak{p}}/\pi\mathcal{O}_{L,\mathfrak{p}}$ as a $k_{\mathfrak{p}}[G]$-module. □

We will now complete the proof of Proposition 2.5.16 by calculating the trace of the element $x_{\mathfrak{p}}$ and showing that $x_{\mathfrak{p}} \in \mathcal{O}_{L,\mathfrak{p}}$.

Proof of Proposition 2.5.16. Proposition 2.5.14 implies that $\frac{(\alpha_k - 1)^{p-1}}{p} \in \mathcal{O}_{L,\mathfrak{p}}$ for each k. Using the fact that $\binom{p-1}{n} \equiv (-1)^n \pmod{p}$, we have $\frac{1}{p}(1 + \alpha_k + ... + \alpha_k^{p-1}) \in \mathcal{O}_{L,\mathfrak{p}}$ for each k, hence their product is in $\mathcal{O}_{L,\mathfrak{p}}$ and $x_{\mathfrak{p}} \in \mathcal{O}_{L,\mathfrak{p}}$.

Now note that the trace of $\boldsymbol{\alpha^j}$ is zero unless $\boldsymbol{j} = \mathbf{0}$ in which case it is p^r. This implies that $x_{\mathfrak{p}}$ has trace 1 and then the result follows from Proposition 2.5.19. □

2.5.7 Using idèlic theory to move from local to global freeness

Having obtained a complete set of local information in the previous section, in this section, we apply Theorem 2.4.16 to determine criteria for global freeness.

Proposition 2.5.20. *The class of $\mathcal{M}\mathcal{O}_L$ in $\mathrm{Cl}(\mathcal{M})$ corresponds to the class of the idèle $(z_\mathfrak{p})_\mathfrak{p}$ where*

$$z_\mathfrak{p} = \sum_{\boldsymbol{i}} \frac{e_{\boldsymbol{i}}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}}.$$

Proof. Let $x = \frac{1}{p^r}\prod_{k=1}^{r}(1+\alpha_k+...+\alpha_k^{p-1}) \in \mathcal{O}_L$. Then x generates L as a free $K[G]$-module. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$, let $x_\mathfrak{p}$ be the free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{O}_{K,\mathfrak{p}}$-module found in Propositions 2.5.15 and 2.5.16. That is

$$x_\mathfrak{p} = \begin{cases} \frac{1}{p^r}\prod_{k=1}^{r}(1+\alpha_k+...+\alpha_k^{p-1}) & \text{if } \mathfrak{p}|p\mathcal{O}_K \\ \frac{1}{p^r}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}} & \text{otherwise} \end{cases}$$

For each $\mathfrak{p}$, the element $z_\mathfrak{p} \in K_\mathfrak{p}G$ is defined by $z_\mathfrak{p} \cdot x = x_\mathfrak{p}$. It is now straightforward to see that

$$z_\mathfrak{p} = \sum_{\boldsymbol{i}} \frac{e_{\boldsymbol{i}}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}},$$

which gives the idèle $(z_\mathfrak{p})_\mathfrak{p}$ in the statement of the proposition. □

Now we use the isomorphism from Proposition 2.4.14

$$\frac{\mathbb{J}(K[G])}{K[G]^\times \mathbb{U}(\mathcal{M})} \cong \mathrm{Cl}(K)^m$$

to interpret the class of $(z_\mathfrak{p})_\mathfrak{p}$ as a p^r-tuple of classes of fractional ideals of K.

Proposition 2.5.21. *The idèle $(z_\mathfrak{p})_\mathfrak{p}$ corresponding to the class of $\mathcal{M}\mathcal{O}_L$ in $\mathrm{Cl}(\mathcal{M})$ corresponds to the p^r-tuple of classes of fractional ideals $\mathfrak{a}_{\boldsymbol{i}}^{-1}$, where*

$$\mathfrak{a}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}.$$

Proof. Recall from Proposition 2.4.14 and Corollary 2.4.15 that to obtain the tuple of ideal classes corresponding to an idèle $(z_\mathfrak{p})_\mathfrak{p}$ we write $z_\mathfrak{p} = \sum_{\boldsymbol{i}} c_{\boldsymbol{i},\mathfrak{p}} e_{\boldsymbol{i}}$ with $c_{\boldsymbol{i},\mathfrak{p}} \in K_\mathfrak{p}$ for all $\boldsymbol{i}$. Then the idèle $(z_\mathfrak{p})_\mathfrak{p}$ is mapped to the p^r-tuple of classes of fractional ideals $(\mathfrak{c}_{\boldsymbol{i}})$, where

$$\mathfrak{c}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(c_{\boldsymbol{i},\mathfrak{p}})}.$$

Applying this to the idèle $(z_{\mathfrak{p}})_{\mathfrak{p}}$ corresponding to the class of $\mathcal{M}\mathcal{O}_L$ in $\mathrm{Cl}(\mathcal{M})$ (constructed in the previous proposition) we see that

$$c_{\boldsymbol{i},\mathfrak{p}} = \frac{1}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}}$$

for all $\boldsymbol{i}$ and $\mathfrak{p}$. Hence $(z_{\mathfrak{p}})_{\mathfrak{p}}$ corresponds to the p^r-tuple of ideal classes $(\mathfrak{a}_{\boldsymbol{i}}^{-1})$ where

$$\mathfrak{a}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}$$

for all $\boldsymbol{i}$. □

Definition 2.5.22. *The ideals $\mathfrak{a}_{\boldsymbol{i}}$ are called the ideals* associated to $\boldsymbol{a}\mathcal{O}_K$.

Corollary 2.5.23. *The $\mathcal{M}$-module $\mathcal{M}\mathcal{O}_L$ is free if and only if the ideals associated to $\boldsymbol{a}\mathcal{O}_K$ are principal for all $\boldsymbol{i}$.*

Proposition 2.5.24. *The $\mathcal{M}$-module $\mathcal{M}\mathcal{O}_L$ has a free generator lying in $\mathcal{O}_L$ if and only if the ideals $\mathfrak{b}_{\boldsymbol{i}}$ are principal with generators $b_{\boldsymbol{i}}$ such that*

$$\frac{1}{p^r}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{b_{\boldsymbol{i}}} \in \mathcal{O}_L.$$

Proof. By the previous proposition $\mathcal{M}\mathcal{O}_L$ is a free $\mathcal{M}$-module if and only if each ideal $\mathfrak{b}_{\boldsymbol{i}}$ is principal. Suppose that this is the case and write $\mathfrak{b}_{\boldsymbol{i}} = c_{\boldsymbol{i}}\mathcal{O}_K$ for some $c_{\boldsymbol{i}} \in \mathcal{O}_K$. Then a free generator for $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module is

$$y = \frac{1}{p^r}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{c_{\boldsymbol{i}}}.$$

The set of free generators of $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module is precisely the set $\{z \cdot y | z \in \mathcal{M}^{\times}\}$. Since $\mathcal{M} \cong \mathcal{O}_K^{p^r}$ via orthogonal idempotents and $e_{\boldsymbol{i}} \cdot \boldsymbol{\alpha}^{\boldsymbol{j}} = \delta_{\boldsymbol{i},\boldsymbol{j}}\boldsymbol{\alpha}^{\boldsymbol{j}}$, we see that an element $y' \in L$ is a free generator for $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module if and only if it has the form

$$y' = \frac{1}{p^r}\sum_{\boldsymbol{i}} \frac{u_{\boldsymbol{i}}\boldsymbol{\alpha}^{\boldsymbol{i}}}{c_{\boldsymbol{i}}}$$

for some $u_{\boldsymbol{i}} \in \mathcal{O}_K^{\times}$. Therefore $\mathcal{M}\mathcal{O}_L$ has a free generator lying in $\mathcal{O}_L$ if and only if there exist elements $u_{\boldsymbol{i}} \in \mathcal{O}_K^{\times}$ such that the corresponding element y' lies in $\mathcal{O}_L$. Writing $b_{\boldsymbol{i}} = u_{\boldsymbol{i}}^{-1}c_{\boldsymbol{i}}$ for each $\boldsymbol{i}$ this is equivalent to the existence of elements $b_{\boldsymbol{i}}$ as in the statement of the proposition. □

By combining the results of this section, we obtain a criterion for $\mathcal{O}_L$ to be a free $\mathcal{O}_K[G]$-module.

Theorem 2.5.25. *Let p be an odd prime number and let K be a number field containing a primitive p^{th} root of unity ζ. Let L/K be a Galois extension with $G = \mathrm{Gal}(L/K) \cong C_p^r$. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the rings of algebraic integers of K and L respectively. Then $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module if and only if there exist $\beta_1, ..., \beta_r \in \mathcal{O}_L$ such that*

1. *$L = K(\beta_1, ..., \beta_r)$*
2. *$b_i = \beta_i^p \in \mathcal{O}_K$ for each i*
3. *The ideals $\mathfrak{b}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\boldsymbol{b^i})}$ are principal with generators $c_{\boldsymbol{i}}$ such that $y = \frac{1}{p^r} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\beta^i}}{c_{\boldsymbol{i}}} \in \mathcal{O}_L$.*

Furthermore in this case the element y is a free generator of $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module.

Proof. If $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module then by Theorem 2.4.16 we have $\mathcal{M}\mathcal{O}_L = \mathcal{M} \cdot x$ for some $x \in \mathcal{O}_L$. Therefore by the previous proposition the ideals $\prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}$ are principal for all $\boldsymbol{i}$ with generators $b_{\boldsymbol{i}}$ satisfying

$$\frac{1}{p^r} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha^i}}{b_{\boldsymbol{i}}} \in \mathcal{O}_L.$$

Therefore the elements $\beta_i = \alpha_i$ for each i satisfy *1.*, *2.* and *3.* Conversely suppose that for each $1 \leq i \leq r$ the elements β_i satisfy *1.*, *2.* and *3.* Then we can write $\boldsymbol{\beta} = \boldsymbol{\alpha^l c}$ for some $\boldsymbol{l} \in \mathbb{Z}^r$ with $p \nmid l_i$ for each i and some $\boldsymbol{c} \in (K^\times)^r$. Define $\boldsymbol{t} \in \mathbb{Z}^r$ by $t_i l_i \equiv 1 \pmod{p}$ for each i. Then for each $\boldsymbol{j} \in \mathbb{Z}^r$ we have

$$\begin{aligned} \boldsymbol{a^l} &= \boldsymbol{c^{-p} b} \\ \Rightarrow \boldsymbol{a^{lt}} &= \boldsymbol{c^{-pt} b^t} \\ \Rightarrow \boldsymbol{a^{jlt}} &= \boldsymbol{c^{-pjt} b^{jt}} \end{aligned}$$

Now given $\boldsymbol{n} \in \mathbb{Z}^r$ let $\overline{\boldsymbol{n}}$ denote the least positive residues of the elements of $\boldsymbol{n}$ modulo p, so that

$$\boldsymbol{n} = p\lfloor \frac{\boldsymbol{n}}{p} \rfloor + \overline{\boldsymbol{n}}.$$

Then we have

$$\begin{aligned}
\boldsymbol{a}^{\boldsymbol{jlt}} &= \boldsymbol{c}^{-p\boldsymbol{jt}}\boldsymbol{b}^{\boldsymbol{jt}} \\
\Rightarrow \boldsymbol{a}^{\boldsymbol{j}}\boldsymbol{a}^{p\lfloor \frac{\boldsymbol{jlt}}{p} \rfloor} &= \boldsymbol{c}^{-p^2\lfloor \frac{\boldsymbol{jt}}{p} \rfloor}\boldsymbol{c}^{-p\overline{\boldsymbol{jt}}}\boldsymbol{b}^{p\lfloor \frac{\boldsymbol{jt}}{p} \rfloor}\boldsymbol{b}^{\overline{\boldsymbol{jt}}} \\
\Rightarrow \boldsymbol{a}^{\boldsymbol{j}}\boldsymbol{a}^{p\boldsymbol{l}\lfloor \frac{\boldsymbol{jt}}{p} \rfloor}\boldsymbol{a}^{p\lfloor \frac{\boldsymbol{l}\overline{\boldsymbol{jt}}}{p} \rfloor} &= \boldsymbol{c}^{-p^2\lfloor \frac{\boldsymbol{jt}}{p} \rfloor}\boldsymbol{c}^{-p\overline{\boldsymbol{jt}}}\boldsymbol{b}^{p\lfloor \frac{\boldsymbol{jt}}{p} \rfloor}\boldsymbol{b}^{\overline{\boldsymbol{jt}}} \\
\Rightarrow \boldsymbol{a}^{\boldsymbol{j}} &= \boldsymbol{c}^{-p^2\lfloor \frac{\boldsymbol{jt}}{p} \rfloor}\boldsymbol{b}^{p\lfloor \frac{\boldsymbol{jt}}{p} \rfloor}\boldsymbol{a}^{-p\boldsymbol{l}\lfloor \frac{\boldsymbol{jt}}{p} \rfloor}\boldsymbol{b}^{\overline{\boldsymbol{jt}}}\boldsymbol{c}^{-p\overline{\boldsymbol{jt}}}\boldsymbol{a}^{-p\lfloor \frac{\boldsymbol{l}\overline{\boldsymbol{jt}}}{p} \rfloor} \\
\Rightarrow \boldsymbol{a}^{\boldsymbol{j}} &= \boldsymbol{b}^{\overline{\boldsymbol{jt}}}\boldsymbol{c}^{-p\overline{\boldsymbol{jt}}}\boldsymbol{a}^{-p\lfloor \frac{\boldsymbol{l}\overline{\boldsymbol{jt}}}{p} \rfloor}
\end{aligned}$$

By our hypotheses the ideals $\mathfrak{b}_{\boldsymbol{i}}$ associated to $\boldsymbol{b}\mathcal{O}_K$ are principal with generators $x_{\boldsymbol{i}}$ say. From the above, we see that the ideals $\mathfrak{a}_{\boldsymbol{j}}$ associated to $\boldsymbol{a}\mathcal{O}_K$ are principal with generators

$$y_{\boldsymbol{j}} = x_{\overline{\boldsymbol{jt}}}\boldsymbol{c}^{-\overline{\boldsymbol{jt}}}\boldsymbol{a}^{-\lfloor \frac{\boldsymbol{l}\overline{\boldsymbol{jt}}}{p} \rfloor}.$$

Moreover, there is an equality of sets

$$\left\{ \frac{\boldsymbol{\alpha}^{\boldsymbol{j}}}{y_{\boldsymbol{j}}} \right\} = \left\{ \frac{\boldsymbol{\beta}^{\boldsymbol{i}}}{x_{\boldsymbol{i}}} \right\},$$

so

$$\frac{1}{p^r}\sum_{\boldsymbol{j}} \frac{\boldsymbol{\alpha}^{\boldsymbol{j}}}{y_{\boldsymbol{j}}} = \frac{1}{p^r}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\beta}^{\boldsymbol{i}}}{x_{\boldsymbol{i}}} \in \mathcal{O}_L$$

and so $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module. □

Note that as expected, the criterion that we obtained for $\mathcal{O}_L$ to be a free $\mathcal{O}_K[G]$-module is identical to that obtained by Del Corso and Rossi in Theorem 11 of [DCR13].

2.6 Hopf algebras and Hopf-Galois structures

This section will introduce Hopf algebras which are the appropriate objects to use to generalise classical Galois theory.

Definition 2.6.1. *Let R be a commutative ring with unity. An R-*coagebra *is an R-module A with a comultiplication map $\Delta : A \to A \otimes A$ which is coassociative i.e. the following diagram commutes.*

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

and a counit map $\epsilon : A \to R$ which is counitary i.e. the following diagrams commute.

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ & \nwarrow^{\text{scalar multiplication}} & \downarrow{\scriptstyle 1\otimes\epsilon} \\ & & A \otimes R \end{array}$$

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ & \nwarrow^{\text{scalar multiplication}} & \downarrow{\scriptstyle \epsilon\otimes 1} \\ & & R \otimes A \end{array}$$

Definition 2.6.2. *An R-module A is an R-*bialgebra *if it is both an R-algebra and an R-coalgebra and the multiplication and comultiplication maps satisfy the compatibility condition given by the following commutative diagram.*

$$\begin{array}{ccccc} A \otimes A & \xrightarrow{\mu} & A & \xrightarrow{\Delta} & A \otimes A \\ {\scriptstyle\Delta\otimes\Delta}\downarrow & & & & \uparrow{\scriptstyle\mu\otimes\mu} \\ A \otimes A \otimes A \otimes A & & \xrightarrow{1\otimes\tau\otimes 1} & & A \otimes A \otimes A \otimes A \end{array}$$

where τ is the switch map defined by $\tau(x \otimes y) = y \otimes x$ for all x, $y \in A$.

Definition 2.6.3. *An R-*Hopf algebra, *H, is an R-bialgebra with an R-module homomorphism $s : H \to H$ called the antipode map which is both an R-algebra and an R-coalgebra antihomomorphism and also satisfies the antipode property*

$$\mu(1 \otimes s)\Delta = \mu(s \otimes 1)\Delta = \iota\epsilon.$$

Definition 2.6.4. Sweedler notation *is a shorthand for representing the comultiplication of an element $h \in H$ as a sum of simple tensors. It is written as*

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

Example 2.6.5. *Let R be a commutative ring with unity and let G be a finite group. The group ring RG is an example of a Hopf algebra. For $\sigma \in G$ the maps are defined as $\Delta(\sigma) = \sigma \otimes \sigma$, $\epsilon(\sigma) = 1$ and $s(\sigma) = \sigma^{-1}$.*

Definition 2.6.6. *Let R be a commutative ring with unity. Let H be an R-Hopf algebra and let S be an R-algebra such that*

1. *S is an H-module*
2. *$h \cdot 1 = \epsilon(h)$ for all $h \in H$*
3. *$h \cdot (st) = \sum_{(h)} (h_{(1)} \cdot s)(h_{(2)} \cdot t)$ for all s, $t \in L$*

*then S is an H-*module algebra*.*

Definition 2.6.7. *Let L/K be a finite extension of fields and let H be a finite cocommutative K-Hopf algebra. L is an H-*Galois extension *of K, or alternatively H gives a* Hopf-Galois structure *on the extension L/K, if L is an H-module algebra and the K-linear map*

$$j : L \otimes H \to End_K(L)$$

defined by

$$j(s \otimes h)(t) = s(h \cdot t)$$

for $h \in H$, s, $t \in L$ is bijective.

Remark 2.6.8. *The previous concept can be defined for extensions of commutative rings however in this thesis we shall only be concerned will applying it to finite extensions of fields. Also in the previous concept, it is implicit that K is viewed as a trivial H-module i.e. the action of H on K is via the counit map ϵ.*

All the field extensions that we will consider in this thesis will be finite and separable. The Hopf-Galois structures on such an extension are classified by a theorem of Greither and Pareigis. Before we can state the theorem we fix some notation. Assume that L/K is a finite separable extension of fields with Galois closure E. Let $G = \mathrm{Gal}(E/K)$, let $G' = \mathrm{Gal}(E/L)$.

Definition 2.6.9. *We define X to be the* left coset space of G' in G, G/G'. *Explicity* $X = \{xG' | x \in G\}$.

We write $\overline{x}$ for the coset xG' and $\mathrm{Perm}(X)$ for the group of permutations on the set X.

Definition 2.6.10. *The* left translation map $\lambda : G \to \mathrm{Perm}(X)$ *is defined by* $\lambda(g)(\overline{x}) = \overline{gx}$ *for* $g \in G$ *and* $\overline{x} \in \mathrm{Perm}(X)$.

Definition 2.6.11. *A subgroup* $N \leq \mathrm{Perm}(X)$ *is called a* regular subgroup *if it satisfies any two of the following three properties.*

1. *N has the same order as X.*
2. *N acts transitively on X (i.e. for all $\overline{x}$ and $\overline{y} \in X$, there exists $\eta \in N$ such that $\eta\overline{x} = \overline{y}$).*
3. *For all cosets $\overline{x} \in X$, $\mathrm{Stab}_N(\overline{x}) = \{1\}$.*

Lemma 2.6.12. *Any two of the above conditions imply the third.*

Proof. The proof of this lemma consists of applications of the Orbit-Stabiliser theorem.

Firstly, suppose that $|N| = |X|$ and that N acts transitively on X. Now assume that there is $\overline{x} \in X$ with $\mathrm{Stab}_N(\overline{x}) \neq \{1\}$. Since by definition we always have $1 \in \mathrm{Stab}_N(\overline{x})$, we must have $|\mathrm{Stab}_N(\overline{x})| > 1$. Since $|N| = |X|$ and the group action is well defined, there is now some $\overline{y} \notin \mathrm{Orb}_N(\overline{x})$. This contradicts N acting transitively on X hence our assumption that there is $\overline{x} \in X$ with $\mathrm{Stab}_N(\overline{x}) \neq \{1\}$ is false and that $\mathrm{Stab}_N(\overline{x}) = \{1\}$ for all $\overline{x} \in X$.

Secondly, suppose that $|N| = |X|$ and that $\mathrm{Stab}_N(\overline{x}) = \{1\}$ for all $\overline{x} \in X$. Now assume that N does not act transitively on X. Then there are $\overline{x}$, $\overline{y} \in X$ such that $\overline{y} \notin \mathrm{Orb}_N(\overline{x})$. Since $|N| = |X|$, there is an element $\overline{z} \neq \overline{x} \in X$ and distinct η, $\nu \in N$ such that $\overline{z} = \eta\overline{x} = \nu\overline{x}$. Then $\eta^{-1}\nu = \nu^{-1}\eta = 1 \in N$, so $\eta = \nu$ which contradicts η and ν being distinct hence our assumption is false and N acts transitively on X.

Thirdly, suppose that N acts transitively on X and that $\mathrm{Stab}_N(\overline{x}) = \{1\}$ for all $\overline{x} \in X$. Choose $\overline{x} \in X$. Since N acts transitively on X, $\mathrm{Orb}_N(\overline{x}) = X$ and we have $|\mathrm{Orb}_N(\overline{x})| = |X|$. Since $\mathrm{Stab}_N(\overline{x}) = \{1\}$ we have $|\mathrm{Stab}_N(\overline{x})| = 1$. Now if we multiply these together as numbers, we get $|\mathrm{Orb}_N(\overline{x})||\mathrm{Stab}_N(\overline{x}) = |X|$, also the Orbit-Stabiliser theorem tells us that $|\mathrm{Orb}_N(\overline{x})||\mathrm{Stab}_N(\overline{x}) = |N|$, hence we must have $|N| = |X|$. □

Definition 2.6.13. *A subgroup N of* $\mathrm{Perm}(X)$ *is* normalised *by $\lambda(G)$ if $\lambda(g)\eta\lambda(g^{-1}) \in N$ for all $g \in G$, $\eta \in N$.*

Theorem 2.6.14 (Greither-Pareigis Theorem)**.** *There is a bijection between the Hopf-Galois structures on L/K and regular subgroups of* $\mathrm{Perm}(X)$ *that are normalised by $\lambda(G)$.*

Proof. See Theorem 6.8 on page 52 of [Chi00]. □

To obtain the Hopf-Galois structure from the subgroup of $\mathrm{Perm}(X)$ we perform Galois descent on the group algebra $E[N]$. Let G act on $E[N]$ by acting on E as Galois automorphisms and acting on N by the the conjugation action ${}^g\eta = \lambda(g)\eta\lambda(g)^{-1}$. Explicitly, the action of G on $E[N]$ is given by

$$^g(\sum_{\eta\in N} c_\eta\eta) = \sum_{\eta\in N} g(c_\eta)\,{}^g\eta = \sum_{\eta\in N} g(c_\eta)\lambda(g)\eta\lambda(g)^{-1},$$

where $c_\eta \in E$. This gives a semi-linear action of G on the E-Hopf algebra $E[N]$ and by Galois descent, the fixed ring $E[N]^G$ is a K-Hopf algebra of dimension $|N|$. Now we define an action of $E[N]^G$ on L by

$$(\sum_{\eta\in N} c_\eta\eta).t = \sum_{\eta\in N} c_\eta\eta^{-1}[1_G G'](t)$$

where $(\sum_{\eta\in N} c_\eta\eta) \in E[N]^G$, $t \in L$ and $\eta^{-1}[1_G G] = \sigma G'$ for some $\sigma \in G$. With this action, the Hopf algebra $E[N]^G$ gives a Hopf-Galois structure of L/K.

Definition 2.6.15. *The group G' has a* normal complement *S in G if there exists some normal subgroup $S \trianglelefteq G$ such that we can write $G = SG'$ with $S \cap G' = \{e\}$.*

Definition 2.6.16. *An extension is* almost classically Galois *if the group G' has a normal complement S in G. For other equivalent conditions see Definition 4.2 of [GP87].*

In this case $\lambda(S) \subseteq \lambda(G) \subseteq \mathrm{Perm}(X)$.

Proposition 2.6.17. *The subgroup $\lambda(S)$ is regular on X and normalised by $\lambda(G)$.*

Proof. Since S is normal in G, we have $\lambda(g)\lambda(s)\lambda(g)^{-1} \in \lambda(S)$ for all $g \in G$ and $s \in S$ hence $\lambda(S)$ is normalised by $\lambda(G)$. Since we can write $G = SG'$ with $S \cap G' = \{e\}$, we have $|S| = \frac{|G|}{|G'|} = |X|$. Recall that the map $\lambda : G \to \mathrm{Perm}(X)$ is given by $\lambda(g)[xG'] = gxG'$. Since S is a normal complement of G', the elements of S form a set of coset representatives for G' in G, so we can write $X = \{xG' | x \in S\}$. Now for $s \in S$ look at $\lambda(s)[eG'] = seG' = sG'$. As s varies, we reach all of the cosets in X, so as sets $\{\lambda(s)[eG'] | s \in S\} = \{sG' | S \in S\} = X$ and we conclude that $\lambda(S)$ is transitive on X. For completeness we will also show that the stabiliser of every element is trivial. Let $xG' \in X$, and $s \in S$. Then $\lambda(s)[xG'] = xG'$ if and only if $sxG' = xG'$ if and only if $x^{-1}sxG' = G'$ if and only if $x^{-1}sx \in G'$. But because S is a normal subgroup of G, we have $x^{-1}sx \in S$, and we get $\lambda(s)[xG'] = xG'$ if and only if $x^{-1}sx \in S \cap G' = \{e\}$ if and only if $s = e$. □

In Section 1 of [Koh98] Kohl discusses almost classical Hopf-Galois structures defined as follows.

Definition 2.6.18. *A Hopf-Galois structure on a separable extension L/K is called an* almost classical Hopf-Galois structure *if the corresponding regular subgroup N of* $\mathrm{Perm}(X)$ *is the opposite of a subgroup of the form $\lambda(S)$, with S a normal complement to G' in G. (That is N is the centraliser in* $\mathrm{Perm}(X)$ *of $\lambda(S)$.)*

Note that if L/K admits an almost classical Hopf-Galois structure then G' has a normal complement in G, so L/K is necessarily an almost classically Galois extension. However, not every Hopf-Galois structure admitted by an almost classically Galois extension is an almost classical Hopf-Galois structure.

Remark 2.6.19. *In this thesis we will consider almost classically Galois extensions with the additional property that each normal complement S of G' in G is abelian. In this case the subgroup $\lambda(S)$ is equal to its own opposite in* $\mathrm{Perm}(X)$*, and so we can characterise almost classical Hopf-Galois structures as those for which the corresponding regular subgroup N of* $\mathrm{Perm}(X)$ *has the form $\lambda(S)$ with S a normal complement to G' in G.*

Definition 2.6.20. *The* type *of a Hopf-Galois structure is the isomorphism class of the corresponding group N.*

Studying regular subgroups of X directly can be difficult when X is large. Byott's translation theorem addresses this problem by instead working with the holomorph of N. We will now see that this is often a much smaller group.

Definition 2.6.21. *The* holomorph of N *is the normaliser in* $\mathrm{Perm}(N)$ *of the image of the left regular representation of N, i.e.* $\mathrm{Hol}(N) = \mathrm{Norm}_{\mathrm{Perm}(N)}\,\lambda(N)$.

Proposition 2.6.22. *Concretely, the holomorph can be described as the semidirect product* $\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N)$*, where ρ is the right regular representation. As a set,*

$$\mathrm{Hol}(N) = \{\rho(\eta)\theta | \eta \in N, \theta \in \mathrm{Aut}(N)\},$$

with multiplication given by

$$\rho(\eta)\theta\rho(\eta')\theta' = \rho(\eta)\rho(\theta(\eta'))\theta\theta' = \rho(\eta\theta(\eta'))\theta\theta'.$$

Proof. See Proposition 7.2 of [Chi00]. □

Remark 2.6.23. *When considering the holomorph, we view N as an abstract group rather than a subgroup of* $\mathrm{Perm}(X)$.

An important consequence of the fact that $\mathrm{Hol}(N)$ is a semidirect product is that $|\mathrm{Hol}(N)| = |\rho(N)||\mathrm{Aut}(N)|$. This is usually much smaller than $|\mathrm{Perm}(N)|$. We can now state Byott's Translation Theorem.

Theorem 2.6.24 (Byott's Translation Theorem)**.** *There is a bijection between*

$$\mathcal{N} = \{\textit{regular embeddings } \alpha : N \hookrightarrow \mathit{Perm}(X)\}$$

and

$$\mathcal{G} = \{\textit{embeddings } \beta : G \hookrightarrow \mathrm{Perm}(N) \textit{ such that } \beta(G') = \mathrm{Stab}_{\beta(G)}(e_N)\}.$$

Furthermore, if α corresponds to β and α' corresponds to β', then $\alpha(N) = \alpha'(N)$ if and only if $\beta' = \gamma\beta\gamma^{-1}$ for some $\gamma \in \mathrm{Aut}(N)$ (explicitly this means $\beta'(\sigma)[\eta] = \gamma\beta(\sigma)\gamma^{-1}[\eta]$ for all $\eta \in N$) and $\alpha(N)$ is normalised by $\lambda(G)$ if and only if $\beta(G) \subseteq \mathrm{Hol}(N)$.

Proof. See Theorem 7.3 of [Chi00]. □

2.7 Hopf-Galois module theory

In order to study the rings of algebraic integers in non-normal extensions we wish to study $\mathcal{O}_L$ relative to a Hopf algebra H. We have a Hopf-Galois analgoue of the normal basis theorem.

Theorem 2.7.1. *If H is a Hopf algebra giving a Hopf-Galois structure on a finite extension of fields L/K, then L is a free H-module of rank one.*

Proof. See Theorem 2.16 of [Chi00]. □

We explicitly construct the largest subring of H over which $\mathcal{O}_L$ is a module in the following way.

Definition 2.7.2. *The* associated order *of $\mathcal{O}_L$ in H is defined as*

$$\mathcal{A}_H := \{h \in H | h \cdot x \in \mathcal{O}_L \textit{ for all } x \in \mathcal{O}_L\}.$$

This is a very natural generalisation of the corresponding definition for $K[G]$. In the context of Greither-Pareigis theory, in which $H = E[N]^G$, the following result relates the associated order to the fixed ring $\mathcal{O}_E[N]^G$.

Proposition 2.7.3. $\mathcal{O}_E[N]^G \subseteq \mathcal{A}_H$.

Proof. See Proposition 2.5 of [Tru11]. □

Recall the material on completions (Section 2.2). This allows us to study $\mathcal{A}_{H,\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ rather than studying $\mathcal{A}_H$ directly. The following result determines the associated order and freeness for primes which do not divide the degree of the extension.

Proposition 2.7.4. *Let L/K be a finite extension of number fields with Galois closure E and let $G = \mathrm{Gal}(E/K)$. Suppose that L/K is H-Galois for some commutative Hopf algebra $H = E[N]^G$. Suppose that $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ lying above a prime number $p \nmid [L : K]$. Then $\mathcal{A}_{H,\mathfrak{p}} = \mathcal{O}_{E,\mathfrak{p}}[N]^G$ and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module.*

Proof. See Theorem 5.8 of [Tru11]. □

The natural approach to determining the associated order is to first describe the structure of the associated order $\mathcal{A}_{H,\mathfrak{p}}$ as a ring, then determine whether $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module. The following proposition combines these, allowing us to do these "all in one" and will be useful for determining the associated order for prime ideals which lie above the degree of the extension.

Theorem 2.7.5 (All in one approach)**.** *Let L/K be a finite extension of number fields of degree n, let H be a Hopf algebra giving a Hopf-Galois structure on L/K and let $\mathcal{A}_H$ denote the associated order of $\mathcal{O}_L$ in H. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and let x_1, ..., x_n be an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$. Suppose that there exists $x \in \mathcal{O}_{L,\mathfrak{p}}$ and elements a_1, ..., $a_n \in \mathcal{A}_{H,\mathfrak{p}}$ such that $a_i \cdot x = x_i$ for each i. Then a_1, ..., a_n form an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{A}_{H,\mathfrak{p}}$ and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module.*

Proof. First we show that a_1, ..., a_n form a $K_{\mathfrak{p}}$-basis of $H_{\mathfrak{p}}$ and that x is a free generator of $L_{\mathfrak{p}}$ as an $H_{\mathfrak{p}}$-module. Suppose that $c_1a_1 + ... + c_na_n = 0$ for some $c_i \in K_{\mathfrak{p}}$. Then

$$\begin{aligned} (c_1a_1 + ... + c_na_n) \cdot x &= 0 \\ \Rightarrow c_1(a_1 \cdot x) + ... + c_n(a_n \cdot x) &= 0 \\ \Rightarrow c_1x_1 + ... + c_nx_n &= 0 \\ \Rightarrow c_1 = ... = c_n &= 0 \end{aligned}$$

since x_1, ..., x_n form a $K_\mathfrak{p}$-basis of $L_\mathfrak{p}$. Hence a_1, ..., a_n are linearly independent over $K_\mathfrak{p}$. Since $H_\mathfrak{p}$ has dimension n over $K_\mathfrak{p}$, these elements form a $K_\mathfrak{p}$-basis of $H_\mathfrak{p}$. Now given $y \in L_\mathfrak{p}$ there exist unique d_1, ..., $d_n \in K_\mathfrak{p}$ such that

$$\begin{aligned} y &= d_1x_1 + ... + d_nx_n \\ &= d_1(a_1 \cdot x) + ... + d_n(a_n \cdot x) \\ &= (d_1a_1 + ... + d_na_n) \cdot x \end{aligned}$$

Thus $y = h \cdot x$ for some unique $h \in H_\mathfrak{p}$ and so x is a free generator of $L_\mathfrak{p}$ as an $H_\mathfrak{p}$-module. Now let $a \in \mathcal{A}_{H,\mathfrak{p}}$. Then $a \cdot x \in \mathcal{O}_{L,\mathfrak{p}}$, so there exist unique c_1, ..., $c_n \in \mathcal{O}_{K,\mathfrak{p}}$ such that

$$\begin{aligned} a.x &= c_1x_1 + ... + c_nx_n \\ &= c_1(a_1 \cdot x) + ... + c_n(a_n \cdot x) \\ &= (c_1a_1 + ... + c_na_n) \cdot x \end{aligned}$$

Since x is a free generator of $L_\mathfrak{p}$ as an $H_\mathfrak{p}$-module, this implies that $a = c_1a_1 + ... + c_na_n$. Hence a_1, ..., a_n form an $\mathcal{O}_{K,\mathfrak{p}}$ basis for $\mathcal{A}_{H,\mathfrak{p}}$. Finally let $y \in \mathcal{O}_{L,\mathfrak{p}}$. Then there exist unique d_1, ..., $d_n \in \mathcal{O}_{K,\mathfrak{p}}$ such that

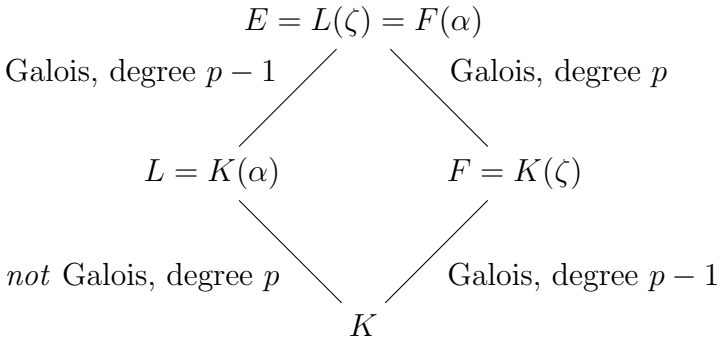
$$\begin{aligned} y &= d_1x_1 + ... + d_nx_n \\ &= d_1(a_1 \cdot x) + ... + d_n(a_n \cdot x) \\ &= (d_1a_1 + ... + d_na_n) \cdot x \end{aligned}$$

Thus $y = a \cdot x$ for a unique element $a \in \mathcal{A}_{H,\mathfrak{p}}$ and so x is a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{A}_{H,\mathfrak{p}}$-module. □

2.8 An example of Hopf-Galois module theory - Tamely ramified radical extensions of prime degree

This section will summarise the approach and results of Truman's 2020 paper "Hopf-Galois module structure of tamely ramified radical extensions of prime de-

gree", [Tru20]. We will apply the same strategy to extensions of prime power and square free degree later. The motivation of Truman's paper is to use Hopf-Galois theory to study tame radical extensions of prime degree and obtain an analogue of Gómez Ayala's criterion for freeness. A field diagram for the class of extensions studied by Truman is the following:



An important hypothesis used in [Tru20] is that the prime number p is unramified in K. Consequences of this assumption are the following.

Lemma 2.8.1. *Let $F = K(\zeta)$ and suppose that p is unramified in K. Then*

1. *The extension F/K has degree $p-1$*
2. *Each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying above p is totally ramified in F/K*
3. *The set $\{1, \zeta, ..., \zeta^{p-2}\}$ is an integral basis of F over K*

Proof. See Lemma 3.1 of [Tru20]. □

Note also that F/K is tamely ramified since it is a Galois extension of degree $p-1$ and it is ramified only at prime ideals lying above $p\mathcal{O}_K$. The following proposition gives a criterion for the extension to be tame.

Proposition 2.8.2. *The extension L/K is tame if and only if there exists $\alpha \in \mathcal{O}_L$ such that*

1. *$L = K(\alpha)$*
2. *$\alpha^p \equiv 1 \pmod{p^2\mathcal{O}_K}$*

Proof. See Proposition 3.3 of [Tru20]. □

Compare these criteria to those required in the Galois case where we had $\alpha^p \equiv 1 \pmod{(\zeta-1)^p\mathcal{O}_K}$, here $\zeta \notin K$ so we require a slightly stronger condition. In order to assist in determining local intergal bases for the extension we first state a lemma.

Lemma 2.8.3. *In the extension $K(\alpha)/K$, prime ideals that do not lie above $p\mathcal{O}_K$ are either unramified or totally ramified.*

Proof. See Proposition 3.4 of [Tru20] □

The following propositions give local integral bases at prime ideals which do not and do lie above p respectively.

Proposition 2.8.4. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ that does not lie above p and let $\pi_\mathfrak{p}$ be a uniformiser of $K_\mathfrak{p}$. An integral basis of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{O}_{K,\mathfrak{p}}$ is given by*

$$\left\{ \frac{\alpha^j}{\pi_\mathfrak{p}^{r_\mathfrak{p}(a^j)}} | j = 0, 1, ..., p-1 \right\}.$$

Proof. See Proposition 3.4 of [Tru20]. □

Proposition 2.8.5. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ that lies above p. An integral basis of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{O}_{K,\mathfrak{p}}$ is given by*

$$\left\{ 1, \alpha, ..., \alpha^{p-2}, \frac{1}{p}(1 + \alpha + ... + \alpha^{p-1}) \right\}.$$

Proof. See Proposition 3.5 of [Tru20]. □

Section 4 of [Tru20] studies the Hopf-Galois structure admitted by the extension and its properties.

Proposition 2.8.6. *The extension L/K admits exactly one Hopf-Galois structure.*

Proof. See Proposition 4.1 of [Tru20] □

Remark 2.8.7. *Although it is not explicitly mentioned in [Tru20], this Hopf-Galois structure is almost classical.*

Remark 2.8.8. *Proposition 4.2 of [Tru20] determines the regular subgroup of* $\mathrm{Perm}(X)$ *that corresponds to this Hopf-Galois structure.*

Proposition 2.8.9. *We have $H \cong K^p$ as K-algebras.*

Proof. See Proposition 4.3 of [Tru20]. □

Proposition 2.8.10. *For $i,\ j = 0, 1, ..., p-1$ we have $e_i \cdot \alpha^j = \delta_{i,j}\alpha^j$ (where the idempotents e_i are analogous to the $e_{k,i}$ defined earlier).*

Proof. See Proposition 4.4 of [Tru20]. □

The following result shows that $\mathcal{O}_L$ is a locally free $\mathcal{A}_H$-module, that $\mathcal{A}_H = \mathcal{O}_E[N]^G$ and gives explicit generators.

Theorem 2.8.11. *We have $\mathcal{A}_H = \mathcal{O}_E[N]^G$ and $\mathcal{O}_L$ is a locally free $\mathcal{A}_H$-module. For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{A}_{H,\mathfrak{p}}$-module is given by*

$$x_{\mathfrak{p}} = \begin{cases} \frac{1}{p}\sum_{j=0}^{p-1} \alpha^j & \text{if } \mathfrak{p} | p\mathcal{O}_K \\ \frac{1}{p}\sum_{j=0}^{p-1} \frac{\alpha^j}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\alpha^j)}} & \text{otherwise.} \end{cases}$$

Proof. See Theorem 5.1 of [Tru20]. □

Chapter 3

A family of non-normal extensions of prime power degree - Field theory and Hopf-Galois structures

3.1 Setup for a non-normal extension of degree p^r

Let p be an odd prime, let K be a number field such that p is unramified in K and let ζ be a primitive p^{th} root of unity. Let $L = K(\alpha_1, ..., \alpha_r)$ where $\alpha_i^p = a_i \in K$, note that $\alpha_i \notin K$ so that $[K(\alpha_i) : K] = p$. Then the extension L/K is separable. We will assume that $[L : K] = p^r$.

Proposition 3.1.1. *The Galois closure of L/K is $E = L(\zeta)$.*

Proof. By adjoining ζ to form the field $E = L(\zeta)$ the extension E/K is Galois because the minimal polynomial of each α_i (for $0 \leq i \leq r$) is $x^p - a_i \in K[x]$ which has roots $\zeta^j \alpha_i$ for $j = 0, ..., p-1$. Hence E is the splitting field over K of the product of these r polynomials, $\prod_{i=1}^{r}(x^p - a_i)$. On the other hand, the Galois closure must contain ζ because all roots of the minimal polynomials of all α_i over K must lie in the Galois closure, so the Galois closure is indeed $E = L(\zeta)$. □

Lemma 3.1.2. *The extension $K(\zeta)/K$ has degree $p - 1$.*

Proof. Since p is unramified in K, the polynomial $x^{p-1} + ... + x + 1$ is irreducible over K and is therefore the minimal polyomial of ζ over K. See also Lemma 3.1 of [Tru20]. □

Note that $[E : K] = p^r(p-1)$ since E is the compositum of $F = K(\zeta)$ and L and their degrees $[F : K] = p - 1$ and $[L : K] = p^r$ are coprime. The Galois group of E/K is $G = \langle \sigma_1, ..., \sigma_r, \tau \rangle$ where

$$\sigma_i(\alpha_i) = \zeta\alpha_i,\ \sigma_i(\alpha_j) = \alpha_j \text{ for } j \neq i,\ \sigma_i(\zeta) = \zeta \text{ for all } i,$$

$$\tau(\alpha_i) = \alpha_i \text{ for all } i \text{ and } \tau(\zeta) = \zeta^d \text{ where } d \text{ is a primitive root modulo } p.$$

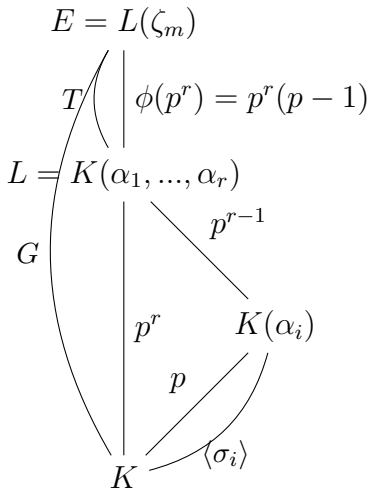
This has relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i \text{ for all } i \text{ and } j \text{ and } \tau\sigma_i = \sigma_i^d\tau \text{ for all } i$$

hence

$$\langle \sigma_1, ..., \sigma_r \rangle \cong C_p^r \text{ and } G = \langle \sigma_1, ..., \sigma_r \rangle \rtimes \langle \tau \rangle.$$

Note that $T = \mathrm{Gal}(E/L) = \langle \tau \rangle$ with order $p - 1$. Hence $|X| = \frac{|G|}{|T|} = p^r$, where X is the left coset space G/T. In the next section, we will discuss the possibilities for N.



3.2 The almost classical Hopf-Galois structure for the extension of degree p^r

Proposition 3.2.1. *The extension L/K has a unique almost classical Hopf-Galois structure.*

Proof. In the notation of the Greither-Pareigis theorem (Theorem 2.6.14) we have $T = \langle\tau\rangle$. Let $S = \langle\sigma_1, ..., \sigma_r\rangle \cong C_p^r$ be the unique Sylow p-subgroup of G. Then because S is the unique Sylow p-subgroup of G, it is normal in G and we have $S \trianglelefteq G$, $ST = G$ and $S \cap T = \{e\}$. Since S is the unique Sylow p-subgroup of G, the extension has a unique almost classical Hopf-Galois structure (given by $\lambda(S)$) as claimed. □

Remark 3.2.2. *Note that the normal complement S is abelian as promised in Chapter 2.*

We will construct the embedding β which gives rise to the unique almost classical Hopf-Galois structure. Let $N \cong C_p^r = \langle\eta_1, ..., \eta_r\rangle$, let $\theta \in \mathrm{Aut}(N)$ be defined by $\theta(\eta_i) = \eta_i^d$ for all i and let $\beta : G \hookrightarrow \mathrm{Hol}(N) \cong N \rtimes \mathrm{Aut}(N)$ be defined by $\beta(\sigma_i) = (\eta_i, 1)$ for all i and $\beta(\tau) = (1, \theta)$. In order to verify that this map β is a suitable embedding, there are various checks that we have to perform.

Proposition 3.2.3. *The map β as defined above is a suitable embedding.*

Proof. To show that $\beta(\sigma_i)$ has order p for all i, note that $\beta(\sigma_i) = (\eta_i, 1)$ and since η_i is one of the generators of C_p^r, it has order p. To show that $\beta(\tau)$ has order $p-1$, note that $\theta^j(\eta_i) = \eta_i^{d^j}$ and since d is a primitive root modulo p this implies that $\beta(\tau)$ has order $p-1$. To show that β respects the relations that define G, we have

$$\beta(\sigma_i\sigma_j) = \beta(\sigma_i)\beta(\sigma_j) = (\eta_i, 1)(\eta_j, 1) = (\eta_i\eta_j, 1),$$

$$\beta(\sigma_j\sigma_i) = \beta(\sigma_j)\beta(\sigma_i) = (\eta_j, 1)(\eta_i, 1) = (\eta_j\eta_i, 1),$$

$$\beta(\tau\sigma_i) = \beta(\tau)\beta(\sigma_i) = (1, \theta)(\eta_i, 1) = (\eta_i^d, \theta),$$

$$\beta(\sigma_i^d\tau) = \beta(\sigma_i^d)\beta(\tau) = (\eta_i^d, 1)(1, \theta) = (x\eta_i^d, \theta).$$

To show that β has a trivial kernel, note that $\beta(e_G) = (1, 1)$. To show that no other element of G is contained in the kernel, note that $\beta(\sigma_i) = (\eta_i, 1)$ for all i and since η_i has order p for all i, no combination of the elements σ_i can be mapped to the identity. Similarly, since $\beta(\tau) = (1, \theta)$ and θ has order $p - 1$, no power of τ can be mapped to the identity. To show that $\beta(\langle\tau\rangle)$ is the stabiliser of e_N, since $\beta(\langle\tau\rangle)[e_N] = (1, \langle\theta\rangle)[e_N] = e_N$, e_N is stabilised by $\beta(\langle\tau\rangle)$, to show that no other element is contained in the stabiliser, note that $\beta(\sigma_i)[e_N] = (\eta_i, 1)[e_N] = \eta_i$ for all i. Hence β is a suitable embedding of G into $\mathrm{Hol}(N)$ as claimed. □

Proposition 3.2.4. *For $i = 1, ..., r$, let $\eta'_i \in \mathrm{Perm}(X)$ be defined by $\eta'_i(\overline{\sigma_1^{j_1}...\sigma_r^{j_r}}) = \overline{\sigma_1^{j_1}...\sigma_i^{j_i-1}...\sigma_r^{j_r}}$. Then $N' = \langle\eta'_1, ..., \eta'_r\rangle$ is the regular subgroup of $\mathrm{Perm}(X)$ that corresponds to the unique almost classical Hopf-Galois structure on L/K.*

Proof. Recall that by construction the map $\alpha(\eta)$ is given by $b^{-1}\lambda_N(\eta)b$ for some $\eta \in N$. In this case the map b is given by $b(\overline{g}) = \beta(g)e_N$. Hence if we write $\eta = \eta_1^{i_1}...\eta_r^{i_r}$ and consider a typical element of G $\sigma_1^{j_1}...\sigma_r^{j_r}\tau^k$, we have $\alpha(\eta)[\overline{\sigma_1^{j_1}...\sigma_r^{j_r}}] = b^{-1}\lambda_N(\eta)b[\overline{\sigma_1^{j_1}...\sigma_r^{j_r}}] = b^{-1}\lambda_N(\eta)(\eta_1^{j_1}...\eta_r^{j_r}) = b^{-1}(\eta_1^{i_1+j_1}...\eta_r^{i_r+j_r}) = \overline{\sigma_1^{i_1+j_1}...\sigma_r^{i_r+j_r}} = \eta_1'^{-i_1}...\eta_r'^{-i_r}(\overline{\sigma_1^{j_1}...\sigma_r^{j_r}})$. Hence $\alpha(N) = \{\eta_n'^{i_n} | 1 \leq n \leq r, 0 \leq i \leq p-1\} = N'$. □

The following remark is a consequence of Proposition 3.2.1.

Remark 3.2.5. *In other words, we have $\alpha(N) = \lambda_G(\langle\sigma_1, ..., \sigma_r\rangle)$ as a subgroup of $\mathrm{Perm}(X)$. This is the image of the unique Sylow p-subgroup S of G under the map λ hence this will give rise to the unique almost classical Hopf-Galois structure on the extension.*

3.3 Hopf-Galois structures when $r = 2$

In this section, our main aim is to prove the following proposition.

Proposition 3.3.1. *The unique almost classical Hopf-Galois structure is the only Hopf-Galois structure on the extension in the case where $r = 2$.*

Our strategy for the proof will be firstly to show that there are no suitable embeddings when $N \cong C_{p^2}$. We then proceed to show that all suitable embeddings when $N \cong C_p \times C_p$ fall under one equivalence class.

Proposition 3.3.2. *There are no suitable embeddings $\beta : G \hookrightarrow \mathrm{Hol}(N)$ in the case where $N \cong C_{p^2}$.*

We will prove this proposition in stages. Recall that by "suitable" we mean the condition that $\beta(\langle\tau\rangle) = \mathrm{Stab}_{\beta(G)}(e_N)$ from the translation theorem. The reason there are no suitable subgroups is connected to the structure of the subgroups of the Sylow p-subgroup of $\mathrm{Hol}(N)$.

If there were such an embedding, then $\beta(\langle\sigma_1, \sigma_2\rangle)$ would be a subgroup of $\mathrm{Hol}(N)$ isomorphic to $C_p \times C_p$. In fact since $C_p \times C_p$ has order p^2, it would have to be contained in the unique Sylow p-subgroup of $\mathrm{Hol}(N)$, which is $N \rtimes T$, where T is the unique subgroup of $\mathrm{Aut}(N)$ of order p. Note that $\mathrm{Aut}(N)$ is a cyclic group here, so it has a unique subgroup of each order dividing its order.

Proposition 3.3.3. *$N \rtimes T$ has a unique subgroup isomorphic to $C_p \times C_p$, but this is not suitable (i.e, it does not satisfy the conditions of the translation theorem).*

We will prove this proposition in stages. The generators of T are the automorphisms of N that have order p, since because T has order p as a subgroup, any non-identity element of T will be a generator. The automorphisms of N are precisely the homomorphisms defined by $\eta \mapsto \eta^r$ with $gcd(r, p^2) = 1$.

Proposition 3.3.4. *Define $\theta \in \mathrm{Aut}(N)$ by $\theta(\eta) = \eta^{p+1}$. Then θ has order p.*

Proof. If we consider θ^2, we have $\theta^2(\eta) = \theta(\eta^{p+1}) = \eta^{(p+1)^2} = \eta^{p^2+2p+1} = \eta^{2p+1}$. If we proceed inductively, we get $\theta^k(\eta) = \eta^{kp+1}$ so $\theta^k(\eta) = \eta$ if and only if $k \equiv 0 \pmod{p}$ so θ has order p. □

Now, we can write the Sylow p-subgroup $N \rtimes T$ as $\langle\eta\rangle \rtimes \langle\theta\rangle$ with typical elements written as ordered pairs (η^i, θ^k), with $i = 0, ..., p^2 - 1$ and $k = 0, ..., p - 1$. We wish to determine more information about the orders of the elements in this subgroup. First, note that the element $(\eta^p, 1)$ has order p.

Proposition 3.3.5. *The subgroup generated by* $(\eta^p, 1)$ *is precisely the centre of* $N \rtimes T$.

Proof. Let (η^i, θ^k) be a typical element of $N \rtimes T$ and let $(\eta^{jp}, 1)$ be a typical element of the subgroup. Then $(\eta^{jp}, 1)(\eta^i, \theta^k) = (\eta^{jp}\eta^i, \theta^k) = (\eta^{jp+i}, \theta^k)$ and $(\eta^i, \theta^k)(\eta^{jp}, 1) = (\eta^i\eta^{jp(p+1)^k}, \theta) = (\eta^{i+jp}, \theta^k)$. To verify that no other elements of the group are in the centre, since the centre of a non-abelian group of order p^3 has order p and since the subgroup generated by $(\eta^p, 1)$ has order p, it is precisely the centre. □

Now, note that $(1, \theta)$ also has order p and because the element $(\eta^p, 1)$ is in the centre, it commutes with all other elements. Hence $\langle(\eta^p, 1), (1, \theta)\rangle \cong C_p \times C_p$. We have two elements of order p and they commute with each other and they generate different subgroups of $N \rtimes T$ so the group that they generate is isomorphic to $C_p \times C_p$. Hence we have found an example of a subgroup of $N \rtimes T$ that is isomorphic to $C_p \times C_p$. To show that this is unique, we will show that there are no more elements of order p. Recall that the elements of the semidirect product $N \rtimes T$ are of the form (η^i, θ^k), with $i = 0, ..., p^2 - 1$ and $k = 0, ..., p - 1$. The elements that we have not accounted for are those of the form (η^i, θ^k), with $i = 0, ..., p^2 - 1$, $p \nmid i$ and $k = 0, ..., p - 1$.

Proposition 3.3.6. *These elements all have order* p^2. *Hence they each generate some cyclic subgroup of order* p^2.

Proof. We will first prove the case $k = 1$ by considering the element $x = (\eta^i, \theta)$. We have

$$x^2 = (\eta^i, \theta)(\eta^i, \theta) = (\eta^i\eta^{i(p+1)}, \theta^2),\ x^3 = (\eta^i, \theta)(\eta^i\eta^{i(p+1)}, \theta^2) = (\eta^i\eta^{i(p+1)}\eta^{i(p+1)^2}, \theta^3)$$

and so on. Inductively, we get

$$x^r = (\eta^{i(1+(p+1)+(p+1)^2+...+(p+1)^{r-1})}, \theta^r) = (\eta^{i\frac{(p+1)^r-1}{p}}, \theta^r).$$

Since η has order p^2, if we study the exponent modulo p^2, we get

$$\begin{aligned}\frac{i}{p}((p+1)^r-1) &= \frac{i}{p}(p^r+\binom{r}{1}p^{r-1}+...+\binom{r}{r-2}p^2+\binom{r}{r-1}p)\\ &= i\left(p^{r-1}+...+\binom{r}{r-2}p+\binom{r}{r-1}\right)\\ &\equiv i\left(\frac{r(r-1)}{2}p+r\right)\begin{cases}\equiv 0 \pmod{p^2} & \text{if } r\equiv 0 \pmod{p^2}.\\ \not\equiv 0 \pmod{p^2} & \text{otherwise.}\end{cases}\end{aligned}$$

Hence $x^r=(1,1)$ if and only if $r\equiv 0 \pmod{p^2}$ so x has order p^2. We will now generalise this argument by considering the other cases. Now let $x=(\eta^i,\theta^k)\in N\rtimes T$ be such that $p\nmid i$ and $k\neq 1$. Then

$$x^2=(\eta^i,\theta^k)(\eta^i,\theta^k)=(\eta^i\eta^{ik(p+1)},\theta^{2k}),$$

$$x^3=(\eta^i,\theta^k)(\eta^i\eta^{ik(p+1)},\theta^{2k})=(\eta^i\eta^{ik(p+1)}\eta^{i(k(p+1))^2},\theta^{3k})$$

and so on. Inductively, we get

$$x^r=(\eta^{i+...+i(k(p+1))^{r-1}},\theta^{rk})=(\eta^{i\frac{(k(p+1))^r-1}{k(p+1)-1}},\theta^{rk}).$$

We now aim to study the exponent of η modulo p^2. To do this, we write $B=i\frac{(k(p+1))^r-1}{k(p+1)-1}$. Then multiplying up gives

$$B(kp+k-1)=i(k^r(p^r+...+\binom{r}{r-1}p+1)-1),$$

taking congruences modulo p^2 gives

$$B(kp+k-1)\equiv i(k^r(\frac{r(r-1)}{2}p+1)-1) \pmod{p^2}$$

and dividing out gives

$$B\equiv\frac{i(k^r(\frac{r(r-1)}{2}p+1)-1)}{kp+k-1} \pmod{p^2}.$$

Now we need to determine when $B\equiv 0 \pmod{p^2}$. Since B is a fraction, this happens if and only if the numerator is congruent to zero modulo p^2, i.e. if and only if $i(k^r(\frac{r(r-1)}{2}p+1)-1)\equiv 0 \pmod{p^2}$. Since we assumed that $p\nmid i$, this happens if and only if $(k^r(\frac{r(r-1)}{2}p+1)-1)\equiv 0 \pmod{p^2}$, which happens if and only if $r\equiv 0 \pmod{p^2}$. Hence, we again conclude that $x^r=(1,1)$ if and only if $r\equiv 0 \pmod{p^2}$ so x has order p^2. □

Combining Propositions 3.3.4 to 3.3.6 we can now prove Proposition 3.3.3.

Proof of Proposition 3.3.3. We have shown that the subgroup $A := \langle(\eta^p, 1), (1, \theta)\rangle$ is the unique subgroup of $\mathrm{Hol}(N)$ isomorphic to $C_p \times C_p$. Hence, if $\beta : G \hookrightarrow \mathrm{Hol}(N)$ is an embedding, then $\beta(\langle\sigma_1, \sigma_2\rangle) = A$. But then some element of $\langle\sigma_1, \sigma_2\rangle$ is mapped to $(1, \theta) \in A$ and this element stabilises e_N because $(1, \theta)[e_N] = e_N\theta[e_N] = e_N$ since $\theta \in \mathrm{Aut}(N)$. Hence $\mathrm{Stab}_{\beta(G)}(e_N) \supsetneq \beta(\langle\tau\rangle)$. The translation theorem says that the stabiliser of the identity should be precisely the image of T under β, but here we get a set that is too large because some combination of σ_1 and σ_2 gets mapped to $(1, \theta)$ and this stabilises the identity e_N. Therefore this β is not a suitable embedding. □

Combining all of the above, we can now prove Proposition 3.3.2.

Proof of Proposition 3.3.2. If β is any embedding of G into $\mathrm{Hol}(N)$, then $\beta(\langle\sigma_1, \sigma_2\rangle) = A$ so $\langle\sigma_1, \sigma_2\rangle$, the unique Sylow p-subgroup of G, is mapped to this unique subgroup A which is the only elementary abelian subgroup of order p^2 in the holomorph. If this is this case, then the embedding β is not suitable to be used in the translation theorem. We conclude that there are no suitable embeddings of G into $\mathrm{Hol}(N)$ when N is cyclic of order p^2. □

We now return to the case in which $N \cong C_p \times C_p$ and show that any suitable embedding of G into $\mathrm{Hol}(N)$ is equivalent to the one we found in Proposition 3.2.3. If $\beta : G \hookrightarrow \mathrm{Hol}(N)$ is a suitable embedding, then $T := \beta(\langle\sigma_1, \sigma_2\rangle \cong C_p \times C_p$ is a subgroup of $\mathrm{Hol}(N)$ and is regular on N because $\mathrm{Stab}_{\beta(G)}(e_N) = \beta(\langle\tau\rangle)$, so by the Orbit-Stabiliser theorem, $\beta(G).e_N = N$ and so T is transitive on N. Since T also has the same order as N, it is a regular subgroup of $\mathrm{Hol}(N)$ isomorphic to $C_p \times C_p$. Since the order of T is a power of the prime p, it must be contained in some Sylow p-subgroup of $\mathrm{Hol}(N)$. Note that $\mathrm{Aut}(N) \cong GL_2(\mathbb{Z}_p)$ (where $\mathbb{Z}_p$ denotes the field of p elements) and $|\mathrm{Aut}(N)| = p(p-1)^2(p+1)$. It can be useful to identify $\mathrm{Aut}(N)$ with $GL_2(\mathbb{Z}_p)$ to make explicit calculations easier. The group $\mathrm{Aut}(N)$ does not have a unique Sylow p-subgroup in this case. One example of a Sylow p-subgroup is the group $S := \langle x, y, \pi\rangle$ where $\pi(x) = x$ and $\pi(y) = xy$.

Our first aim is to determine equivalence classes of suitable embeddings β such that $T \subseteq S$. One example is the particular embedding β which we defined in Proposition 3.2.3. Henceforth we will refer to this particular embedding as β_0. In order to understand if there are any other embeddings, we will try to describe all subgroups of the particular Sylow p-subgroup S that are isomorphic to $C_p \times C_p$.

Proposition 3.3.7. *The subgroups of S that are isomorphic to $C_p \times C_p$ are $T_k := \langle (x,1),(y,\pi^k)\rangle$ for $k = 0,...,p-1$ and $T_* := \langle (x,1),(1,\pi)\rangle$. Each of the T_k is regular but T_* is not.*

Proof. Firstly, we seek elements of S of order p. If we consider a typical element of S, $s = (x^i y^j, \pi^k)$, we have

$$s^2 = (x^i y^j, \pi^k)(x^i y^j, \pi^k) = (x^i y^j x^i x^{kj} y^j, \pi^{2k}) = (x^{kj} x^{2i} y^{2j}, \pi^{2k}),$$

$$s^3 = (x^{kj} x^{2i} y^{2j}, \pi^{2k})(x^i y^j, \pi^k) = (x^{kj} x^{2i} y^{2j} x^i x^{2kj} y^j, \pi^{3k}) = (x^{3kj} x^{3i} y^{3j}, \pi^{3k}).$$

Inductively, we get

$$(x^i y^j, \pi^k)^r = (x^{\frac{r(r-1)}{2} kj} x^{ri} y^{rj}, \pi^{rk}), \text{ where } 0 \leq i,j,k \leq p-1 \text{ and } r \in \mathbb{Z}.$$

Hence, every element of S except for the identity element has order p.

Now consider subgroups generated by elements of order p,

$$S_1 := \langle (x^I y^J, \pi^K)\rangle \text{ and } S_2 := \langle (x^{I'} y^{J'}, \pi^{K'})\rangle.$$

For these to yield a subgroup isomorphic to $C_p \times C_p$, we need the generators to commute but because these groups have order p, every element except for the identity is a generator, so we need all elements in S_1 to commute with all elements in S_2.

If $J' = 0$ and $J \neq 0$ (the reverse is similar), then we can write S_2 as $\langle (x^{I'}, \pi^{K'})\rangle$ and we can rewrite S_1 as $\langle (x^i y, \pi^k)\rangle$ by taking a suitable power of the generator such that the exponent of y is congruent to 1 modulo p. Then, considering multiplication of the generators, we have on the one hand

$$((x^i y, \pi^k)(x^{I'}, \pi^{K'}) = (x^{i+I'} y, \pi^{k+K'})$$

and on the other hand

$$(x^{I'}, \pi^{K'})(x^i y, \pi^k) = (x^{i+I'} x^{K'} y, \pi^{k+K'}).$$

These agree if and only if $K' = 0$, so in this case we have $S_2 = \langle (x^{I'}, 1) \rangle$ which is equal to $Z(S)$ if $I' \neq 0$ and by taking a power of the generator, we can rewrite $S_2 = \langle (x, 1) \rangle$. Then S_1 and S_2 generate $\langle (x, 1), (x^i y, \pi^k) \rangle$ and by using suitable negative powers of the first element, we can remove the x^i factor from the second element and hence rewrite the subgroup as $\langle (x, 1), (y, \pi^k) \rangle = T_k$.

Now if $J \neq 0$ and $J' \neq 0$ we rescale by taking powers of the generators so that the exponent of y is congruent to 1 modulo p in both cases. This allows us to rewrite the subgroups as $S_1 = \langle (x^i y, \pi^k) \rangle$ and $S_2 = \langle (x^{i'} y, \pi^{k'}) \rangle$. Then, considering multiplication of the generators, we have on the one hand

$$(x^i y, \pi^k)(x^{i'} y, \pi^{k'}) = (x^{i+i'} x^k y^2, \pi^{k+k'})$$

and on the other hand

$$(x^{i'} y, \pi^{k'})(x^i y, \pi^k) = (x^{i+i'} x^{k'} y^2, \pi^{k+k'}).$$

These agree if and only if $k = k'$, so in this case our subgroups of order p are $\langle (x^i y, \pi^k) \rangle$ and $\langle (x^{i'} y, \pi^k) \rangle$ so if we assume that $i \neq i'$, these generate the subgroup $S_* := \langle (x^i y, \pi^k), (x^{i'} y, \pi^k) \rangle \cong C_p \times C_p$. Now notice that we can write the second generator as $(x^{i'-i}, 1)(x^i y, \pi^k)$ so this implies that $(x^{i'-i}, 1) \in S_*$, so since we assumed that $i \neq i'$, we can take a power of this element to get that $(x, 1) \in S_*$ which means that $S_* = \langle (x, 1), (x^i y, \pi^k) \rangle$ and as before we can use suitable negative powers of the first element, we can remove the x^i factor from the second element and hence rewrite the subgroup as $\langle (x, 1), (y, \pi^k) \rangle = T_k$.

Now if $J = J' = 0$, then we have $S_1 = \langle (x^I, \pi^K) \rangle$ and $S_2 = \langle (x^{I'}, \pi^{K'}) \rangle$. Then, considering multiplication of the generators, we have on the one hand

$$(x^I, \pi^K)(x^{I'}, \pi^{K'}) = (x^{I+I'}, \pi^{K+K'})$$

and on the other hand

$$(x^{I'}, \pi^{K'})(x^I, \pi^K) = (x^{I+I'}, \pi^{K+K'}).$$

These generators commute regardless of the values of I, I', K and K'. Hence S_1 and S_2 generate the subgroup $\langle (x^I, \pi^K), (x^{I'}, \pi^{K'}) \rangle$. Now note that we can take powers of the generators in the following way to obtain

$$((x^I, \pi^K)^{K'}(x^{I'}, \pi^{K'})^{-K})^{(IK'-I'K)^{-1}} = (x, 1) \in \langle (x^I, \pi^K), (x^{I'}, \pi^{K'}) \rangle,$$

$$((x^I, \pi^K)^{-I'}(x^{I'}, \pi^{K'})^{I})^{(IK'-I'K)^{-1}} = (1, \pi) \in \langle (x^I, \pi^K), (x^{I'}, \pi^{K'}) \rangle.$$

Hence we see that S_1 and S_2 generate the subgroup $\langle (x, 1), (1, \pi) \rangle = T_*$.

Note that if $I = I' = 0$, then we have $S_1 = \langle (y^J, \pi^K) \rangle$ and $S_2 = \langle (y^{J'}, \pi^{K'}) \rangle$. Then, considering multiplication of the generators, we have on the one hand

$$(y^J, \pi^K)(y^{J'}, \pi^{K'}) = (x^{KJ'} y^{J+J'}, \pi^{K+K'})$$

and on the other hand

$$(y^{J'}, \pi^{K'})(y^J, \pi^K) = (x^{K'J} y^{J+J'}, \pi^{K+K'}).$$

These agree if and only if $KJ' = K'J$ but if this is the case then $(y^J, \pi^K) \in \langle (y^{J'}, \pi^{K'}) \rangle$ so these elements only generate a subgroup of order p which is not what we require.

Above we have shown that the subgroups T_k are isomorphic to $C_p \times C_p$. This implies that they have the required order to be regular. To complete the proof that they are regular, we let the subgroups act on the identity. A typical element of T_k is $(x, 1)^a (y, \pi^k)^b = (x^{a+k\frac{b(b-1)}{2}} y^b, \pi^k)$. If we let this act on the identity, we have $(x^{a+k\frac{b(b-1)}{2}} y^b, \pi^k)[e_N] = \sigma_1^{a+k\frac{b(b-1)}{2}} \sigma_2^b$. As a and b vary we reach the whole of $\langle \sigma_1, \sigma_2 \rangle$ so the subgroups T_k are transitive and hence regular as claimed.

To show that T_* the last subgroup mentioned in the proposition is not regular, if $\beta : G \hookrightarrow \mathrm{Hol}(N)$ is an embedding such that $\beta(\langle \sigma_1, \sigma_2 \rangle) = \langle (x, 1), (1, \pi) \rangle$, then some element of $\langle \sigma_1, \sigma_2 \rangle$ is mapped to $(1, \pi) \in \langle (x, 1), (1, \pi) \rangle$ and this element stabilises e_N because $(1, \pi)[e_N] = e_N \pi[e_N] = e_N$ since $\pi \in \mathrm{Aut}(N)$. Hence $\mathrm{Stab}_{\beta(G)}(e_N) \supsetneq \beta(\langle \tau \rangle)$. The translation theorem says that the stabiliser of the identity should be precisely the image of T under β, but here we get a set that is too large because some combination of σ_1 and σ_2 gets mapped to $(1, \pi)$ and this stabilises the identity e_N. so this β is not a suitable embedding. □

Proposition 3.3.8. *If $\beta(\langle\sigma_1, \sigma_2\rangle)$ is a regular subgroup of S, then β is equivalent to β_0.*

Proof. In this case $\beta(\langle\sigma_1, \sigma_2\rangle) = T_k$ for some k and we have $\beta(G) = \langle(x, 1), (y, \pi^k), (1, \phi)\rangle$ with $\phi \in \mathrm{Aut}(N)$ satisfying $(1, \phi)(x, 1) = (x^d, \phi)$ and $(1, \phi)(y, \pi^k) = (y, \pi^k\phi)^d \in \mathrm{Hol}(N)$. This is because in G, we have $\tau\sigma_1 = \sigma_1^d\tau$ and $\tau\sigma_2 = \sigma_2^d\tau$ so τ behaves "uniformly" on the subgroup i.e. $\tau\sigma = \sigma^d\tau$ for all $\sigma \in \langle\sigma_1, \sigma_2\rangle$. Hence $\phi(x) = x^d$. To find $\phi(y)$, we need to find the "N-component" of h^d where $h = (y, \pi^k) \in \mathrm{Hol}(N)$. We have

$$h^2 = (y, \pi^k)(y, \pi^k) = (y^2x^k, \pi^{2k}),$$

$$h^3 = (y, \pi^k)(y^2x^k, \pi^{2k}) = (yx^{2k}y^2x^k = (y^3x^{3k}, \pi^{3k})$$

and

$$h^4 = (y, \pi^k)(y^3x^{3k}, \pi^{3k}) = (yx^{3k}y^3x^{3k}, \pi^{4k}) = (y^4x^{6k}, \pi^{4k}).$$

Inductively, we get

$$h^d = (y^d x^{\frac{kd(d-1)}{2}}, \pi^{kd}),$$

hence $\phi(y)$ is given by the "N-component" of this, which is $\phi(y) = x^{\frac{kd(d-1)}{2}}y^d$. Since some power of ϕ is the image of τ, ϕ should have order $p-1$. We now calculate ϕ^r for some r. We have $\phi^r(x) = x^{d^r}$ and $\phi^r(y) = x^{d^r\frac{rk(d-1)}{2}}y^{d^r}$. If $k = 0$, then ϕ has order $p-1$ but in fact $\phi = \theta$ in this case. If $k \neq 0$ then ϕ^r is equal to the identity. $p-1|r$ (to ensure that the multiplier $d^r \equiv 1 \pmod p$) and $p|r$ (to ensure that the top right entry of the matrix is zero) which is if and only if $p(p-1)|r$. Hence in this case, ϕ does not have order $p-1$. Hence if β is an embedding that satisfies $\beta(\langle\sigma_1, \sigma_2\rangle) \subseteq S$, then in fact $\beta(G) = \langle x, y, \theta\rangle$ so $\beta(\sigma_1) = x^iy^j$ for some i and j, $\beta(\sigma_2) = x^{i'}y^{j'}$ for some i' and j' and $\beta(\tau) = \theta^t$ with $gcd(t, p-1) = 1$. Using the relations in the group, we have that

$$\beta(\tau\sigma_1) = \beta(\tau)\beta(\sigma_1) = (1, \theta)(x^iy^j, 1) = (x^{itd}y^{jtd}, \theta),$$

$$\beta(\sigma_1^d\tau) = \beta(\sigma_1^d)\beta(\tau) = (x^{id}y^{jd}, 1)(1, \theta) = (x^{id}y^{id}, \theta).$$

Since these elements are both equal, this forces $t = 1$ (where t is as previously defined). □

Proposition 3.3.9. *Let $\gamma : N \to N$ be defined by $\gamma(x) = x^i y^j$ and $\gamma(y) = x^{i'} y^{j'}$. Then γ is such that $\beta = \gamma\beta_0\gamma^{-1}$.*

Proof. First, to verify that $\gamma \in \mathrm{Aut}(N)$, note that $\gamma \in \mathrm{Aut}(N)$ if and only if $ij' \neq i'j$. If $ij' = i'j$, then $Im(\gamma) \subsetneqq N$ so γ^{-1} would not be well defined. To show that γ satisfies $\beta(g) = (1, \gamma)\beta_0(g)(1, \gamma^{-1})$ for all $g \in G$, it is sufficient to check this for the generators of G, σ_1, σ_2 and τ, because the maps β and β_0 are homomorphisms. Hence, we have

$$(1, \gamma)\beta_0(\sigma_1)(1, \gamma^{-1}) = (1, \gamma)(x, 1)(1, \gamma^{-1}) = (\gamma(x), 1) = x^i y^j = \beta(\sigma_1).$$

similarly

$$(1, \gamma)\beta_0(\sigma_2)(1, \gamma^{-1}) = (1, \gamma)(y, 1)(1, \gamma^{-1}) = (\gamma(y), 1) = x^{i'} y^{j'} = \beta(\sigma_2)$$

and finally

$$(1, \gamma)\beta_0(\tau)(1, \gamma^{-1}) = (1, \gamma)(1, \theta)(1, \gamma^{-1}) = (1, \gamma\theta\gamma^{-1}) = (1, \theta) = \beta(\tau)$$

where the penultimate equality follows from the fact that $\theta \in Z(\mathrm{Aut}(N))$. □

We conclude that there is one equivalence class of embeddings satisfying $\beta(\langle\sigma_1, \sigma_2\rangle) \subseteq S$. It remains to understand how this interacts with conjugating S. More generally if β is any suitable embedding, then $\beta(\langle\sigma_1, \sigma_2\rangle) \subseteq hSh^{-1}$ for some $h \in \mathrm{Hol}(N)$.

Proposition 3.3.10. *The conjugate subgroups of S can be written as $(1, \psi)S(1, \psi^{-1})$ for some $\psi \in \mathrm{Aut}(N)$.*

Proof. Let $P = \langle\pi\rangle$ be the Sylow p-subgroup of $\mathrm{Aut}(N)$ discussed previously. Then Sylow theory tells us that the other Sylow p-subgroups of $\mathrm{Aut}(N)$ are given by $\psi P\psi^{-1}$ for some elements $\psi \in \mathrm{Aut}(N)$. If we now consider "lifting" this to $\mathrm{Hol}(N)$ (by considering $\mathrm{Hol}(N)$ as $N \rtimes \mathrm{Aut}(N)$) we see that only the "$\mathrm{Aut}(N)$-component" changes when we conjugate the subgroup and the "N-component" remains fixed i.e. we have that $S = N \rtimes P$ and $hSh^{-1} = N \rtimes \psi P\psi^{-1}$ so the elements h which conjugate S are precisely the elements $(1, \psi)$ where ψ are the elements which conjugate P. □

Corollary 3.3.11. *If $\beta : G \hookrightarrow \mathrm{Hol}(N)$ is any embedding, then β is equivalent to β_0.*

Proof. Here we are concerned with embeddings such that $Im(\beta) \subseteq hSh^{-1}$, where hSh^{-1} is a conjugate Sylow p-subgroup of S (the case $\beta(\langle\sigma_1, \sigma_2\rangle) \subseteq S$ was dealt with in Proposition 3.3.8). If $Im(\beta) \subseteq hSh^{-1}$, then using the previous proposition, we can write $h = (1, \psi)$ for some $\psi \in \mathrm{Aut}(N)$. Now conjugating by h^{-1} ensures that $Im(\psi^{-1}\beta\psi) \subseteq S$ and we can now apply the arguments in Proposition 3.3.8 to show that β is equivalent to β_0. □

In conclusion, we have now completed the proof of Proposition 3.2.1 having successfully shown that the unique almost classical Hopf-Galois structure is the only Hopf-Galois structure on the extension in the case where $r = 2$.

3.4 Properties of the almost classical Hopf-Galois structure

We now return to the case in which $L = K(\alpha_1, ..., \alpha_r)$ and study the unique almost classical Hopf-Galois structure on L/K, corresponding to the regular subgroup $N = \lambda(S)$ of $\mathrm{Perm}(X)$.

Proposition 3.4.1. *We have $H \cong K^{p^r}$ as K-algebras.*

Proof. Since $\zeta \in E$, the group algebra $E[N]$ has a basis of mutually orthogonal idempotents given by

$$e_{\boldsymbol{i}} = \frac{1}{p^r} \prod_{k=1}^{r} \sum_{n=0}^{p-1} \zeta^{-i_k n} \lambda(\sigma_k)^n$$

for $0 \leq i_k \leq p-1$ so $E[\lambda(S)] \cong E^{p^r}$ as E-algebras. We now study the action of G on $\lambda(S)$. We have

$$^{\sigma_i}(\lambda(\sigma_j)) = \lambda(\sigma_i)\lambda(\sigma_j)\lambda(\sigma_i^{-1}) = \lambda(\sigma_i\sigma_j\sigma_i^{-1}) = \lambda(\sigma_j)$$

for all i and j and

$$^{\tau}(\lambda(\sigma_j)) = \lambda(\tau)\lambda(\sigma_j)\lambda(\tau^{-1}) = \lambda(\tau\sigma_j\tau^{-1}) = \lambda(\sigma_j)^d$$

for all j. This implies that each idempotent $e_{\boldsymbol{i}}$ is fixed by each element of G and so lies in $E[\lambda(S)]^G = H$. Therefore H has a K-basis consisting of mutually orthogonal idempotents and so $H \cong K^{p^r}$ as K-algebras. □

Corollary 3.4.2. *The Greither-Pareigis theorem implies that the action of H on L is given by*

$$\prod_{n=1}^{r}\sum_{i=0}^{p-1} c_{i_n}\eta_n^{i_n}\cdot z = \prod_{n=1}^{r}\sum_{i=0}^{p-1} c_{i_n}\eta_n^{-i_n}[\overline{1_G}](z) = \prod_{n=1}^{r}\sum_{i=0}^{p-1} c_{i_n}\overline{\sigma_n^{i_n}}(z)$$

for all $z \in L$.

Proof. This is a consequence of Theorem 2.6.14. □

Proposition 3.4.3. *The orthogonal idempotents detect the elements of L in the following way.*

$$e_{\boldsymbol{i}}(\boldsymbol{\alpha^j}) = \frac{1}{p^r}\prod_{k=1}^{r}\sum_{n=0}^{p-1}\zeta^{i_k n}\sigma_k^n(\alpha_k^{j_k}) = \begin{cases} \boldsymbol{\alpha^j} & \text{if } i_k = j_k \text{ for all } k. \\ 0 & \text{otherwise} \end{cases}$$

Proof. This is a consequence of Proposition 3.4.1 and Corollary 3.4.2. Also note that the proof of this is similar to the proof of Proposition 2.5.6. □

Chapter 4

A family of non-normal extensions of prime power degree - Ramification and rings of integers

4.1 Ramification

Recall that K is a number field in which p is unramified, and L is a degree p^r extension of K of the form $L = K(\alpha_1, ..., \alpha_r)$ with $a_i = \alpha_i^p \in K$ for each $i = 1, ..., r$.

Proposition 4.1.1. *The extension L/K is tame if and only if the elements a_i can be chosen to satisfy $a_i \equiv 1 \pmod{p^2\mathcal{O}_K}$ for each i.*

Proof. To ensure that L/K is tame, applying Proposition 2.1.9 (which states that a compositum of extensions is tame if and only if each of the subextensions is tame), then applying Proposition 2.8.2 (which states that $K(\alpha_i)/K$ is tame if and only if a_i can be chosen to satisfy $a_i \equiv 1 \pmod{p^2\mathcal{O}_K}$) we get that it is necessary and sufficient to assume that $a_i \equiv 1 \pmod{p^2\mathcal{O}_K}$ for all i. □

Henceforth we will assume that these congruences hold.

4.2 Local integral bases for $\mathfrak{p} \nmid p\mathcal{O}_K$

Proposition 4.2.1. *For $\mathfrak{p} \nmid pa_i\mathcal{O}_K$ for all i an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is*

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}} | 0 \leq i_k \leq p-1 \text{ for all } 1 \leq k \leq r \right\}.$$

Proof. In this case $\mathfrak{p}$ is unramified in each of the subextensions so we can apply arithmetic disjointness and induction to combine copies of the local integral basis from Proposition 2.8.4 and obtain the result. Note that in this case we have $r_{\mathfrak{p}}(\boldsymbol{a^i}) = 0$ but writing the integral basis in this form allows for a more unified description of the integral bases for different prime ideals $\mathfrak{p}$. □

We are now left with the case $\mathfrak{p} \nmid p\mathcal{O}_K$ and $\mathfrak{p} | a_i\mathcal{O}_K$ for some i.

Proposition 4.2.2. *For $\mathfrak{p} \nmid p\mathcal{O}_K$ and $\mathfrak{p} | a_i\mathcal{O}_K$ for some i an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by*

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}} | 0 \leq i_k \leq p-1 \text{ for all } 1 \leq k \leq r \right\}$$

Proof. First suppose that $p | v_{\mathfrak{p}}(a_i)$ for all i. Then $\mathfrak{p}$ is unramified in $K(\alpha_i)$ for all i and an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by the set of products

$$\left\{ \frac{\alpha_1^{i_1} ... \alpha_r^{i_r}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_1^{i_1})} ... \pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_r^{i_r})}} | 0 \leq i_k \leq p-1 \text{ for } 1 \leq k \leq r \right\}$$

In this case $r_{\mathfrak{p}}(a_k^{i_k}) = \frac{v_{\mathfrak{p}}(a_k^{i_k})}{p}$ for each k so we may combine the exponents obtaining

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}} | 0 \leq i_k \leq p-1 \text{ for all } 1 \leq k \leq r \right\}$$

Now suppose that $p \nmid v_{\mathfrak{p}}(a_i)$ for some i. Without loss of generality suppose that $p \nmid v_{\mathfrak{p}}(a_1)$. Then there exist n_2, ..., $n_r \in \{0, ..., p-1\}$ such that $v_{\mathfrak{p}}(a_1^{n_i} a_i) = 0$ for $i = 2, ..., r$. We can write L as the compositum of the fields $K(\alpha_1)$, $K(\alpha_1^{n_2}\alpha_2)$, ..., $K(\alpha_1^{n_r}\alpha_r)$ and these fields are arithmetically disjoint at $\mathfrak{p}$ so an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by

$$\left\{ \frac{\alpha_1^{i_1}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_1^{i_1})}} \prod_{k=2}^{r} \frac{(\alpha_1^{n_k}\alpha_k)^{i_k}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}((a_1^{n_k}a_k)^{i_k})}} \right\}.$$

We can simplify as before obtaining an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ of the form

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}} | 0 \leq i_k \leq p-1 \text{ for all } 1 \leq k \leq r \right\}$$

More specifically, we first note that since $v_{\mathfrak{p}}(a_1)$ is the only term which is not congruent to 0 modulo p, we do not get a "carry" in the floor function and we can combine the exponents of $\pi_{\mathfrak{p}}$ as expected. Now we must be able to reach a typical element,

$$\left\{ \frac{\alpha_1^{s_1} ... \alpha_r^{s_r}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_1^{s_1} ... a_r^{s_r})}} | 0 \leq i_k \leq p-1 \text{ for all } 1 \leq k \leq r \right\}$$

We can do this by first choosing each i_k to be the unique element in $\{0, ..., p-1\}$ such that $n_k i_k \equiv s_k \pmod{p}$ for $2 \leq k \leq r$ and finally choosing i_1 to be the unique element in $\{0, ..., p-1\}$ such that $\sum_{k=1}^{r} i_k \equiv s_1 \pmod{p}$. By doing this, we extract a unit power of each a_i but since these are in K already, this does not affect the extension. We can relabel the indices to rewrite the integral basis in terms of the original elements and get a basis of the following form.

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}} | 0 \leq i_k \leq p-1 \text{ for all } 1 \leq k \leq r \right\}$$

□

4.3 Local integral bases for $\mathfrak{p}|p\mathcal{O}_K$

To get an $\mathcal{O}_{K,\mathfrak{p}}$- basis of $\mathcal{O}_{L,\mathfrak{p}}$ we find an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{E,\mathfrak{p}}$ and take traces from $E_{\mathfrak{p}}$ to $L_{\mathfrak{p}}$. Recall that since E/L is tame, the trace map from $\mathcal{O}_E$ to $\mathcal{O}_L$ is surjective (see Proposition 2.1.10). Since an $\mathcal{O}_{K,\mathfrak{p}}$- basis of $\mathcal{O}_{L,\mathfrak{p}}$ and an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{E,\mathfrak{p}}$ has $p^r(p-1)$ elements, when we have taken traces of our basis of $\mathcal{O}_{E,\mathfrak{p}}$ it will certainly span $\mathcal{O}_{L,\mathfrak{p}}$ but there will be too many elements so we must resolve linear dependencies. Consequences of p being unramified in K are that $[F : K] = p - 1$ and that there is a unique prime ideal $\mathfrak{P}$ lying above $\mathfrak{p}$ (see Lemma 2.8.1 which is based on Lemma 3.1 of [Tru20]). Note that here we are using $\mathfrak{P}$ to refer to a prime ideal of F (rather than L) lying over $\mathfrak{p}$. By the Galois case, an $\mathcal{O}_{F,\mathfrak{P}}$-basis of $\mathcal{O}_{E,\mathfrak{P}}$

is given by

$$\left\{\prod_{i=1}^{r}(\frac{\alpha_i-1}{\zeta-1})^{j_i}|0\leq j_i\leq p-1 \text{ for all } 1\leq i\leq r\right\}.$$

(Since E/F is Galois, the subextensions $F(\alpha_i)$ are actually arithmetically disjoint at $\mathfrak{P}$ for all i.) Recall that since $p\mathcal{O}_F=(1-\zeta)^{p-1}\mathcal{O}_F$ (see Proposition 2.1.11), we can rewrite the $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{E,\mathfrak{p}}$ as

$$\left\{\prod_{i=1}^{r}\frac{(\alpha_i-1)^{j_i}}{p}(1-\zeta)^{p-1-j_i}\zeta^k|0\leq j_i\leq p-1 \text{ for all } 1\leq i\leq r, 0\leq k\leq p-2\right\}.$$

Proposition 4.3.1. *An $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by the following elements,*

$$\begin{array}{ll}\prod_{i=1}^{r}\alpha_i^{j_i} & \text{for } \sum_{i=1}^{r}j_i<p-1\\ \frac{\prod_{i=1}^{r}(\alpha_i-1)^{j_i}}{p^Q} & \text{for } p-1\leq\sum_{i=1}^{r}j_i<r(p-1)\\ \frac{1}{p^r}(1+\alpha_1+...+\alpha_1^{j_1})...(1+\alpha_r+...+\alpha_r^{j_r}) & \text{for } j_1+...+j_r=r(p-1)\end{array}$$

where Q is a function of j_1, ..., j_r obtained by using the Euclidean division algorithm to write $j_1+...+j_r=Q(p-1)+R$ with $0\leq R<p-1$.

Proof. In this proof we will write Tr as a shorthand for $\mathrm{Tr}_{E/L}$. We wish to calculate

$$\mathrm{Tr}(\frac{\prod_{i=1}^{r}(\alpha_i-1)^{j_i}}{p}(1-\zeta)^{p-1-j_i}\zeta^k)$$

Since $\frac{\prod_{i=1}^{r}(\alpha_i-1)^{j_i}}{p}\in L$, we can simplify the trace as follows.

$$\frac{\prod_{i=1}^{r}(\alpha_i-1)^{j_i}}{p}\,\mathrm{Tr}((1-\zeta)^{r(p-1)-\sum_{i=1}^{r}j_i}\zeta^k)$$

Using binomial expansion and linearity of the trace, this becomes the following.

$$\frac{\prod_{i=1}^{r}(\alpha_i-1)^{j_i}}{p}\sum_{n=0}^{r(p-1)-\sum_{i=1}^{r}j_i}\binom{r(p-1)-\sum_{i=1}^{r}j_i}{n}(-1)^n\,\mathrm{Tr}(\zeta^{k+n})$$

An $\mathcal{O}_{F,\mathfrak{P}}$- basis of $\mathcal{O}_{E,\mathfrak{P}}$ consists of elements of the form

$$\frac{\prod_{i=1}^{r}(\alpha_i-1)^{j_i}}{(\zeta-1)^{\sum_{i=1}^{r}j_i}}.$$

We can use the Euclidean division algorithm to write $j_1 + ... + j_r = Q(p-1) + R$ with $0 \leq R < p-1$. This allows us to rewrite the $\mathcal{O}_{F,\mathfrak{P}}$- basis of $\mathcal{O}_{E,\mathfrak{P}}$ (up to units of $\mathcal{O}_{F,\mathfrak{p}}$) as

$$\frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^{Q+1}}(1-\zeta)^{p-1-R}.$$

To get an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{E,\mathfrak{p}}$, we observe that an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{F,\mathfrak{P}}$ is given by $\{1, \zeta, ..., \zeta^{p-2}\}$ (see Lemma 3.1 of [Tru20]). Hence an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{E,\mathfrak{p}}$ is given by

$$\left\{ \frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^{Q+1}}(1-\zeta)^{p-1-R}\zeta^k | 1 \leq i \leq r, 0 \leq j \leq p-1, 0 \leq k \leq p-2 \right\}.$$

As we expected, there are $p^r(p-1)$ elements here. We now proceed to take traces. First suppose that $j_1 + ... + j_r < r(p-1)$. In this case we obtain the following.

$$\mathrm{Tr}(\frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^{Q+1}}(1-\zeta)^{p-1-R}\zeta^k)$$

Since $\frac{\prod_{i=1}^{r}(\alpha_i-1)^{j_i}}{p^{Q+1}} \in L$, we can simplify the trace as follows

$$\frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^{Q+1}} \mathrm{Tr}((1-\zeta)^{p-1-R}\zeta^k)$$

Using binomial expansion and linearity of the trace, this becomes the following

$$\frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^{Q+1}} \sum_{n=0}^{p-1-R} \binom{p-1-R}{n} (-1)^n \mathrm{Tr}(\zeta^{k+n})$$

Evaluating the trace, this becomes

$$\begin{aligned} &\frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^{Q+1}}((\binom{p-1-R}{p-k}(-1)^{p-k}p - \sum_{n=0}^{p-1-R}\binom{p-1-R}{n}(-1)^n) \\ &= (-1)^{p-k}\binom{p-1-R}{p-k}\frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^Q} \end{aligned}$$

Since $(-1)^{p-k}\binom{p-1-R}{p-k} \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$, the span of these traces is equal to the span of

$$\begin{aligned} &\prod_{i=1}^{r}\alpha_i^{j_i} && \text{for } \sum_{i=1}^{r} j_i < p-1 \\ &\frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^Q} && \text{for } p-1 \leq \sum_{i=1}^{r} j_i < r(p-1) \end{aligned}$$

Now we consider the case $j_i = p-1$ for all i. For any $0 \leq k \leq p-2$, we have

$$\mathrm{Tr}\left(\frac{\prod_{i=1}^{r}(\alpha_i-1)^{p-1}}{p^r}\zeta^k\right) = \begin{cases} \frac{(p-1)\prod_{i=1}^{r}(\alpha_i-1)^{p-1}}{p^r} & \text{if } k=0 \\ -\frac{\prod_{i=1}^{r}(\alpha_i-1)^{p-1}}{p^r} & \text{otherwise} \end{cases}$$

Therefore $\frac{\prod_{i=1}^{r}(\alpha_i-1)^{p-1}}{p^r} \in \mathcal{O}_{L,\mathfrak{p}}$ and using the fact that $\binom{p-1}{n} \equiv (-1)^n \pmod{p}$, we have

$$\frac{1}{p^r}\prod_{i=1}^{r}\sum_{n=0}^{p-1}\alpha_i^n \in \mathcal{O}_{L,\mathfrak{p}}.$$

To prove linear independence, since we end up with p^r elements if they span $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{O}_{K,\mathfrak{p}}$ then they span $L_\mathfrak{p}$ over $K_\mathfrak{p}$, so by a dimension argument they form a basis of $L_\mathfrak{p}$ over $K_\mathfrak{p}$, so they must be linearly independent over $K_\mathfrak{p}$, hence over $\mathcal{O}_{K,\mathfrak{p}}$. We conclude that the set in the proposition is indeed an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$. □

4.4 Associated order and local generators

The aim of this section is to prove the following theorem

Theorem 4.4.1. *The ring of integers $\mathcal{O}_L$ is locally free over $\mathcal{A}_H$ in the unique almost classical Hopf-Galois structure.*

The proof of this theorem will take the form of a sequence of propositions. Recall the information on orders from the background chapter, in particular Theorem 2.3.7 which gives some properties of maximal orders. We will study the associated order by relating it to the fixed points of the group ring $\mathcal{O}_E[N]^G$. In fact, we will show that $\mathcal{A}_H = \mathcal{O}_E[N]^G$. Recall from Proposition 2.7.3 that $\mathcal{O}_E[N]^G \subseteq \mathcal{A}_H$.

Proposition 4.4.2. *If $\mathfrak{p} \nmid p\mathcal{O}_K$, then each $e_{\boldsymbol{i}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G$ so $\mathcal{O}_{E,\mathfrak{p}}[N]^G = \mathcal{A}_{H,\mathfrak{p}} = \mathcal{M}_\mathfrak{p}$ and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module.*

Proof. See Proposition 2.7.4 which is based on Theorem 5.8 of [Tru11]. □

To determine the associated order for prime ideals $\mathfrak{p}|p\mathcal{O}_K$, we will use the "all in one" approach (recall Theorem 2.7.5). We will denote the elements of the $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ by $x_{\boldsymbol{j}}$. That is,

$$\text{for } \sum_{i=1}^{r} j_i < p-1, \text{ we have } x_{\boldsymbol{j}} = \prod_{i=1}^{r}\alpha_i^{j_i},$$

$$\text{for } p-1 \leq \sum_{i=1}^{r} j_i < r(p-1) \text{ we have } x_{\boldsymbol{j}} = \frac{\prod_{i=1}^{r}(\alpha_i - 1)^{j_i}}{p^Q},$$

$$\text{for } \sum_{i=1}^{r} j_i = r(p-1) \text{ we have } x_{\boldsymbol{p-1}} = \frac{1}{p^r}(1+\alpha_1+...+\alpha_1^{p-1})...(1+\alpha_r+...+\alpha_r^{p-1}).$$

Proposition 4.4.3. *For $\mathfrak{p}|p\mathcal{O}_K$ we have $\mathcal{A}_{H,\mathfrak{p}} = \mathcal{O}_{E,\mathfrak{p}}[N]^G$ and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module.*

Proof. Firstly, we will take

$$x = x_{\boldsymbol{p-1}} = \frac{1}{p^r}(1+\alpha_1+...+\alpha_1^{p-1})...(1+\alpha_r+...+\alpha_r^{p-1})$$

as a candidate generator. To check that x generates L as an H-module, note that $e_{\boldsymbol{j}} \cdot x = \boldsymbol{\alpha^j}$ and this sets spans L. To simplify notation, we will write $Q(\sum j_i)$ for $Q(j_1+...+j_r)$ and later we will write $Q(\sum l_k)$ for $Q(l_1+...+l_r)$. Recall that we can use the element x to define elements $a_{\boldsymbol{j}} \in H_{\mathfrak{p}}$ by the rule $a_{\boldsymbol{j}} \cdot x = x_{\boldsymbol{j}}$. Explicitly

$$\begin{aligned}
a_{\boldsymbol{j}} &= p^r e_{\boldsymbol{j}} && \text{for } \sum_{i=1}^{r} j_i < p-1, \\
a_{\boldsymbol{j}} &= p^{r-Q(\sum \boldsymbol{j})} \sum_{i=1}^{r} \sum_{n_i=0}^{p-1} \prod_{i=1}^{r} \binom{j_i}{n_i} (-1)^{j_i-n_i} e_{\boldsymbol{n}} && \text{for } p-1 \leq \sum_{i=1}^{r} j_i < r(p-1) \\
a_{\boldsymbol{j}} &= 1 && \text{for } \sum_{i=1}^{r} j_i = r(p-1).
\end{aligned}$$

To determine whether $a_{\boldsymbol{j}} \in \mathcal{A}_{H,\mathfrak{p}}$ we will study the fixed group ring $\mathcal{O}_{E,\mathfrak{p}}[N]^G$. We have $H = E[N]^G$ where $N = \lambda(S)$. Inside H we have the order $\mathcal{O}_E[N]^G$. We know that $\mathcal{O}_E[N]^G \subseteq \mathcal{A}_H$ or equivalently $\mathcal{O}_{E,\mathfrak{p}}[N]^G \subseteq \mathcal{A}_{H,\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$.

For $\mathfrak{p}|p\mathcal{O}_K$, we have written down elements $a_{\boldsymbol{j}} \in H_{\mathfrak{p}}$ such that $a_{\boldsymbol{j}} \cdot x = x_{\boldsymbol{j}}$. We aim to determine whether these elements have integral coefficients i.e. whether the coefficient of $\lambda(\boldsymbol{\sigma^i})$ is in $\mathcal{O}_{E,\mathfrak{p}}$ for each $\boldsymbol{i}$. If so(i. e. if $a_{\boldsymbol{j}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G$), then this is sufficient to show that $a_{\boldsymbol{j}} \in \mathcal{A}_{H,\mathfrak{p}}$ and we get $\mathcal{A}_H = \mathcal{O}_E[N]^G$ (globally).

It is straightforward to see that $a_{\boldsymbol{j}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G$ for $\sum \boldsymbol{j} < p-1$ and $\sum \boldsymbol{j} = r(p-1)$. Now note that for $p-1 \leq \sum \boldsymbol{j} < r(p-1)$ we have

$$a_{\boldsymbol{j}} = p^{r-Q(\sum \boldsymbol{j})} \sum_{m=1}^{r} \sum_{n_m=0}^{p-1} \prod_{i=1}^{r} \binom{j_i}{n_i} (-1)^{j_i-n_i} e_{\boldsymbol{n}}.$$

Substituting in the expression for the orthogonal idempotent, we get

$$a_{\boldsymbol{j}} = p^{-Q(\sum \boldsymbol{j})} \sum_{m=1}^{r} \sum_{n_m=0}^{p-1} \prod_{i=1}^{r} \binom{j_i}{n_i} (-1)^{j_i - n_i} \sum_{s=0}^{p-1} \prod_{k=1}^{r} \zeta^{-n_k s_k} \lambda(\boldsymbol{\sigma}^{\boldsymbol{s}})$$

We can rewrite this expression using the bold notation to obtain

$$a_{\boldsymbol{j}} = p^{-Q(\sum \boldsymbol{j})} \sum_{\boldsymbol{n}} \prod_{i=1}^{r} \binom{j_i}{n_i} (-1)^{j_i - n_i} \prod_{k=1}^{r} \sum_{\boldsymbol{s}} \zeta^{-n_k s_k} \lambda(\boldsymbol{\sigma}^{\boldsymbol{s}})$$

We will move the sum over $\boldsymbol{s}$ to the front of the expression to obtain

$$a_{\boldsymbol{j}} = \sum_{\boldsymbol{s}} (p^{-Q(\sum \boldsymbol{j})} \sum_{\boldsymbol{n}} \prod_{i=1}^{r} \binom{j_i}{n_i} (-1)^{j_i - n_i} \prod_{k=1}^{r} \zeta^{-n_k s_k}) \lambda(\boldsymbol{\sigma}^{\boldsymbol{s}})$$

For all possible values of $\boldsymbol{s} = (s_1, ..., s_r)$, the coefficient of $\lambda(\boldsymbol{\sigma}^{\boldsymbol{s}})$ in the above expression is equal to the expression in the brackets, which is

$$p^{-Q(\sum \boldsymbol{j})} \sum_{\boldsymbol{n}} \prod_{i=1}^{r} \binom{j_i}{n_i} (-1)^{j_i - n_i} \prod_{k=1}^{r} \zeta^{-n_k s_k}.$$

Observing that there are no cross terms, we can combine the two products in this expression using a single index to get

$$p^{-Q(\sum \boldsymbol{j})} \sum_{\boldsymbol{n}} \prod_{i=1}^{r} \binom{j_i}{n_i} (-1)^{j_i - n_i} \zeta^{-n_i s_i}.$$

Now notice that for all $i = 1, ..., r$ each individual term of the product can be written as a binomial expansions as follows.

$$p^{-Q(\sum \boldsymbol{j})} \prod_{i=1}^{r} (\zeta^{-s_i} - 1)^{j_i}.$$

Now since $\zeta^{-s_i} - 1$ and $\zeta - 1$ differ by a unit of $\mathcal{O}_{K,\mathfrak{p}}$ and also p and $(\zeta - 1)^{p-1}$ differ by a unit of $\mathcal{O}_{K,\mathfrak{p}}$, the above expression is equal to (up to units)

$$\frac{(\zeta - 1)^{\sum \boldsymbol{j}}}{(\zeta - 1)^{(p-1)Q(\sum \boldsymbol{j})}}.$$

Since $(p-1)Q(\sum \boldsymbol{j}) \leq \sum \boldsymbol{j}$ by construction of Q, the above experssion lies in $\mathcal{O}_{E,\mathfrak{p}}$ and we have $\mathcal{O}_{E,\mathfrak{p}}[N]^G = \mathcal{A}_{H,\mathfrak{p}}$ as claimed. □

Since $a_{\boldsymbol{j}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G$ for all $\boldsymbol{j}$ and $\mathcal{O}_{E,\mathfrak{p}}[N]^G \subseteq \mathcal{A}_{H,\mathfrak{p}}$, we have $a_{\boldsymbol{j}} \cdot x_{\boldsymbol{i}} \in \mathcal{O}_{L,\mathfrak{p}}$ for all $\boldsymbol{i}$ and $\boldsymbol{j}$ (so we do not need to check this explicitly). Hence $\mathcal{A}_{H,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}\langle a_{\boldsymbol{j}} \rangle = \mathcal{O}_{E,\mathfrak{p}}[N]^G$ but $\mathcal{A}_{H,\mathfrak{p}} \neq \mathcal{M}_{\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}\langle e_{\boldsymbol{n}} \rangle$.

We have achieved our aim of proving Theorem 4.4.1, that the ring of integers $\mathcal{O}_L$ is locally free over $\mathcal{A}_H$ in the unique almost classical Hopf-Galois structure.

We need explicit local generators of $\mathcal{A}_{H,\mathfrak{p}}$ over $\mathcal{O}_{L,\mathfrak{p}}$ in order to apply the idèlic theory in the following section. We have shown that for prime ideals $\mathfrak{p}|p\mathcal{O}_K$, a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{A}_{H,\mathfrak{p}}$ is given by $x_\mathfrak{p} = \frac{1}{p^r}(1+\alpha_1+...+\alpha_1^{p-1})...(1+\alpha_r+...+\alpha_r^{p-1})$ (see Proposition 4.4.3).

Proposition 4.4.4. *For prime ideals $\mathfrak{p} \nmid p\mathcal{O}_K$, the element $x_\mathfrak{p} = \frac{1}{p^r}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha^i}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a^i})}}$ is a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{A}_{H,\mathfrak{p}}$.*

Proof. For prime ideals $\mathfrak{p} \nmid p\mathcal{O}_K$, since the associated order coincides with the maximal order and we have $\mathcal{A}_{H,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}\langle e_{\boldsymbol{i}}\rangle$. If we consider summing the basis elements i.e. we take $x_\mathfrak{p} = \frac{1}{p^r}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha^i}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a^i})}}$ as stated in the proposition, we can use these orthogonal idempotents to detect each of the terms in the sum and recover the local integral basis, hence our element $x_\mathfrak{p}$ as given above is a local generator. □

4.5 Using idèlic theory to move from local to global freeness

In the previous sections we have shown that $\mathcal{O}_L$ is locally free over $\mathcal{A}_H$ and given an explicit generator of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{A}_{H,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathcal{O}_K$. In this section we determine a criterion for $\mathcal{O}_L$ to be a free $\mathcal{A}_H$-module. Our main tool will be a theorem of Bley and Johnston, Theorem 2.4.16. Recall from Proposition 3.4.1 that we have an isomorphism of K-algebras $H \cong K^{p^r}$ arising from the fact that H has a K-basis of mutually orthogonal idempotents. This isomorphism implies that H contains a unique maximal order $\mathcal{M}$ given by

$$\mathcal{M} = \mathcal{O}_K\langle e_{\boldsymbol{i}} | 0 \leq i_k \leq p-1 \text{ for each } 1 \leq k \leq r\rangle.$$

We write $\mathcal{M}\mathcal{O}_L$ for the smallest $\mathcal{M}$-module in L containing $\mathcal{O}_L$. Explicitly

$$\mathcal{M}\mathcal{O}_L = \left\{ \sum_{\text{finite}} z \cdot x | z \in \mathcal{M}, x \in \mathcal{O}_L \right\}.$$

Theorem 2.4.16 implies that $\mathcal{O}_L$ is a free $\mathcal{A}_H$-module if and only if $\mathcal{M}\mathcal{O}_L$ is a free $\mathcal{M}$-module with a generator lying in $\mathcal{O}_L$. Our strategy will be to determine a criterion for $\mathcal{M}\mathcal{O}_L$ to be a free $\mathcal{M}$-module and then a further criterion for it to have a generator in $\mathcal{O}_L$. For the first of these, note that $\mathcal{M}\mathcal{O}_L$ is a locally free $\mathcal{M}$-module and recall from Section 2.4 that since H is commutative, $\mathcal{O}_L$ is a free $\mathcal{M}$-module if and only if it has trivial class in the locally free class group $\mathrm{Cl}(\mathcal{M})$. Also recall from Theorem 2.4.10 that we have an isomorphism

$$\mathrm{Cl}(\mathcal{M}) \cong \frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathcal{M})}.$$

Proposition 4.5.1. *The class of $\mathcal{M}\mathcal{O}_L$ in $\mathrm{Cl}(\mathcal{M})$ corresponds to the class of the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ where*

$$h_{\mathfrak{p}} = \sum_{\boldsymbol{i}} \frac{e_{\boldsymbol{i}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}}.$$

Proof. Let $x = \frac{1}{p^r}(1+\alpha_1+...+\alpha_1^{p-1})...(1+\alpha_r+...+\alpha_r^{p-1}) \in \mathcal{O}_L$. Then x generates L as a free H-module. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ let $x_{\mathfrak{p}}$ be the free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{A}_{H,\mathfrak{p}}$-module found in Propositions 4.4.3 and 4.4.4. That is

$$x_{\mathfrak{p}} = \begin{cases} \frac{1}{p^r}(1+\alpha_1+...+\alpha_1^{p-1})...(1+\alpha_r+...+\alpha_r^{p-1}) & \text{if } \mathfrak{p}|p\mathcal{O}_K \\ \frac{1}{p^r}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}} & \text{otherwise} \end{cases}$$

For each $\mathfrak{p}$, we have $(\mathcal{M}\mathcal{O}_L)_{\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}}\mathcal{O}_{L,\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}}(\mathcal{A}_{H,\mathfrak{p}} \cdot x_{\mathfrak{p}}) = \mathcal{M}_{\mathfrak{p}} \cdot x_{\mathfrak{p}}$ so the element $x_{\mathfrak{p}}$ given above is a free generator of $(\mathcal{M}\mathcal{O}_L)_{\mathfrak{p}}$ as an $\mathcal{M}_{\mathfrak{p}}$-module. Now, as described in Section 2.4, the element $h_{\mathfrak{p}} \in H_{\mathfrak{p}}$ is defined by $h_{\mathfrak{p}} \cdot x = x_{\mathfrak{p}}$. Recalling (from Corollary 3.4.2) the formulae for the actions of the orthogonal idempotents on elements of L, we find

$$h_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \mathfrak{p}|p\mathcal{O}_K \\ \sum_{\boldsymbol{i}} \frac{e_{\boldsymbol{i}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}} & \text{otherwise} \end{cases}$$

Finally note that if $\mathfrak{p}|p\mathcal{O}_K$, then $v_{\mathfrak{p}}(a_k) = 0$ for all k and $\sum_{\boldsymbol{i}} e_{\boldsymbol{i}} = 1$ so we may combine the expressions above into the single expression in the statement of the proposition. □

Since $H \cong K^{p^r}$ as K-algebras we have $\mathcal{M} \cong \mathcal{O}_K^{p^r}$ as $\mathcal{O}_K$-orders and so

$$\frac{\mathbb{J}(H)}{H^\times \mathbb{U}(\mathcal{M})} \cong \left(\frac{\mathbb{J}(K)}{K^\times \mathbb{U}(\mathcal{O}_K)}\right)^{p^r}.$$

Now

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

the ideal class group of K via $(z_\mathfrak{p})_\mathfrak{p} \to \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(z_\mathfrak{p})}$. Thus each element of

$$\frac{\mathbb{J}(H)}{H^\times \mathbb{U}(\mathcal{M})}$$

corresponds to a p^r-tuple of fractional ideals of K.

Proposition 4.5.2. *The idèle $(h_\mathfrak{p})_\mathfrak{p}$ corresponding to the class of $\mathcal{M}\mathcal{O}_L$ in $\mathrm{Cl}(\mathcal{M})$ corresponds to the p^r-tuple of classes of ideals $\mathfrak{a}_{\boldsymbol{i}}^{-1}$ where*

$$\mathfrak{a}_{\boldsymbol{i}} = \prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}.$$

Proof. Recall from Proposition 2.4.14 and Corollary 2.4.15 that to obtain the tuple of ideal classes corresponding to an idèle $(z_\mathfrak{p})_\mathfrak{p}$ we write

$$z_\mathfrak{p} = \sum_{\boldsymbol{i}} c_{\boldsymbol{i},\mathfrak{p}} e_{\boldsymbol{i}}$$

with $c_{\boldsymbol{i},\mathfrak{p}} \in K_\mathfrak{p}$ for all i. Then the idèle $(h_\mathfrak{p})_\mathfrak{p}$ is mapped to the p^r-tuple of classes of fractional ideals $(\mathfrak{c}_{\boldsymbol{i}})$ where

$$\mathfrak{c}_{\boldsymbol{i}} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(c_{\boldsymbol{i},\mathfrak{p}})}.$$

Applying this to the idèle $(h_\mathfrak{p})_\mathfrak{p}$ corresponding to the class of $\mathcal{M}\mathcal{O}_L$ in $\mathrm{Cl}(\mathcal{M})$ (constructed in the previous proposition) we see that

$$\mathfrak{c}_{\boldsymbol{i},\mathfrak{p}} = \frac{1}{\pi_\mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}}$$

for all $\boldsymbol{i}$ and $\mathfrak{p}$. Hence $(h_\mathfrak{p})_\mathfrak{p}$ corresponds to the p^r-tuple of ideal classes $(\mathfrak{a}_{\boldsymbol{i}})^{-1}$ where

$$\mathfrak{a}_{\boldsymbol{i}} = \prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}$$

for all $\boldsymbol{i}$. □

Corollary 4.5.3. *The $\mathcal{M}$-module $\mathcal{M}\mathcal{O}_L$ is free if and only if the ideals $\mathfrak{a}_{\boldsymbol{i}}$ are principal for all $\boldsymbol{i}$.*

Proposition 4.5.4. *The $\mathcal{M}$-module $\mathcal{M}\mathcal{O}_L$ has a free generator lying in $\mathcal{O}_L$ if and only if the ideals $\mathfrak{a}_{\boldsymbol{i}}$ are principal for all $\boldsymbol{i}$ with generators $a_{\boldsymbol{i}}$ such that*

$$\frac{1}{p^r}\sum_{\boldsymbol{i}}\frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{a_{\boldsymbol{i}}} \in \mathcal{O}_L.$$

Proof. By the previous proposition $\mathcal{M}\mathcal{O}_L$ is a free $\mathcal{M}$-module if and only if each ideal $\mathfrak{a}_{\boldsymbol{i}}$ is principal. Suppose that this is the case and write $\mathfrak{a}_{\boldsymbol{i}} = c_{\boldsymbol{i}}\mathcal{O}_K$ for some $c_{\boldsymbol{i}} \in \mathcal{O}_K$. Then a free generator for $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module is

$$y = \frac{1}{p^r}\sum_{\boldsymbol{i}}\frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{c_{\boldsymbol{i}}}.$$

The set of free generators of $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module is precisely the set $\{z \cdot y | z \in \mathcal{M}^\times\}$. Since $\mathcal{M} \cong \mathcal{O}_K^{p^r}$ via orthogonal idempotents and $e_{\boldsymbol{i}} \cdot \boldsymbol{\alpha}^{\boldsymbol{j}} = \delta_{\boldsymbol{i},\boldsymbol{j}}\boldsymbol{\alpha}^{\boldsymbol{j}}$ we see that an element $y' \in L$ is a free generator for $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module if and only if it has the form

$$y' = \frac{1}{p^r}\sum_{\boldsymbol{i}}\frac{u_{\boldsymbol{i}}\boldsymbol{\alpha}^{\boldsymbol{i}}}{c_{\boldsymbol{i}}}$$

for some $u_{\boldsymbol{i}} \in \mathcal{O}_K^\times$. Therefore $\mathcal{M}\mathcal{O}_L$ has a free generator lying in $\mathcal{O}_L$ if and only if there exist elements $u_{\boldsymbol{i}} \in \mathcal{O}_K^\times$ such that the corresponding element y' lies in $\mathcal{O}_L$. Writing $a_{\boldsymbol{i}} = u_{\boldsymbol{i}}^{-1}c_{\boldsymbol{i}}$ for each $\boldsymbol{i}$, this is equivalent to the existence of elements $a_{\boldsymbol{i}}$ as in the statement of the proposition. □

By combining the results of this section, we obtain a criterion for $\mathcal{O}_L$ to be a free $\mathcal{A}_H$-module:

Theorem 4.5.5. *Let p be an odd prime number, let K be a number field such that p is unramified in K, and let L be a tamely ramified extension of K of degree p^r for some positive integer r having the form $L = K(\delta_1, ..., \delta_r)$ for some $\delta_i \in L$ such that each $\delta_i^p \in K$. Let H be the Hopf algebra giving the unique almost classical Hopf-Galois structure on L/K. The ring of algebraic integers $\mathcal{O}_L$ is a free $\mathcal{A}_H$-module if and only if there exist β_1, ..., $\beta_r \in \mathcal{O}_L$ such that*

1. $L = K(\beta_1, ..., \beta_r)$

2. $b_i = \beta_i^p \in \mathcal{O}_K$ *for each* i

3. *The ideals* $\mathfrak{b}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\boldsymbol{b^i})}$ *are principal with generators* $c_{\boldsymbol{i}}$ *such that* $y = \frac{1}{p^r} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\beta^i}}{c_{\boldsymbol{i}}} \in \mathcal{O}_L$.

Furthermore in this case the element y *is a free generator of* $\mathcal{O}_L$ *as an* $\mathcal{A}_H$*-module.*

Proof. If $\mathcal{O}_L$ is a free $\mathcal{A}_H$-module then by Theorem 2.4.16 we have $\mathcal{M}\mathcal{O}_L = \mathcal{M} \cdot x$ for some $x \in \mathcal{O}_L$. Therefore by the previous proposition the ideals $\prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}$ are principal for all $\boldsymbol{i}$ with generators $b_{\boldsymbol{i}}$ satisfying

$$\frac{1}{p^r} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha^i}}{b_{\boldsymbol{i}}} \in \mathcal{O}_L.$$

Therefore the elements $\beta_i = \alpha_i$ for each i satisfy *1.*, *2.* and *3.* To prove the converse, the same argument used in the proof of Theorem 2.5.25 applies here. □

Chapter 5

A family of non-normal simple radical extensions of square free degree - Field theory and Hopf-Galois structures

5.1 Setup for an extension of degree m

Let K be a number field and let m be an odd square free positive integer. Let ζ_m be a primitive m^{th} root of unity. Suppose that all primes $p|m$ are unramified in K. Note that this implies that $\zeta_m \notin K$ and that $[K(\zeta_m) : K] = \phi(m)$. Let $d \in K$ be such that $x^m - d$ is irreducible over K.

Proposition 5.1.1. *The polynomial $x^m - d$ is irreducible over K if and only if $x^p - d$ is irreducible over K for all $p|m$, i.e. $d \notin K^p$ for $p|m$.*

Proof. See Theorem 13.1.5 of [Rom05]. □

Henceforth, we will write $m = p_1...p_r$ for the prime factorisation of m and we will write ζ_i for a p_i^{th} root of unity. Let δ be a root of $x^m - d$, let $L = K(\delta)$ and let $F = K(\zeta_m)$. For $i = 1, ..., r$, let $\alpha_i = \delta^{\frac{m}{p_i}}$ (so $\alpha_i^{p_i} \in K$ but $\alpha_i \notin K$).

Proposition 5.1.2. *In this notation, we have $L = K(\alpha_1, ..., \alpha_r)$.*

Proof. It is clear to see that $K(\alpha_1, ..., \alpha_r) \subseteq K(\delta)$. For the reverse inclusion, write $q_i = \frac{m}{p_i}$ for each i. Then there exist $u_i \in \mathbb{Z}$ such that $u_1 q_1 + ... + u_r q_r = 1$. Then $\alpha_1^{u_1} ... \alpha_r^{u_r} \delta^{u_1 q_1 + ... + u_r q_r} = \delta$ which completes the proof. □

Let E be the Galois closure of L/K. We will now aim to determine the degree $[E : K]$. We show this by writing $E = F(\delta) = K(\zeta_m)(\delta)$. Firstly we aim to show that the extension E/F has degree m. Note that the minimal polynomial of α_i over K is $x^{p_i} - d$. We can also write $E = F(\alpha_1, ..., \alpha_r)$. Each of the extensions $F(\alpha_i)/F$ has degree dividing p_i (i.e. either p_i or 1).

Proposition 5.1.3. *Each of the extensions $F(\alpha_i)/F$ has degree p_i.*

Proof. If $[F(\alpha_i) : F] \neq p_i$ for some i, then $x^{p_i} - d$ is not the minimal polymial of α_i over F. Hence $x^{p_i} - d$ is reducible over F. The polynomial $x^{p_i} - d$ is reducible over F if and only if it has a root in F. (see Theorem 13.1.5 of [Rom05]). Since $\zeta_{p_i} \in F$, once $x^{p_i} - d$ has *a* root in F, it splits into linear factors in F. Hence $[F(\alpha_i) : F] = 1$ and $K(\zeta_{p_i}, \alpha_i) \subseteq F$. However F/K is Galois with abelian Galois group and $K(\zeta_{p_i}, \alpha_i)/K$ is Galois with non-abelian Galois group (see [Rom05]). Since it is impossible for an abelian group to have a non-abelian quotient, we have a contradicition. Hence $[F(\alpha_i) : F] = p_i$ as claimed. □

Proposition 5.1.4. $[E : K] = m\phi(m)$.

Proof. By Proposition 5.1.3 we have $[E : F]$ is divisible by $p_1, ..., p_r$, hence is divisble by m and hence $[E : F] = m$. We can now apply the tower law to conclude that $[E : K] = m\phi(m)$ as claimed. □

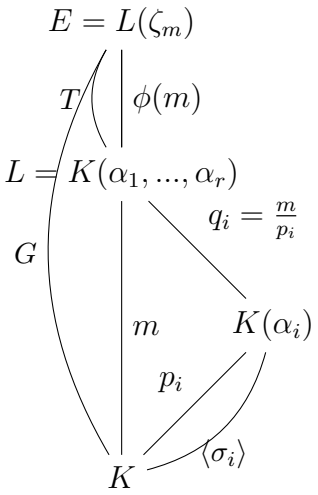
Remark 5.1.5. *Note that in the proof of Proposition 5.1.3, we showed that the polynomials $x^{p_i} - d$ are irreducible over F, hence the polynomial $x^m - d$ is irreducible over F.*

The Galois group of E/K is given by $G = \text{Gal}(E/K) = \langle \sigma_1, ..., \sigma_r, \tau_1, ..., \tau_r \rangle$ where

$$\sigma_i(\alpha_i) = \zeta_i \alpha_i,\ \sigma_i(\alpha_j) = \alpha_j \text{ for } i \neq j,\ \sigma_i(\zeta_j) = \zeta_j \text{ for all } i \text{ and } j,$$

$$\tau_i(\alpha_j) = \alpha_j \text{ for all } i \text{ and } j,\ \tau_i(\zeta_i) = \zeta_i^{d_i} \text{ where } d_i \text{ is a primitive root modulo } p_i$$

$$\text{and } \tau_i(\zeta_j) = \zeta_j \text{ for } i \neq j.$$



5.2 The almost classical Hopf-Galois structure

Henceforth, we will write $S = \langle\sigma_1, ..., \sigma_r\rangle$ and $T = \langle\tau_1, ..., \tau_r\rangle$.

Proposition 5.2.1. *The extension L/K is almost classically Galois.*

Proof. The field L is the fixed field E^T and T has a normal complement in G (namely S). □

Hence $\lambda(S) \subseteq \mathrm{Perm}(X)$ gives an almost classical Hopf-Galois structure on the extension.

To describe the corresponding embedding, write $N \cong C_{p_1} \times ... \times C_{p_r} = \langle\eta_1\rangle \times ... \times \langle\eta_r\rangle$. In this case $\mathrm{Aut}(N) \cong C_m^\times \cong C_{p_1}^\times ... \times C_{p_r}^\times$ via the description $\mathrm{Aut}(N) = \langle\phi_1, ..., \phi_r\rangle$ where $\phi_i(\eta_i) = \eta_i^{d_i}$ where d_i is a primitive root modulo p_i and $\phi_i(\eta_j) = \eta_j$ for $i \neq j$.

The corresponding embedding is given by $\beta(\sigma_i) = (\eta_i, id)$, $\beta(\tau_i) = (e, \phi_i)$.

Proposition 5.2.2. *The embedding given above corresponds to the Hopf-Galois structure given by $\lambda(S)$.*

Proof. For $1 \leq i \leq r$ let $\eta_i \in \mathrm{Perm}(X)$ be defined by $\eta_i(\overline{\sigma_1^{j_1}...\sigma_r^{j_r}}) = \overline{\sigma_1^{j_1}...\sigma_i^{j_i-1}...\sigma_r^{j_r}}$. Recall that by construction the map $\alpha(\eta_1^{j_1}...\eta_r^{j_r})$ is given by $b^{-1}\lambda_N(\eta_1^{j_1}...\eta_r^{j_r})b$. In this case the map b is given by $b(\overline{g}) = \beta(g)e_N$. Hence if we consider a typical element of G $\sigma_1^{s_1}...\sigma_r^{s_r}$ we have $\alpha(\eta_1^{j_1}...\eta_r^{j_r})[\overline{\sigma_1^{s_1}...\sigma_r^{s_r}}] = b^{-1}\lambda_N(\eta_1^{j_1}...\eta_r^{j_r})b[\overline{\sigma_1^{s_1}...\sigma_r^{s_r}}] =$

$b^{-1}\lambda_N(\eta_1^{j_1}...\eta_r^{j_r})(\eta_1^{s_1}...\eta_r^{s_r}) = b^{-1}(\eta_1^{j_1+s_1}...\eta_r^{j_r+s_r}) = \eta_1^{-s_1}...\eta_r^{-s_r}(\overline{\sigma_1^{j_1}...\sigma_r^{j_r}})$. Hence $\alpha(N) = \langle \eta_1, ..., \eta_r \rangle \cong \lambda(S)$. □

5.3 Unique normal complement

In this section, we will prove that S is the unique normal complement of T in G directly using group theory.

Lemma 5.3.1. *For $i = 1, ..., r$, let $G_i = \langle \sigma_i, \tau_i \rangle$. Then $G_i \trianglelefteq G$ and $G \cong G_1 \times G_2 \times ... \times G_r$.*

Proof. It is clear that $G_i \leq G$ for each i and for $j \neq i$ the elements σ_j and τ_j commute with all elements of G_i. Hence $G_i \trianglelefteq G$ and $\prod_{i=1}^r G_i \leq G$. We have $G_i \cap G_j = \{e\}$ for $i \neq j$, so $|\prod_{i=1}^r G_i| = \prod_{i=1}^r |G_i| = \prod_{i=1}^r p_i(p_i - 1) = |G|$. Hence $G = \prod_{i=1}^r G_i \cong G_1 \times ... \times G_r$. □

Lemma 5.3.2. *For each $i = 1, ..., r$ the subgroup $\langle \sigma_i \rangle$ is the unique normal complement to $\langle \tau_i \rangle$ in G_i.*

Proof. It is clear to see that $\langle \sigma_i \rangle$ is a normal complement to $\langle \tau_i \rangle$ in G_i. If U_i is a normal complement to $\langle \tau_i \rangle$ in G_i then $|U_i| = p_i$, but $\langle \sigma_i \rangle$ is the unique Sylow p_i-subgroup of G_i, so $U_i = \langle \sigma_i \rangle$. □

Proposition 5.3.3. *The subgroup $S = \langle \sigma_1, ..., \sigma_r \rangle$ is the unique normal complement to $T = \langle \tau_1, ..., \tau_r \rangle$ in G.*

Proof. It is clear to see that S is a normal complement to T in G. Now suppose that U is a normal complement T in G. Then $|U| = p_1...p_r = m$. By Lemma 5.3.1 we have $G \cong G_1 \times ... \times G_r$. For each i, let $\pi_i : G \to G_i$ be the natural projection. Then for each i we have $\pi_i(T) = \langle \tau_i \rangle$ and $\pi_i(U)$ is a normal complement to $\langle \tau_i \rangle$ in G_i. By Lemma 5.3.2, $\pi_i(U) = \langle \sigma_i \rangle$. For each j the subgroup U contains an element u_j of order p_j. Now for each i the order of $\pi_i(u_j)$ divides p_j. Since $\pi_i(u_j) \in \langle \sigma_i \rangle$ for each i we find that $\pi_i(u_j) = e$ for $i \neq j$ and $\pi_j(u_j) = \sigma_j^{s_j}$ for some $s_j = 1, ..., p_j - 1$. Hence $u_j = \sigma_j^{s_j}$ and so $\sigma_j \in U$. Since this holds for each $j = 1, ..., r$ we

see that $S \subseteq U$ and comparing orders gives $S = U$. Hence S is the unique normal complement to T in G. □

5.4 Classifying the Hopf-Galois structures on the extension when $r = 2$

For this section we will change notation from p_1 and p_2 to p and q and assume that $p > q$. The aim of this section is to classify all Hopf-Galois structures on the extension of degree pq. More specifically we will prove the following proposition.

Proposition 5.4.1. *The unique almost classical Hopf-Galois structure is the only Hopf-Galois structure on the extension in the case where $r = 2$.*

Since there are only two groups of order pq, there are only two possibilities for the group N from Greither-Pareigis theory (up to isomorphism). The two possibilities for N are $N \cong C_{pq}$ and $N \cong C_p \rtimes C_q$. Note that the second possibility can only occur when $p \equiv 1 \pmod{q}$. Note that $G \cong S \rtimes T \cong C_{pq} \rtimes C_{p-1} \times C_{q-1}$. We will apply Byott's translation theorem. This tells us that we seek equivalence classes of embeddings $\beta : G \hookrightarrow \mathrm{Hol}(N)$ such that $\beta(T) = \mathrm{Stab}(e_N)$. We firstly show that all suitable embeddings when N is cyclic fall under one equivalence class. We then proceed to show that there are no suitable embedding when N is metabelian.

Proposition 5.4.2. *There is exactly one equivalence class of embeddings in the case that N is cyclic.*

The proof of this will take the form of a sequence of propositions. We will write $N \cong C_{pq} = \langle \mu, \eta | \mu^p = \eta^q = e \rangle$. (Note that we use two generators for this cyclic group to simplify the construction of the embeddings later.) In this case $\mathrm{Aut}(N) \cong C_{pq}^{\times} \cong C_p^{\times} \times C_q^{\times}$ via the automorphism $(\phi_k, \psi_l)[\mu\eta] = \mu^k \eta^l$. A typical element of $\mathrm{Hol}(N)$ is an ordered pair $(\mu^i \eta^j, \phi_k \psi_l)$. Then $|\mathrm{Hol}(N)| = |N||\mathrm{Aut}(N)| = pq(p-1)(q-1) = |G|$. In this case since $|G| = |\mathrm{Hol}(N)|$, the embeddings that we are looking for are actually isomorphisms. Note that we will write σ_p for σ_1 and σ_q for σ_2, which emphasises the fact that the automorohisms have orders p and

q respectively. Recall that we require the embeddings to satisfy $\beta(T) \subseteq \mathrm{Aut}(N)$, $\beta(\sigma_p)$ must have order p, $\beta(\sigma_q)$ must have order q, $\beta(\tau_p) \in \mathrm{Aut}(N)$ and must have order $p-1$ and $\beta(\tau_q) \in \mathrm{Aut}(N)$ and must have order $q-1$. Recall that two embeddings β and β' are equivalent if and only if $\beta'(g) = \gamma\beta(g)\gamma^{-1}$ for all $g \in G$ and some $\gamma \in \mathrm{Aut}(N)$. A suitable embedding is given by $\beta(\sigma_p) = (\mu, id)$, $\beta(\sigma_q) = (\eta, id)$, $\beta(\tau_p) = (e, \phi_c)$ and $\beta(\tau_q) = (e, \psi_d)$ with c a primitive root modulo p and d a primitive root modulo q.

Proposition 5.4.3. *The embedding given above corresponds to the Hopf-Galois structure that we have already found.*

Proof. Let $\mu \in \mathrm{Perm}(X)$ be defined by $\mu(\overline{\sigma_p^i\sigma_q^j}) = \overline{\sigma_p^{i-1}\sigma_q^j}$ and let $\eta \in \mathrm{Perm}(X)$ be defined by $\eta(\overline{\sigma_p^i\sigma_q^j}) = \overline{\sigma_p^i\sigma_q^{j-1}}$.

Recall that by construction the map $\alpha(\mu^i\eta^j)$ is given by $b^{-1}\lambda_N(\mu^i\eta^j)b$. In this case the map b is given by $b(\overline{g}) = \beta(g)e_N$. Hence if we consider a typical elenent of G $\sigma_p^r\sigma_q^s\tau^t$, we have $\alpha(\mu^i\eta^j)[\overline{\sigma_p^r\sigma_q^s}] = b^{-1}\lambda_N(\mu^i\eta^j)b[\overline{\sigma_p^r\sigma_q^s}] = b^{-1}\lambda_N(\mu^i\eta^j)(\mu^r\eta^s) = b^{-1}(\mu^{i+r}\eta^{j+s}) = \overline{\sigma_p^{i+r}\sigma_q^{j+s}} = \mu^{-r}\eta^{-s}(\overline{\sigma_p^i\sigma_q^j})$. Hence $\alpha(N) = \langle\mu, \eta\rangle \cong \lambda(S)$. □

We now aim to determine whether there are any inequivalent embeddings. Suppose that $\beta' : G \hookrightarrow \mathrm{Hol}(N)$ is another suitable embedding.

Proposition 5.4.4. *$\beta'(\tau_p) = \beta(\tau_p)^u$ for some $1 \leq u \leq p-1$ such that $gcd(u, p-1) = 1$.*

Proof. A priori it is possible that $\beta(\tau_p) = (e, \phi_i\psi_j)$ for some i and j with $\phi_i\psi_j$ having order $p-1$, we will show that $j = 1$ (note that ϕ_1 and ψ_1 are the identity maps). In G we have $\tau_p\sigma_q = \sigma_q\tau_p$, so $\beta'(\tau_p)\beta'(\sigma_q) = \beta'(\sigma_q)\beta'(\tau_p)$. If we write $\beta'(\sigma_q) = (\mu^k\eta^l, f) \in \mathrm{Hol}(N)$, then the previous equation becomes $(e, \phi_i\psi_j)(\mu^k\eta^l, f) = (\mu^k\eta^l, f)(e, \phi_i\psi_j)$. If we let both sides of this equation act on e_N, we get $\phi_i\psi_j(\mu^k\eta^l) = \mu^k\eta^l$. This implies that $\mu^{ik}\eta^{jl} = \mu^k\eta^l$, which in turn implies that $ik \equiv k \pmod{p}$ and $jl \equiv l \pmod{q}$. We have $i \equiv 1 \pmod{p}$ or $k \equiv 0 \pmod{p}$ and $j \equiv 1 \pmod{q}$ or $l \equiv 0 \pmod{q}$. Note that one of the congruences modulo p has to hold *and* one of the congruences modulo q has to hold. If $i \equiv 1 \mod p$, then since ϕ_1 is the identity element of $\mathrm{Aut}(\langle\mu\rangle)$, $\beta'(\tau_p) = (e, \psi_j)$ but since ψ_j is an element of a group of order

$q-1$ and $q-1 < p-1$, this means that $\beta'(\tau_p)$ cannot have order $p-1$. If $k \equiv 0 \pmod{p}$ and $l \equiv 0 \pmod{q}$, then $\beta'(\sigma_q) = (e_N, f)$ which cannot happen because $\beta'(\sigma_q)$ cannot be trivial in the N-component. Hence the only possibility is that $k \equiv 0 \pmod{p}$ and $j \equiv 1 \pmod{q}$. So far we have shown that $\beta'(\tau_p) = (e, \phi_i)$ for some i. Now, the fact that $\beta'(\tau_p)$ has order $p-1$ implies that $i \equiv c^u \pmod{p}$ with $gcd(u, p-1) = 1$, so $\beta'(\tau_p) = (e, \phi_c)^u = \beta(\tau_p)^u$ as claimed. □

Remark 5.4.5. *In the above proof, we determined that* $\beta'(\sigma_q) = (\eta^l, f)$.

Proposition 5.4.6. *The subgroup generated by* (μ, id) *is normal in* $\mathrm{Hol}(N)$.

Proof. The subgroup $\langle(\mu, id)\rangle$ is normal in $\mathrm{Hol}(N)$ if and only if $g(\mu, id)g^{-1} = (\mu^r, id)$ for all $g \in \mathrm{Hol}(N)$ and some $0 \leq r \leq p-1$. It is sufficient to check this for g the generators of $\mathrm{Hol}(N)$. We have

$$(\mu, id)(\mu, id)(\mu, id)^{-1} = (\mu\mu\mu^{-1}, id) = (\mu, id),$$

$$(\eta, id)(\mu, id)(\eta, id)^{-1} = (\eta\mu\eta^{-1}, id) = (\mu, id),$$

$$(e, \phi_c)(\mu, id)(e, \phi_c)^{-1} = (\phi_c(\mu), \phi_c\phi_c^{-1}) = (\mu^c, id),$$

$$(e, \psi_d)(\mu, id)(e, \psi_d)^{-1} = (\psi_d(\mu), \psi_d\psi_d^{-1}) = (\mu, id).$$

Since all of these are of the form (μ^r, id), the subgroup generated by (μ, id) is normal in $\mathrm{Hol}(N)$ as claimed. □

Corollary 5.4.7. *The subgroup generated by* (μ, id) *is the unique Sylow* p*-subgroup of* $\mathrm{Hol}(N)$.

Proposition 5.4.8. *Further to Proposition 5.4.4, we have* $u = 1$ *so* $\beta'(\tau_p) = \beta(\tau_p)$.

Proof. Since the subgroup generated by (μ, id) is the unique Sylow p-subgroup of $\mathrm{Hol}(N)$, this implies that $\beta'(\sigma_p) = (\mu^m, id) = \beta(\sigma_p)^m$ for some m with $gcd(m, p) = 1$. Now in G, we have $\tau_p\sigma_p = \sigma_p^c\tau_p$, which implies that $\beta'(\tau_p)\beta'(\sigma_p) = \beta'(\sigma_p^c)\beta'(\tau_p)$, which implies that $\beta(\tau_p)^u\beta(\sigma_p)^m = \beta(\sigma_p^{mc})\beta(\tau_p)^u$. Now writing these elements as ordered pairs, we have $(e, \phi_c^u)(\mu^m, id) = (\mu^{mc}, id)(e, \phi_c^u)$. If we let both sides of this equation act on e_N, we get $\phi_c^u\mu^m = \mu^{mc}$ which impies that $\mu^{mc^u} = \mu^{mc}$ which tells us that $u = 1$ as claimed. □

Proposition 5.4.9. *In the previous proof, we can take $m = 1$ (i.e. $\beta'(\sigma_p) = (\mu, id)$).*

Proof. Let $\gamma : N \to N$ be the automorphism defined by $\gamma(\mu) = \mu^{m^{-1}}$ (where the inverse is taken modulo p) and $\gamma(\eta) = \eta$. Let β'' be the result of conjugating the embedding β' by the automorphism γ. Then in particular, $\beta''(\sigma_p) = (e, \theta)(\mu^m, id)(e, \theta)^{-1} = (\theta(\mu^m), id) = (\mu, id)$. □

Remark 5.4.10. *Henceforth, we will assume that we have conjugated the embedding to ensure that $m = 1$ so we can write $\beta'(\sigma_p) = (\mu, id)$.*

Proposition 5.4.11. *$\beta'(\tau_q) = \beta(\tau_q)^v$ for some $1 \leq v \leq q - 1$.*

Proof. In G, we have $\tau_q \sigma_p = \sigma_p \tau_q$, which implies that $\beta'(\tau_q)\beta'(\sigma_p) = \beta'(\sigma_p)\beta'(\tau_q)$. Writing these elements as ordered pairs, we have $(e, \phi_c^u \psi_d^v)(\mu, id) = (\mu, id)(e, \phi_c^u \psi_d^v)$. If we let both sides of this equation act on e_N, we get $\phi_c^u \psi_d^v(\mu) = \mu$. This implies that $\mu^{c^u} = \mu$, which implies that $c^u \equiv 1 \pmod p$, which tells us that $u \equiv 0 \pmod{p-1}$ (as a primitive root nmodulo p the element u has order $p - 1$ modulo p) hence the ϕ component in $\beta'(\tau_q)$ is just the identity. Hence $\beta'(\tau_q) = \beta(\tau_q)^v$ as claimed. □

Proposition 5.4.12. *$\beta'(\sigma_q) = \beta(\sigma_q)^l$ for some $0 \leq l \leq q - 1$.*

Proof. In the proof of Proposition 5.4.4, we found that $\beta'(\sigma_q) = (\eta^l, \phi_c^x \psi_d^y)$ for some $1 \leq x, y \leq p - 1$. In G, we have $\sigma_q \sigma_p = \sigma_p \sigma_q$, which implies that $\beta'(\sigma_q)\beta'(\sigma_p) = \beta'(\sigma_p)\beta'(\sigma_q)$. Writing these elements as ordered pairs, we have $(\eta^l, \phi_c^x \psi_d^y)(\mu, id) = (\mu, id)(\eta^l, \phi_c^x \psi_d^y)$. Letting both sides of this equation act on e_N gives $\eta^l \phi_c^x(\mu) = \mu \eta^l$. This implies that $\mu^{c^x} \eta^l = \mu \eta^l$ which tells us that $x = p - 1$ hence the ϕ component in $\beta'(\sigma_q)$ is just the identity. Now to prove that there is no ψ component, note that $\beta'(\sigma_q)$ must have order q which is prime. Let $\pi : \mathrm{Hol}(N) \twoheadrightarrow \mathrm{Aut}(N)$ be the projection given by $\pi((x, f)) = f$. Since $\beta'(\sigma_q)$ must have order q, when we project it onto the $\mathrm{Aut}(N)$ component we get $\pi(\beta'(\sigma_q))^q = \psi_d^{yq}$ which must have order dividing q. Since the element ψ_d has order $q - 1$, no power of ψ_d can have an order which divides q except for the identity. Hence $\beta'(\sigma_q) = (\eta^l, id) = \beta(\sigma_q)^l$ as claimed. □

Proposition 5.4.13. *Further to Proposition 5.4.11, we have $v = 1$, so $\beta'(\tau_q) = \beta(\tau_q)$.*

Proof. In G, we have $\tau_q\sigma_q = \sigma_q^d\tau_q$, which implies that $\beta'(\tau_q)\beta'(\sigma_q) = \beta'(\sigma_q)^d\beta'(\tau_q)$, which implies that $\beta(\tau_q)^v\beta(\sigma_q)^l = \beta(\sigma_q)^{ld}\beta(\tau_q)^v$. Now writing these elements as ordered pairs, we have $(e, \psi_d^v)(\eta^l, id) = (\eta^{ld}, id)(e, \psi_d)^v$. If we let both sides of this equation act on e_N, we get $\psi_d^v\eta^l = \eta^{ld}$ which impies that $\eta^{ld^v} = \eta^{ld}$ which tells us that $v = 1$ as claimed. □

Proposition 5.4.14. *Further to Proposition 5.4.12, we can take $l = 1$ (i.e. $\beta'(\sigma_q) = (\eta, id)$).*

Proof. Let $\gamma : N \to N$ be the automorphism defined by $\gamma(\mu) = \mu$ and $\gamma(\eta) = \eta^{-l}$. Let β'' be the result of conjugating the embedding β' by the automorphism γ. Then in particular, $\beta''(\sigma_q) = (e, \theta)(\eta^l, id)(e, \theta) = (\theta(\eta^l), id) = (\eta, id)$. □

To conclude, in all of the above we have shown that the embedding β' turns out to be equivalent to the embedding β. This tells us that there is only one equivalence class of embeddings and this completes the proof of Proposition 5.4.2.

We will now determine the Hopf-Galois structures admitted by the extension when $N \cong C_p \rtimes C_q$. Now we will suppose that $p \equiv 1 \pmod q$. Let

$$M = C_p \rtimes C_q = \langle \mu, \eta | \mu^p = \eta^q = e, \eta\mu\eta^{-1} = \mu^g \rangle$$

where g has multiplicative order q modulo p. ($C_p^\times$ is cyclic of order $p-1$. since $q|p-1$, there is an element in $C_p^\times$ of order q. Concretely, we could take $g = c^{\frac{p-1}{q}}$ with c a primitive root modulo p.) We aim to use Greither-Pareigis theory to determine whether there are any regular G-stable subgroups of $\mathrm{Perm}(X)$ that are isomorphic to M. This is equivalent to seeking regular embeddings $\alpha : M \hookrightarrow \mathrm{Perm}(X)$ with a G-stable image. By Byott's translation theorem, this is equivalent to finding suitable embeddings $\beta : G \hookrightarrow \mathrm{Hol}(M)$ with $\beta(T) = \mathrm{Stab}(e_N)$. Recall that $\mathrm{Hol}(M) = M \rtimes \mathrm{Aut}(M)$. We now determine what $\mathrm{Aut}(M)$ is as a group.

Proposition 5.4.15. $\mathrm{Aut}(M)$ *has order $p(p-1)$.*

Proof. We first consider the orders of elements in M. Since μ has order p, $\langle\mu\rangle$ is the Sylow p-subgroup of M. It is unique because $n_p|pq$ and $n_p \equiv 1 \pmod{p}$ so $n_p = 1$ (where n_p denotes the number of Sylow p-subgroups of M). Since η has order q, $\langle\eta\rangle$ is a Sylow q-subgroup of M. This is not unique. Note that all elements of $M\backslash\langle\mu\rangle$ have order q. There are p Sylow q-subgroups given by $\langle\mu^n\eta\rangle$ for $0 \leq n \leq p-1$. The formula for taking powers of elements of M is

$$(\mu^i\eta^j)^r = \mu^{i\frac{g^{jr}-1}{g-1}}\eta^{jr}.$$

To see this, we can view M as a semidirect product $M \cong \langle\mu\rangle \rtimes \langle\eta\rangle$ where η acts on μ by $\eta * \mu = \mu^g$. This allows us to write the elements of M as ordered pairs with multiplication given by

$$(\mu^i, \eta^j)(\mu^k, \eta^l) = (\mu^i(\eta^j * \mu^k), \eta^l) = (\mu^{i+kg^j}, \eta^{j+l}).$$

As a consequence of this, the subgroup generated by a typical element of M $\mu^i\eta^j$ (with $j \not\equiv 0 \pmod{q}$) is the same as that generated by $\mu^n\eta$ since we can take the r^{th} power of the element where r is such that $jr \equiv 1 \pmod{q}$. Now we return to considering the automorphism group. If $\phi \in \mathrm{Aut}(M)$ then $\phi(\mu)$ has order p so $\phi(\mu) = \mu^s$ for some $1 \leq s \leq p-1$. The map ϕ must send η to $\mu^t\eta^u$ with $1 \leq u \leq q-1$.

Next we show that we have $u = 1$ (so $\phi(\eta) = \mu^t\eta$ for some $0 \leq t \leq p-1$).

In M we have the relation $\eta\mu = \mu^g\eta$. This implies that $\phi(\eta\mu) = \phi(\mu^g\eta)$. Since ϕ is an automorphism, this implies that $\phi(\eta)\phi(\mu) = \phi(\mu)^g\phi(\eta)$. Substituting in the values for ϕ, we have $\mu^t\eta^u\mu^s = \mu^{sg}\mu^t\eta^u$. Rearranging the left hand side of this using the group relation to move the powers of μ to the left gives $\mu^{t+sg^u}\eta^u = \mu^{t+sg}\eta^u$ which tells us that $u = 1$ as claimed.

We can now *define* $\phi_{s,t}$ to be a homomorphism that maps μ to μ^s and η to $\mu^t\eta$. To check that $\phi_{s,t}$ preserves the group relations, note that $\phi_{s,t}(\eta\mu\eta^{-1}) = \phi_{s,t}(\eta)\phi_{s,t}(\mu)\phi_{s,t}(\eta^{-1}) = \mu^t\eta\mu^s\eta^{-1}\mu^{-t} = \mu^{sg} = \phi_{s,t}(\mu^g)$. To check that ϕ is surjective, given a target $\mu^k\eta^l$ we must be able to find i and j such that $\phi_{s,t}(\mu^i\eta^j) = \mu^k\eta^l$. We have $\phi_{s,t}(\mu^i\eta^j) = \mu^{si+t\frac{g^j-1}{g-1}}\eta^j$ hence $\phi_{s,t}(\mu^i\eta^j) = \mu^k\eta^l$ if and only if $j \equiv l \pmod{q}$ and $i \equiv s^{-1}(k - t\frac{g^l-1}{g-1}) \pmod{p}$. This tells us that as a set $\mathrm{Aut}(M) = \{\phi_{s,t}|1 \leq$

$s \leq p-1, 0 \leq t \leq p-1\}$, hence we conclude that $\mathrm{Aut}(M)$ has order $p(p-1)$ as claimed. □

Corollary 5.4.16. *There are no suitable embeddings $\beta : G \hookrightarrow \mathrm{Hol}(M)$ with $M \cong C_p \rtimes C_q$.*

Proof. Note that since β is an embedding its image must be a subgroup of $\mathrm{Hol}(M)$ of order $|G|$. The group G has order $pq(p-1)(q-1)$ and $\mathrm{Hol}(M)$ has order $p^2q(p-1)$. Therefore $Hol(M)$ does not have any subgroups of order $pq(p-1)(q-1)$ and we conclude that there are no suitable embeddings as claimed. □

In conclusion, we have now completed the proof of Proposition 5.4.1 having successfully shown that the unique almost classical Hopf-Galois structure is the only Hopf-Galois structure on the extension in the case where $r = 2$.

5.5 Unique Hopf-Galois structure of abelian type

Previously we determined an almost classical Hopf-Galois structure admitted by the extension. In this section, we will denote the corresponding embedding by β. We now return to the case in which m is a positive odd square free number and aim to use Byott's translation theorem to determine whether there are any other Hopf-Galois structures of abelian type. Recall that we have $G \cong S \rtimes T$ with S cyclic of order m and $|T| = \phi(m)$ with m square free and N is a group of order m. We seek inequivalent embeddings $\beta' : G \hookrightarrow \mathrm{Hol}(N)$ such that $\mathrm{Stab}(e_N) = \beta'(T)$.

Lemma 5.5.1. *If $\beta' : G \hookrightarrow \mathrm{Hol}(N)$ is a suitable embedding, then $\beta'(S)$ is a regular subgroup of* $\mathrm{Hol}(N)$.

Proof. We first observe that $|\beta'(S)| = m$. To show that $\beta'(S)$ acts transitively, since β' is a suitable embedding, we know that $\mathrm{Stab}(e_N) = \beta'(T)$ so by the Orbit-Stabiliser theorem $|\,\mathrm{Orb}(e_N)| = \frac{|\beta'(G)|}{|\beta'(T)|} = \frac{|G|}{|T|} = m$ and since $\mathrm{Orb}(e_N) \subseteq N$ we have that $\beta'(G)$ acts transitively on N. For a typical element $st \in G$ (where $s \in S$ and $t \in T$), $\beta'(st)[e_N] = \beta'(s)\beta'(t)[e_N] = \beta'(s)[e_N]$ where the last equality holds because $\beta'(t)$ stabilises e_N, so in fact $\beta'(S)$ acts transitively. □

Proposition 5.5.2. *If N is cyclic, then* $\mathrm{Hol}(N)$ *contains a unique cyclic regular subgroup, which is* (N, id).

Proof. See Lemma 5.3 and Example 7.1 of [AB18]. □

Proposition 5.5.3. *$\beta'(\sigma_i) = \beta(\sigma_i)^{k_i}$ for all i and some k_i depending on i.*

Proof. The previous lemma and proposition tell us that if $\beta' : G \hookrightarrow \mathrm{Hol}(N)$ is a suitable embedding, then $\beta'(S) = (N, id)$. Hence $\beta'(\sigma_i) = (\eta_i^{k_i}, id)$ for all i and some k_i depending on i. □

Proposition 5.5.4. *For all i we have $\beta'(\tau_i) = \beta(\tau_i)$.*

Proof. Firstly, note that $\beta'(\tau_i) \in (e_N, Aut(N))$ for each i (by the stabiliser condtion in the definition of β'). Now, suppose that we fix i. For each $j \neq i$, we have $\tau_j\sigma_i = \sigma_i\tau_j$ in G, so $\beta'(\tau_i\sigma_j) = \beta'(\sigma_j\tau_i)$, which implies that $\beta'(\tau_i)(\eta_j^{k_j}, id) = (\eta_j^{k_j}, id)\beta'(\tau_i)$. Since the previous equation holds for *all* $j \neq i$, this tells us that $\beta'(\tau_i) = (e_n, \phi_i^{l_i})$ for some l_i. Now (for $j = i$), in G we have $\tau_i\sigma_i = \sigma_i^{d_i}\tau_i$ hence $\beta'(\tau_i\sigma_i) = \beta'(\sigma_i^{d_i}\tau_i)$. Writing these elements as ordered pairs, we have $(e_N, \phi_i^{l_i})(\eta_i^{k_i}, id) = (\eta_i^{k_i d_i}, \phi_i^{l_i})$. Doing the multiplication on the left hand side gives $(\eta_i^{k_i d_i^{l_i}}, \phi_i^{l_i}) = (\eta_i^{k_i d_i}, \phi_i^{l_i})$. Comparing the exponents of η_i, this tells us that $l_i = 1$. □

Finally, we aim to show that β' is equivalent to β. Recall that $\beta(\sigma_i) = (\eta_i, id)$ and $\beta(\tau_i) = (e_N, \phi_i)$ also recall that β and β' are equivalent if and only if $\beta' = \gamma\beta\gamma^{-1}$ for some $\gamma \in Aut(N)$.

Proposition 5.5.5. *The embedding β' is equivalent to β.*

Proof. Define $\gamma \in \mathrm{Aut}(N)$ by $\gamma = \phi_1^{n_1}...\phi_r^{n_r}$ where $d_i^{n_i} = k_i$ for all i. For each i, we have $\gamma\beta(\tau_i)\gamma^{-1} = (e_N, \phi_1^{n_1}...\phi_r^{n_r})(e_N, \phi_i)(e_N, \phi_1^{-n_1}...\phi_r^{-n_r}) = (e_N, \phi_i) = \beta'(\tau_i)$ where the second equality holds because $\mathrm{Aut}(N)$ is abelian (since N is cyclic). Also, we have $\gamma\beta(\sigma_i)\gamma^{-1} = (e_N, \phi_1^{n_1}...\phi_r^{n_r})(\eta_i, id)(e_N, \phi_1^{-n_1}...\phi_r^{-n_r}) = (\phi_i^{n_i}(\eta_i, id) = (\eta_i^{k_i}, id) = \beta'(\sigma_i)$. Hence β' is equivalent to β as claimed. □

In conclusion, we have now shown that there is a unique Hopf-Galois structure of abelian type admitted by the extension.

5.6 Properties of the almost classical Hopf-Galois structure

We now return to the case in which $L = K(\alpha_1, ..., \alpha_r)$ with $\alpha^{p_i} \in \mathcal{O}_K$ for each i and study the unique almost classical Hopf-Galois structure on L/K, corresponding to the regular subgroup $N = \lambda(S)$ of $\mathrm{Perm}(X)$.

Proposition 5.6.1. *We have $H \cong K^m$ via orthogonal idempotents.*

Proof. The orthogonal idempotents are given by

$$e_{\boldsymbol{i}} = \frac{1}{m} \prod_{k=1}^{r} \sum_{n=0}^{p_k - 1} \zeta^{-i_k n} \lambda(\sigma_k)^n$$

These form an E-basis of $E[N]$. Since G acts on N by ${}^{\sigma_i}\lambda(\sigma_j) = \lambda(\sigma_j)$ for all i and j, ${}^{\tau_i}\lambda(\sigma_i) = \lambda(\sigma_i)^{d_i}$ where d_i is a primitive root modulo p_i and ${}^{\tau_i}\lambda(\sigma_j) = \lambda(\sigma_j)$ for $i \neq j$, we have that each idempotent $e_{\boldsymbol{i}}$ is fixed by each element of G and so lies in $E[N]^G = H$. Therefore H has a K-basis of mutually orthogonal idempotents and so $H \cong K^m$ as K-algebras. □

Corollary 5.6.2. *The Greither-Pareigis theorem implies that the action of H on L is given by*

$$\prod_{n=1}^{r} \sum_{i=0}^{p-1} c_{i_n} \eta_n^{i_n} \cdot z = \prod_{n=1}^{r} \sum_{i=0}^{p-1} c_{i_n} \eta_n^{-i_n} [\overline{1_G}](z) = \prod_{n=1}^{r} \sum_{i=0}^{p-1} c_{i_n} \overline{\sigma_n^{i_n}}(z)$$

for all $z \in L$.

Proof. This is a consequence of Theorem 2.6.14. □

Proposition 5.6.3. *The orthogonal idempotents detect the elements of L in the following way.*

$$e_{\boldsymbol{i}}(\boldsymbol{\alpha^j}) = \frac{1}{m} \prod_{k=1}^{r} \sum_{n=0}^{p_k - 1} \zeta^{i_k n} \sigma_k^n(\alpha_k^{j_k}) = \begin{cases} \boldsymbol{\alpha^j} & \text{if } \boldsymbol{i} = \boldsymbol{j}. \\ 0 & \text{otherwise.} \end{cases}$$

Proof. This is a consequence of Proposition 5.6.1 and Corollary 5.6.2. Also note that the proof of this is similar to the proof of Proposition 2.5.6. □

Chapter 6

A family of non-normal simple radical extensions of square free degree - Ramification and rings of integers

6.1 Ramification

Recall that $m = p_1...p_r$ is an odd square free number, K is a number field in which each p_i is unramified, and L is an extension of K of degree m and of the form $L = K(\alpha_1, ..., \alpha_r)$ with $a_i := \alpha_i^{p_i} \in K$ for each $i = 1, ..., r$.

Proposition 6.1.1. *The extension L/K is tame if and only if the elements a_i can be chosen to satisfy $a_i \equiv 1 \pmod{p_i^2\mathcal{O}_K}$ for each i.*

Proof. To ensure that L/K is tame, applying Proposition 2.1.9 (which states that a compositum of extensions is tame if and only if each of the subextensions is tame), then applying Proposition 2.8.2 (which states that $K(\alpha_i)/K$ is tame if and only if a_i can be chosen to satisfy $a_i \equiv 1 \pmod{p_i^2\mathcal{O}_K}$) we get that it is necessary and sufficient to assume that $a_i \equiv 1 \pmod{p_i^2\mathcal{O}_K}$ for all i. □

Henceforth we will assume that these congruences hold. A consequence of this

assumption is that we can no longer assume that $\alpha_i^{p_i} = d$ for each i.

6.2 Local integral bases for $\mathfrak{p} \nmid m\mathcal{O}_K$

Recall Lemma 2.8.3 which states that for each i the prime ideals that do not lie above $p_i\mathcal{O}_K$ are either unramified or totally ramified in $K(\alpha_i)$. First we consider the case where $\mathfrak{p}$ is totally ramified in $K(\alpha_i)$ for all i. By Theorem 118 of [HGK81], this case occurs if and only if $v_{\mathfrak{p}}(a_i) \not\equiv 0 \pmod{p_i}$ for all i.

Proposition 6.2.1. *$\mathfrak{p}$ is totally ramified in L.*

Proof. Consider the ideal $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}...\mathfrak{P}_g^{e_g}$, we know that $\sum_{j=1}^{g} e_j f_j = [L : K] = m$. Let $\mathfrak{P}$ be one of the $\mathfrak{P}_j$ and write $e = e_j$. Let $\mathfrak{P}_{\alpha_i} = \mathfrak{P} \cap \mathcal{O}_{K(\alpha_i)}$. Then $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{P}_{\alpha_i}$ and $\mathfrak{P}_{\alpha_i}$ is a prime ideal of $\mathcal{O}_{K(\alpha_i)}$ lying above $\mathfrak{p}$. The ramification index $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_{\alpha_i})e(\mathfrak{P}_{\alpha_i}/\mathfrak{p})$ and we know that $e(\mathfrak{P}_{\alpha_i}/\mathfrak{p}) = p_i$ because $\mathfrak{p}$ is totally ramified in $K(\alpha_i)/K$. Hence $e(\mathfrak{P}/\mathfrak{p})$ is divisible by p_i. Since this argument is valid for each i in turn, we obtain that $e(\mathfrak{P}/\mathfrak{p})$ is divisible by all primes p_i. Hence $e(\mathfrak{P}/\mathfrak{p})$ is divisible by m. Since $\mathfrak{P}$ was an arbitrary $\mathfrak{P}_j$, one of the e_j is equal to m. Hence $g = 1$ and $f_1 = 1$. Hence we have $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^m$ and $\mathfrak{p}$ is totally ramified as claimed. □

The prevous proposition allows us to apply Theorem 2.2.10. This says that L/K is totally ramified if and only if $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}[x]$ where $v_{\mathfrak{P}}(x) = 1$. In other words, the elements 1, x, x^2, ..., x^{m-1} cover all the valuations between 0 and $m-1$ (at $\mathfrak{P}$). We could try to find such an x or alternatively we can try to find a set of elements which cover all valuations from 0 to $m-1$.

Definition 6.2.2. *For $1 \leq i \leq r$, we will use q_i to denote the integer $\frac{m}{p_i}$. Also let $\boldsymbol{q}$ denote the collection $(q_1, ..., q_r)$.*

Proposition 6.2.3. *The set*

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}} | 0 \leq i_k \leq p_k - 1 \text{ for each } 1 \leq k \leq r \right\}$$

covers all valuations from 0 to $m-1$.

Proof. Let $\mathfrak{P}$ be the unique prime of L lying above $\mathfrak{p}$. Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^m$. For each $0 \leq j \leq r$ we have

$$mv_{\mathfrak{p}}(a_j) = v_{\mathfrak{P}}(a_j) = v_{\mathfrak{P}}(\alpha_j^{p_j}) = p_j v_{\mathfrak{P}}(\alpha_j),$$

so

$$v_{\mathfrak{P}}(\alpha_j) = q_j v_{\mathfrak{p}}(a_j) = v_{\mathfrak{p}}(a_j^{q_j}).$$

Hence

$$v_{\mathfrak{P}}\left(\frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}}\right) = v_{\mathfrak{P}}(\boldsymbol{\alpha^i}) - v_{\mathfrak{P}}(\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}) = v_{\mathfrak{p}}(\boldsymbol{a^{iq}}) - mr_{\mathfrak{p}}(\boldsymbol{a^{iq}}).$$

As noted above, this is the least positive remainder of $v_{\mathfrak{p}}(\boldsymbol{a^{iq}})$ modulo m, which lies between 0 and $m-1$. To show that every value in this range is achieved, it is sufficient to show that the values $v_{\mathfrak{p}}(\boldsymbol{a^{iq}})$ are all distinct modulo m as $\boldsymbol{i}$ varies. Suppose that $v_{\mathfrak{p}}(\boldsymbol{a^{iq}}) \equiv v_{\mathfrak{p}}(\boldsymbol{a^{nq}})$ for some $\boldsymbol{i}$ and $\boldsymbol{n}$. Then $v_{\mathfrak{p}}(\boldsymbol{a^{q(i-n)}}) \equiv 0 \pmod{m}$ and expanding the bold notation we have

$$\begin{aligned} & v_{\mathfrak{p}}(a_1^{q_1(i_1-n_1)}...a_r^{q_r(i_r-n_r)}) \equiv 0 \pmod{m} \\ \Rightarrow & \sum_{k=1}^{r} q_k v_{\mathfrak{p}}(a_k)(i_k - n_k) \equiv 0 \pmod{m}. \end{aligned}$$

Recalling that $q_k = \frac{m}{p_k}$ for each k, we see that for each k we have

$$q_k v_{\mathfrak{p}}(a_k)(i_k - n_k) \equiv 0 \quad (p_k).$$

Since $p_k \nmid q_k$ by definition and $p_k \nmid v_{\mathfrak{p}}(a_k)$ by assumption, we find that $i_k - n_k \equiv 0 \pmod{p_k}$. Finally, since $0 \leq i_k, n_k \leq p_k - 1$, we obtain $i_k = n_k$ and so $\boldsymbol{i} = \boldsymbol{n}$. Thus $v_{\mathfrak{p}}(\boldsymbol{a^{iq}})$ covers all residues modulo m as $\boldsymbol{i}$ varies, so $v_{\mathfrak{P}}\left(\frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}}\right)$ covers the values $0, ..., m-1$ exactly once each as $\boldsymbol{i}$ varies. □

Corollary 6.2.4. *If $p_i \nmid v_{\mathfrak{p}}(a_i)$ for all i then the set*

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}} | 0 \leq i_k \leq p_k - 1 \text{ for each } 1 \leq k \leq r \right\}$$

forms an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$.

Next we show that this set also forms an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ in the case that $p_i | v_{\mathfrak{p}}(a_i)$ for some i.

Proposition 6.2.5. *If $p_i | v_{\mathfrak{p}}(a_i)$ for at least one i then an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by*

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}} | 0 \leq i_k \leq p_k - 1 \text{ for each } 1 \leq k \leq r \right\}.$$

Proof. Relabelling if necessary there exists $1 \leq s \leq r$ such that $p_i \nmid v_{\mathfrak{p}}(a_i)$ for $i = 1, ..., s$ and $p_i | v_{\mathfrak{p}}(a_i)$ for $i = s+1, ..., r$. Let $L_s = K(\alpha_1, ..., \alpha_s)$. Applying the preceeding proposition and corollary to the extension L_s/K, we find that an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}} | 0 \leq i_k \leq p_k - 1 \text{ for each } 1 \leq k \leq s \right\}.$$

Now consider $L_{s+1} = L_s(\alpha_{s+1})$. Since $\mathfrak{p}$ is unramified in $K(\alpha_{s+1})$, the extensions L_s/K and $K(\alpha_{s+1})/K$ are arithmetically disjoint at $\mathfrak{p}$ and so an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}} \frac{\alpha_{s+1}^{i_{s+1}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(a_{s+1}^{i_{s+1}q_{s+1}})}} | 0 \leq i_k \leq p_k - 1 \text{ for each } 1 \leq k \leq s+1 \right\}.$$

Since $p_{s+1} | v_{\mathfrak{p}}(a_{s+1})$ we have

$$r_{\mathfrak{p}}(a_{s+1}^{i_{s+1}q^{s+1}}) = \frac{v_{\mathfrak{p}}(a_{s+1}^{i_{s+1}q^{s+1}})}{m},$$

so we may combine exponents in the denominator obtaining an $\mathcal{O}_{K,\mathfrak{p}}$-basis of the form

$$\left\{ \frac{\boldsymbol{\alpha^i}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a^{iq}})}} | 0 \leq i_k \leq p_k - 1 \text{ for each } 1 \leq k \leq s+1 \right\}.$$

Repeating this process yields the result. □

6.3 Local integral bases for $\mathfrak{p} | m\mathcal{O}_K$

Henceforth we will assume that if $\mathfrak{p} | p_j \mathcal{O}_K$ for some $p_j | m$, then $\mathfrak{p}$ is unramified in $K(\alpha_i)$ for all $i \neq j$. This assumption allows us to apply arithmetic disjointness which will ease obtaining the integral bases. Since we have previously assumed that each p_j is unramified in K, we may choose $\pi_{\mathfrak{p}} = p_j$ whenever $\mathfrak{p} | p_j$.

Proposition 6.3.1. *If $\mathfrak{p}|p_j$ for some $j = 1, ..., r$ then an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is given by*

$$\left\{ \frac{\boldsymbol{\alpha^i}}{p_j^{r_\mathfrak{p}(\boldsymbol{a^{iq}})}} | 0 \leq i_k \leq p_k - 1 \text{ for } 1 \leq k \leq r \text{ and } i_j \neq p_j - 1 \right\}$$
$$\cup \left\{ \frac{1 + \alpha_j + ... + \alpha_j^{p_j - 1}}{p_j} \frac{\boldsymbol{\alpha^i}}{p_j^{r_\mathfrak{p}(\boldsymbol{a^{iq}})}} | 0 \leq i_k \leq p_k - 1 \text{ for } 1 \leq k \leq r \text{ and } i_j = 0 \right\}.$$

Proof. Since we have assumed that $\mathfrak{p}$ is unramified in $K(\alpha_i)$ for all $i \neq j$, the extensions $K(\alpha_j)$ and $L_j = K(\alpha_1, ..., \alpha_{j-1}, \alpha_{j+1}, ..., \alpha_r)$ are arithmetically disjoint at $\mathfrak{p}$. By Proposition 2.8.5, an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{K(\alpha_j),\mathfrak{p}}$ is

$$\left\{ 1, \alpha_j, ..., \alpha_j^{p_j - 2}, \frac{1}{p_j}(1 + \alpha_j + ... + \alpha_j^{p_j - 1}) \right\}$$

and by Section 6.2 an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L_j,\mathfrak{p}}$ is

$$\left\{ \frac{\boldsymbol{\alpha^i}}{p_j^{r_\mathfrak{p}(\boldsymbol{a^{iq}})}} | 0 \leq i_k \leq p_k - 1 \text{ for } 1 \leq k \leq r \text{ and } i_j = 0 \right\}.$$

Hence an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ is the product of these two sets, which gives the set described in the proposition. □

6.4 Associated order and local generators

The aim of this section is to prove the following theorem

Theorem 6.4.1. *The ring of integers $\mathcal{O}_L$ is locally free over $\mathcal{A}_H$ in the unique almost classical Hopf-Galois structure.*

The proof of this theorem will take the form of a sequence of propositions. Recall the information on orders from the background chapter, in particular Theorem 2.3.7 which gives some properties of maximal orders. We will study the associated order by relating it to the fixed points of the group ring $\mathcal{O}_E[N]^G$. In fact, we will show that $\mathcal{A}_H = \mathcal{O}_E[N]^G$. Recall from Proposition 2.7.3 that $\mathcal{O}_E[N]^G \subseteq \mathcal{A}_H$.

Proposition 6.4.2. *If $p \nmid m\mathcal{O}_K$ then each $e_{\boldsymbol{i}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G$, $\mathcal{O}_{E,\mathfrak{p}}[N]^G = \mathcal{A}_{H,\mathfrak{p}} = \mathcal{M}_\mathfrak{p}$ and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module.*

Proof. See Proposition 5.7 of [Tru11]. □

To determine the associated order for prime ideals $\mathfrak{p}|m\mathcal{O}_K$, we will use the "all in one" approach (recall Theorem 2.7.5).

Proposition 6.4.3. *Suppose that $\mathfrak{p}|m\mathcal{O}_K$. Then $\mathcal{A}_{H,\mathfrak{p}} = \mathcal{O}_{E,\mathfrak{p}}[N]^G$ and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module.*

Proof. Since $\mathfrak{p}|m\mathcal{O}_K$ we have $\mathfrak{p}|p_j\mathcal{O}_K$ for exactly one $j = 1, ..., r$. Now fix j to be the unique value such that $\mathfrak{p}|p_j\mathcal{O}_K$. For each vector $\boldsymbol{i}$ with $0 \leq i_k \leq p_k - 1$ for each k, let

$$\boldsymbol{i}^{(l)} = (i_1^{(l)}, ..., i_r^{(l)}) \text{ where } i_k^{(l)} = \begin{cases} l \text{ if } k = j \\ i_k \text{ otherwise.} \end{cases}$$

(Thus $\boldsymbol{i}^{(l)}$ agrees with $\boldsymbol{i}$ in all but possibly the j^{th} position where it is equal to l.) Note that $0 \leq l \leq p_k - 1$. Label the $\mathcal{O}_{K,\mathfrak{p}}$-basis elements of $\mathcal{O}_{L,\mathfrak{p}}$ found in Proposition 6.4.2 as follows:

$$x_{\boldsymbol{i}} = \begin{cases} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{p_j^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}}\boldsymbol{q})}} \text{ if } i_j \neq p_j - 1 \\ \frac{1+\alpha_j+...+\alpha_j^{p_j-1}}{p_j} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}^{(0)}}}{p_j^{r_{\mathfrak{p}}\left(\boldsymbol{\alpha}^{\boldsymbol{i}^{(0)}}\boldsymbol{q}\right)}} \text{ if } i_j = p_j - 1. \end{cases}$$

Now let

$$x_{\mathfrak{p}} = \frac{1 + \alpha_j + ... + \alpha_j^{p_j-1}}{m} \sum_{\boldsymbol{i}^{(0)}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}^{(0)}}}{p_j^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}^{(0)}}\boldsymbol{q})}} \in \mathcal{O}_{L,\mathfrak{p}}.$$

This element generates $L_{\mathfrak{p}}$ as an $H_{\mathfrak{p}}$-module: for each $\boldsymbol{i}$ we have $e_{\boldsymbol{i}} \cdot x_{\mathfrak{p}} = c_{\boldsymbol{i}}\boldsymbol{\alpha}^{\boldsymbol{i}}$ for some nonzero $c_{\boldsymbol{i}} \in K_{\mathfrak{p}}$. Therefore, following the method of Theorem 2.7.5, for each $\boldsymbol{i}$ there is a unique element $a_{\boldsymbol{i}} \in H_{\mathfrak{p}}$ such that $a_{\boldsymbol{i}} \cdot x_{\mathfrak{p}} = x_{\boldsymbol{i}}$. We can determine the $a_{\boldsymbol{i}}$ explicitly. We have

$$e_{\boldsymbol{i}} \cdot x_{\mathfrak{p}} = \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{p_j^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}}\boldsymbol{q})}}.$$

Hence

$$a_{\boldsymbol{i}} = \begin{cases} me_{\boldsymbol{i}} & \text{if } i_j \neq p_j - 1 \\ \sum_l e_{\boldsymbol{i}^{(l)}} & \text{if } i_j = p_j - 1. \end{cases}$$

To complete the proof we must show that $a_{\boldsymbol{i}} \in \mathcal{A}_{H,\mathfrak{p}}$ for all $\boldsymbol{i}$. In fact we show that $a_{\boldsymbol{i}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G \subseteq \mathcal{A}_{H,\mathfrak{p}}$ for all $\boldsymbol{i}$. Recall that $e_{\boldsymbol{i}} = \frac{1}{m} \prod_{k=1}^{r} \sum_{n=0}^{p_k-1} \zeta^{-i_k n} \lambda(\sigma_k)^n$. It is

clear that $me_{\boldsymbol{i}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G$ and so $a_{\boldsymbol{i}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G$ for $i_j \neq p_j - 1$. If $i_j = p_j - 1$ then we have

$$\begin{aligned} a_{\boldsymbol{i}} &= \sum_l e_{\boldsymbol{i}^{(l)}} \\ &= \sum_l \frac{1}{m} \prod_{k=1}^{r} \sum_{n=0}^{p_k-1} \zeta^{-i_k^{(l)} n} \lambda(\sigma_k)^n \\ &= \frac{p_j}{m} \prod_{k=1, k\neq j}^{r} \sum_{n=0}^{p_k-1} \zeta^{-i_k n} \lambda(\sigma_k)^n \\ &\in \mathcal{O}_{E,\mathfrak{p}}[N]^G. \end{aligned}$$

Hence $a_{\boldsymbol{i}} \in \mathcal{O}_{E,\mathfrak{p}}[N]^G \subseteq \mathcal{A}_{H,\mathfrak{p}}$ for each $\boldsymbol{i}$, so the $a_{\boldsymbol{i}}$ form an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{E,\mathfrak{p}}[N]^G = \mathcal{A}_{H,\mathfrak{p}}$ and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module with generator $x_{\mathfrak{p}}$. □

We have achieved our aim of proving Theorem 6.4.1, that the ring of integers $\mathcal{O}_L$ is locally free over $\mathcal{A}_H$ in the unique almost classical Hopf-Galois structure.

Proposition 6.4.4. *For prime ideals $\mathfrak{p} \nmid m\mathcal{O}_K$, the element*

$$x_{\mathfrak{p}} = \frac{1}{m} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}}$$

is a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{A}_{H,\mathfrak{p}}$.

Proof. For prime ideals $\mathfrak{p} \nmid m\mathcal{O}_K$ we have

$$\mathcal{A}_{H,\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}\langle e_{\boldsymbol{i}} | 0 \leq i_k \leq p_k - 1 \text{ for each } 1 \leq k \leq r \rangle$$

Now

$$e_{\boldsymbol{i}} \cdot x_{\mathfrak{p}} = \frac{1}{m} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}}$$

for each $\boldsymbol{i}$. Refering to the $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$ constructed in Section 6.2 and noting that $\frac{1}{m} \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$in this case, we see that the set

$$\{e_{\boldsymbol{i}} \cdot x_{\mathfrak{p}} | 0 \leq i_k \leq p_k - 1 \text{ for } 1 \leq k \leq r\}$$

forms an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{L,\mathfrak{p}}$. Hence $x_{\mathfrak{p}}$ is a free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{A}_{H,\mathfrak{p}}$-module. □

6.5 Using idèlic theory to move from local to global freeness

In the previous sections, we have shown that $\mathcal{O}_L$ is locally free over $\mathcal{A}_H$ and given an explicit generator of $\mathcal{O}_{L,\mathfrak{p}}$ over $\mathcal{A}_{H,\mathfrak{p}}$ for each prime $\mathfrak{p}$ of $\mathcal{O}_K$. In this section we determine a criterion for $\mathcal{O}_L$ to be a free $\mathcal{A}_H$-module. Our strategy will be the same as in Section 4.5. By Theorem 2.4.16 $\mathcal{O}_L$ is a free $\mathcal{A}_H$-module if and only if $\mathcal{M}\mathcal{O}_L$ is a free $\mathcal{M}$-module with a generator in $\mathcal{O}_L$. (Here as before $\mathcal{M}$ denotes the unique maximal order in H.) In this case we have

$$\mathcal{M} = \mathcal{O}_K\langle e_{\boldsymbol{i}} | 0 \leq i_k \leq p_k - 1 \text{ for } 1 \leq k \leq r\rangle \cong \mathcal{O}_K^m.$$

As noted in Section 4.5, $\mathcal{M}\mathcal{O}_L$ is certainly a locally free $\mathcal{M}$-module and it is a free $\mathcal{M}$-module if and only if it has trivial class in the locally free class group $\mathrm{Cl}(\mathcal{M})$. As before there are isomorphisms

$$\mathrm{Cl}(\mathcal{M}) \cong \frac{\mathbb{J}(H)}{H^\times \mathbb{U}(\mathcal{M})} \cong \mathrm{Cl}(K)^m.$$

We use these to determine a criterion for $\mathcal{M}\mathcal{O}_L$ to be a free $\mathcal{M}$-module and then obtain a further criterion for it to have a generator in $\mathcal{O}_L$.

Proposition 6.5.1. *The class of $\mathcal{M}\mathcal{O}_L$ in $\mathrm{Cl}(\mathcal{M})$ corresponds to the class of the idèle $(h_\mathfrak{p})_\mathfrak{p}$, where*

$$h_\mathfrak{p} = \sum_{\boldsymbol{i}} \frac{e_{\boldsymbol{i}}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}}$$

for all $\mathfrak{p}$.

Proof. Let $x = \frac{1}{m}(1+\alpha_1+\ldots+\alpha_1^{p_1-1})\ldots(1+\alpha_r+\ldots+\alpha_r^{p_r-1}) \in \mathcal{O}_L$. Then x generates L as a free H-module. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$ let $x_\mathfrak{p}$ be the free generator of $\mathcal{O}_{L,\mathfrak{p}}$ as an $\mathcal{A}_{H,\mathfrak{p}}$-module found in Propositions 6.4.3 and 6.4.4. That is

$$x_\mathfrak{p} = \begin{cases} \frac{1+\alpha_j+\ldots+\alpha_j^{p_j-1}}{m} \sum_{\boldsymbol{i}^{(0)}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}^{(0)}}}{p_j^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}^{(0)}}\boldsymbol{q})}} & \text{if } \mathfrak{p} | p_j\mathcal{O}_K \text{ for some } j \\ \frac{1}{m}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{\pi_\mathfrak{p}^{r_\mathfrak{p}(\boldsymbol{a}^{\boldsymbol{i}})}} & \text{otherwise.} \end{cases}$$

Noting that $v_{\mathfrak{p}}(a_j) = 0$ for $\mathfrak{p}|p_j\mathcal{O}_K$, we may rewrite this as

$$x_{\mathfrak{p}} = \frac{1}{m}\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{iq}})}}$$

for all $\mathfrak{p}$. Then $x_{\mathfrak{p}}$ is also a free generator of $(\mathcal{M}\mathcal{O}_L)_{\mathfrak{p}}$ as an $\mathcal{M}_{\mathfrak{p}}$-module. For each $\mathfrak{p}$ the element $h_{\mathfrak{p}} \in H_{\mathfrak{p}}$ is defined by $h_{\mathfrak{p}} \cdot x = x_{\mathfrak{p}}$. We find

$$h_{\mathfrak{p}} = \sum_{\boldsymbol{i}} \frac{e_{\boldsymbol{i}}}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{iq}})}}$$

for all $\mathfrak{p}$. this gives the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ in the statement of the proposition. □

Now we use the isomorphism

$$\frac{\mathbb{J}(H)}{H^{\times}\mathbb{U}(\mathcal{M})} \cong \mathrm{Cl}(K)^m$$

to interpret the class of $(h_{\mathfrak{p}})_{\mathfrak{p}}$ as an m-tuple of classes of fractional ideals of K.

Proposition 6.5.2. *The idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ corresponding to the class of $\mathcal{M}\mathcal{O}_L$ in $\mathcal{M}$ corresponds to the m-tuple of classes of ideals $\mathfrak{a}_{\boldsymbol{i}}^{-1}$ where*

$$\mathfrak{a}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}.$$

Proof. Recall from Proposition 2.4.14 and Corollary 2.4.15 that to obtain the tuple of ideal classes corresponding to an idèle $(z_{\mathfrak{p}})_{\mathfrak{p}}$ we write

$$z_{\mathfrak{p}} = \sum_{\boldsymbol{i}} c_{\boldsymbol{i},\mathfrak{p}} e_{\boldsymbol{i}}$$

with $c_{\boldsymbol{i},\mathfrak{p}} \in K_{\mathfrak{p}}$ for all $\boldsymbol{i}$. Then the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ is mapped to the m-tuple of classes of fractional ideals $(\mathfrak{c}_{\boldsymbol{i}})$, where

$$\mathfrak{c}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(c_{\boldsymbol{i},\mathfrak{p}})}.$$

Applying this to the idèle $(h_{\mathfrak{p}})_{\mathfrak{p}}$ corresponding to the class of $\mathcal{M}\mathcal{O}_L$ in $\mathrm{Cl}(\mathcal{M})$ (constructed in the previous proposition) we see that

$$c_{\boldsymbol{i},\mathfrak{p}} = \frac{1}{\pi_{\mathfrak{p}}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{iq}})}}$$

for all $\boldsymbol{i}$ and $\mathfrak{p}$. Hence $(h_{\mathfrak{p}})_{\mathfrak{p}}$ corresponds to the m-tuple of ideal classes $(\mathfrak{a}_{\boldsymbol{iq}}^{-1})$ where

$$\mathfrak{a}_{\boldsymbol{iq}} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{iq}})}$$

for all $\boldsymbol{i}$. Finally, since $\boldsymbol{q}$ is fixed, all of these ideals are principal if and only if the ideals

$$\mathfrak{a}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(\boldsymbol{a^i})}$$

are principal for all $\boldsymbol{i}$ with $0 \leq i_k \leq p_k - 1$ for $1 \leq k \leq r$. □

Corollary 6.5.3. *The $\mathcal{M}$-module $\mathcal{M}\mathcal{O}_L$ is free if and only if the ideals $\mathfrak{a}_{\boldsymbol{i}}$ are principal for all $\boldsymbol{i}$.*

Proposition 6.5.4. *The $\mathcal{M}$-module $\mathcal{M}\mathcal{O}_L$ has a free generator lying in $\mathcal{O}_L$ if and only if the ideals $\mathfrak{a}_{\boldsymbol{i}}$ are principal for all $\boldsymbol{i}$ with generators $a_{\boldsymbol{i}}$ such that*

$$\frac{1}{m} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha^i}}{a_{\boldsymbol{i}}} \in \mathcal{O}_L.$$

Proof. By the previous proposition $\mathcal{M}\mathcal{O}_L$ is a free $\mathcal{M}$-module if and only if each ideal $\mathfrak{a}_{\boldsymbol{i}}$ is principal. Suppose that this is the case and write $\mathfrak{a}_{\boldsymbol{i}} = c_{\boldsymbol{i}}\mathcal{O}_K$ for some $c_{\boldsymbol{i}} \in \mathcal{O}_K$. Then a free generator for $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module is

$$y = \frac{1}{m} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha^i}}{c_{\boldsymbol{i}}}.$$

The set of free generators of $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module is precisely the set $\{z \cdot y | z \in \mathcal{M}^\times\}$. Since $\mathcal{M} \cong \mathcal{O}_K^m$ via orthogonal idempotents and $e_{\boldsymbol{i}} \cdot \boldsymbol{\alpha^j} = \delta_{\boldsymbol{i},\boldsymbol{j}}\boldsymbol{\alpha^j}$ we see that an element $y' \in L$ is a free generator for $\mathcal{M}\mathcal{O}_L$ as an $\mathcal{M}$-module if and only if it has the form

$$y' = \frac{1}{m} \sum_{\boldsymbol{i}} \frac{u_{\boldsymbol{i}}\boldsymbol{\alpha^i}}{c_{\boldsymbol{i}}}$$

for some $u_{\boldsymbol{i}} \in \mathcal{O}_K^\times$. Therefore $\mathcal{M}\mathcal{O}_L$ has a free generator lying in $\mathcal{O}_L$ if and only if there exist elements $u_{\boldsymbol{i}} \in \mathcal{O}_K^\times$ such that the corresponding element y' lies in $\mathcal{O}_L$. Writing $a_{\boldsymbol{i}} = u_{\boldsymbol{i}}^{-1}c_{\boldsymbol{i}}$ for each $\boldsymbol{i}$, this is equivalent to the existence of elements $a_{\boldsymbol{i}}$ as in the statement of the proposition. □

By combining the results of this section, we obtain a criterion for $\mathcal{O}_L$ to be a free $\mathcal{A}_H$-module:

Theorem 6.5.5. *The ring of algebraic integers $\mathcal{O}_L$ is a free $\mathcal{A}_H$-module if and only if the ideals $\mathfrak{b}_{\boldsymbol{i}}$ are principal for all $\boldsymbol{i}$ with generators $b_{\boldsymbol{i}}$ such that*

$$\frac{1}{m} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha^i}}{b_{\boldsymbol{i}}} \in \mathcal{O}_L.$$

Proof. This follows immediately from the previous proposition. □

6.6 Obtaining conditions for freeness that are independent of the choice of generators

The conditions for freeness from the paper of Del Corso and Rossi are independent of the choice of Kummer generators. Currently our conditions for freeness in the non-normal case are dependent on our specific initial choice of radical generators. We can resolve this by rewriting the extension using a single radical generator. It would be more natural to view the extension as $L = K(\delta)$ with the minimum polynomial of δ being $x^m - d$ (where m is odd and square free). This would be more like the Del Corso and Rossi "cyclic" paper [DCR10] where they study a cyclic Kummer extension using a single Kummer generator. In order to rewrite the extension using a single generator, we will first link α_1, ..., α_r to a *specific* δ, then afterwards we will vary δ.

To link α_1, ..., α_r to a *specific* δ we first let s_i be the inverse of q_i modulo p_i. Then we choose $\delta = \prod_{i=1}^{r} \alpha_i^{s_i}$.

Proposition 6.6.1. $L = K(\delta)$.

Proof. To prove this we will show that $K(\alpha_1, ..., \alpha_r) \subseteq K(\delta)$ and $K(\delta) \subseteq K(\alpha_1, ..., \alpha_r)$. It follows from the construction of δ that $K(\delta) \subseteq K(\alpha_1, ..., \alpha_r)$. For the reverse inclusion we will take specific powers of δ to show that α_1, ..., α_r are in $K(\delta)$. We have $\delta^{q_i} = a_i^{\lfloor \frac{s_i q_i}{p_i} \rfloor} \prod_{j \neq i} a_j^{\frac{s_i q_i}{p_i}} \alpha_i$ which shows that $\alpha_i \in K(\delta)$. Since this holds for all i, we have shown that $K(\alpha_1, ..., \alpha_r) \subseteq K(\delta)$ which completes the proof. □

Proposition 6.6.2. *Let*

$$\mathfrak{D}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(d^k)}{m} \rfloor}$$

be the ideals associated to d. These ideals are principal if and only if the ideals $\mathfrak{b}_i$ associated to b are principal.

Proof. Given $1 \leq k \leq m$, write $k = \sum_{j=1}^{r} q_j i_j$, then $\delta^k = \prod_{j=1}^{r} \delta^{q_j i_j} = c \prod_{j=1}^{r} \alpha_j^{i_j}$ for some $c \in \mathcal{O}_K$. In particular we have $d = \delta^m = \prod_{j=1}^{r} a_j^{s_j q_j}$. Similarly writing $k =$

$\sum_{j=1}^{r} q_j i_j$ again, we can take powers of d and write d^k in the form $d^k = c^m \prod_{j=1}^{r} a_j^{q_j i_j}$ for some $c \in \mathcal{O}_K$. Henceforth, we will use the bold notation and denote $\prod_{j=1}^{r} a_j^{q_j i_j}$ by $\boldsymbol{a}^{\boldsymbol{qi}}$. Now the ideals associated to d are $\mathfrak{D}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(d^k)}{m} \rfloor}$. To connect these to the ideals $\mathfrak{b}_{\boldsymbol{i}}$ associated to a_1, ..., a_r, we examine the exponents. We have

$$\lfloor \frac{v_{\mathfrak{p}}(d^k)}{m} \rfloor = \lfloor \frac{v_{\mathfrak{p}}(c^m \boldsymbol{a}^{\boldsymbol{qi}})}{m} \rfloor = \lfloor \frac{m v_{\mathfrak{p}}(c) + v_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{qi}})}{m} \rfloor = v_{\mathfrak{p}}(c) + \lfloor \frac{v_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{qi}})}{m} \rfloor,$$

so for $0 \leq k \leq m-1$ we have

$$\mathfrak{D}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor v_{\mathfrak{p}}(c) + \frac{v_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{qi}})}{m} \rfloor} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(c)} \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{qi}})}{m} \rfloor} = \langle c \rangle \mathfrak{b}_{\boldsymbol{iq}}.$$

Hence the ideals $\mathfrak{D}_k$ are all principal if and only if the ideals $\mathfrak{b}_{\boldsymbol{i}}$ are all principal. □

Proposition 6.6.3. *The ideals $\mathfrak{D}_k$ are principal with generators d_k satisfying*

$$\frac{1}{m} \sum_{k=0}^{m-1} \frac{\delta^k}{d_k} \in \mathcal{O}_L$$

if and only if the ideals $\mathfrak{b}_{\boldsymbol{i}}$ are principal for all $\boldsymbol{i}$ with generators $b_{\boldsymbol{i}}$ such that

$$y = \frac{1}{m} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{b_{\boldsymbol{iq}}} \in \mathcal{O}_L.$$

Furthermore in this case the element y is a free generator of $\mathcal{O}_L$ as an $\mathcal{A}_H$-module.

Proof. If $\mathfrak{b}_{\boldsymbol{i}} = \langle b_{\boldsymbol{i}} \rangle$ then $\mathfrak{D}_k = \langle c b_{\boldsymbol{i}} \rangle$. (Recall that k is connected to i_1, ..., i_r via $k = \sum_{j=1}^{r} q_j i_j$.) Hence if the $b_{\boldsymbol{i}}$ satisfy $\frac{1}{m} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{b_{\boldsymbol{i}}} \in \mathcal{O}_L$, then $\frac{1}{m} \sum_{k=0}^{m-1} \frac{\delta^k}{c b_{\boldsymbol{i}}} = \frac{1}{m} \sum_{k=0}^{m-1} \frac{c \boldsymbol{\alpha}^{\boldsymbol{i}}}{c b_{\boldsymbol{i}}} = \frac{1}{m} \sum_{k=0}^{m-1} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{b_{\boldsymbol{i}}} \in \mathcal{O}_L$ and the converse also holds. □

Del Corso and Rossi address the issue of varying the generator in Remark 1 of their "cyclic" paper [DCR10]. Their result will also turn out to be valid in our case. Here we expand on Del Corso and Rossi's remark and provde full detail in the calculations. Suppose there exists $\delta \in \mathcal{O}_L$ such that $L = K(\delta)$ and $\delta^m \in \mathcal{O}_K$ i.e. the minimum polynomial of δ over K is $x^m - d$ (where $d = \delta^m$) and the ideals assocated to d (given by $\mathfrak{D}_i = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(d^i)}{m} \rfloor}$) are prinicipal with generators x_i such that $\frac{1}{m} \sum_{i=0}^{m-1} \frac{\delta^i}{x_i} \in \mathcal{O}_L$. Now suppose that β is another integral radical generator (i.e. $b = \beta^m \in \mathcal{O}_K$ and $L = K(\beta)$).

Proposition 6.6.4. *The ideals associated to b are all principal.*

Proof. Following the remark from Del Corso and Rossi, we write $\delta = \beta^l c$ with $gcd(l, m) = 1$ and $c \in K$. Let t be the inverse of l modulo m. For each $0 \leq j \leq m-1$, write k_j for the class of jt modulo m. Let $y_j = x_{k_j} c^{-k_j} b^{-\lfloor \frac{lk_j}{m} \rfloor}$. Then we claim that for each j, y_j generates $\mathfrak{b}_j$. We first study b^j. We have $\delta = \beta^l c$ which implies that $d = b^l c^m$ which implies that $b^l = c^{-m} d$ which implies that $b^{lt} = c^{-mt} d^t$. Recalling that $lt \equiv 1 \pmod{m}$ we can write $lt = m\lfloor \frac{lt}{m} \rfloor + 1$. This allows us to write the previous expression as $b^{m\lfloor \frac{lt}{m} \rfloor + 1} = c^{-mt} d^t$ which implies that $b = b^{m\lfloor \frac{lt}{m} \rfloor} c^{-mt} d^t$ and hence $b^j = b^{mj\lfloor \frac{lt}{m} \rfloor} c^{-mjt} d^{jt}$. Now we write $jt = m\lfloor \frac{jt}{m} \rfloor + k_j$ and use this expression to remove as many powers of m as we can from the previous expression to obtain $b^j = b^{mj\lfloor \frac{lt}{m} \rfloor} c^{-mjt} d^{m\lfloor \frac{jt}{m} \rfloor} d^{k_j}$. Now we use $d = b^l c^m$ to replace the first d in the previous expression to obtain

$$b^j = b^{mj\lfloor \frac{lt}{m} \rfloor} c^{-mjt} b^{lm\lfloor \frac{jt}{m} \rfloor} c^{m^2 \lfloor \frac{jt}{m} \rfloor} d^{k_j} = b^{m(l\lfloor \frac{jt}{m} \rfloor - j\lfloor \frac{lt}{m} \rfloor)} c^{m(m\lfloor \frac{jt}{m} \rfloor - jt)} d^{k_j}.$$

Since $jt = m\lfloor \frac{jt}{m} \rfloor + k_j$ the bracket in the exponent of c in the previous expression is equal to $-k_j$. Hence the previous expression becomes $b^{m(l\lfloor \frac{jt}{m} \rfloor - j\lfloor \frac{lt}{m} \rfloor)} c^{-mk_j} d^{k_j}$. To simplify the bracket in the exponent of the b term, we first note that $lt \equiv 1 \pmod{m}$, so $lt = um + 1$, so $jlt = jum + j$, since $0 \leq j \leq m-1$, we get $\lfloor \frac{jlt}{m} \rfloor = ju = j\lfloor \frac{lt}{m} \rfloor$. Since $lt \equiv 1 \pmod{m}$, this allows us to bring the j inside the floor function without introduing "carries". Hence we obtain $b^{m(l\lfloor \frac{jt}{m} \rfloor - \lfloor \frac{jlt}{m} \rfloor)} c^{-mk_j} d^{k_j}$. Now write $jt = m\lfloor \frac{jt}{m} \rfloor + k_j$, which implies that $jlt = ml\lfloor \frac{jt}{m} \rfloor + lk_j$, which imples that $\lfloor \frac{jlt}{m} \rfloor = l\lfloor \frac{jt}{m} \rfloor + \lfloor \frac{lk_j}{m} \rfloor$. Hence the bracket in the exponent of the b term becomes $-\lfloor \frac{lk_j}{m} \rfloor$ and we obtain $b^{-m\lfloor \frac{lk_j}{m} \rfloor} c^{-mk_j} d^{k_j}$. Hence taking valuations, we have

$$\lfloor \frac{v_{\mathfrak{p}}(b^j)}{m} \rfloor = v_{\mathfrak{p}}|(b^{-\lfloor \frac{lk_j}{m} \rfloor} c^{-k_j}) + \lfloor \frac{v_{\mathfrak{p}}(d^{k_j})}{m} \rfloor,$$

hence

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(b^j)}{m} \rfloor} = \langle b^{-\lfloor \frac{lk_j}{m} \rfloor} c^{-k_j} x_{k_j} \rangle = \langle y_j \rangle.$$

□

Proposition 6.6.5. *The generators of the ideals associated to b satisfy* $\frac{1}{m} \sum_{j=0}^{m-1} \frac{\beta^j}{y_j} \in \mathcal{O}_L$.

Proof. Following Del Corso and Rossi, we prove this by showing that there is an equality of sets: $\{\frac{\delta^i}{x_i}\} = \{\frac{\beta^j}{y_j}\}$. Fix j and consider $\frac{\beta^j}{y_j}$. We have

$$\frac{\beta^j}{y_j} = \frac{b^{-j\lfloor\frac{lt}{m}\rfloor}c^{-jt}\delta^{jt}}{b^{-\lfloor\frac{lk_j}{m}\rfloor}c^{-k_j}x_{k_j}}.$$

Since $jt = m\lfloor\frac{jt}{m}\rfloor + k_j$ we can rewrite the exponent of δ to obtain

$$\frac{b^{-j\lfloor\frac{lt}{m}\rfloor}c^{-jt}\delta^{m\lfloor\frac{jt}{m}\rfloor}\delta^{k_j}}{b^{-\lfloor\frac{lk_j}{m}\rfloor}c^{-k_j}x_{k_j}}.$$

Since $\delta^m = d = b^l c^m$ we can rewrite the first δ in the previous expression to obtain $\frac{b^{-j\lfloor\frac{lt}{m}\rfloor}c^{-jt}b^{l\lfloor\frac{jt}{m}\rfloor}c^{m\lfloor\frac{jt}{m}\rfloor}\delta^{k_j}}{b^{-\lfloor\frac{lk_j}{m}\rfloor}c^{-k_j}x_{k_j}}$. Now we collect powers of b and c. We have $b^{l\lfloor\frac{jt}{m}\rfloor+\lfloor\frac{lk_j}{m}\rfloor-j\lfloor\frac{lt}{m}\rfloor}$. Since $lt \equiv 1 \pmod m$ we can move the j inside the floor function to obtain $b^{l\lfloor\frac{jt}{m}\rfloor+\lfloor\frac{lk_j}{m}\rfloor-\lfloor\frac{jlt}{m}\rfloor}$. Earlier we showed that $\lfloor\frac{jlt}{m}\rfloor = l\lfloor\frac{jt}{m}\rfloor + \lfloor\frac{lk_j}{m}\rfloor$, which implies that the exponent of the b term is equal to zero. Also we have $c^{m\lfloor\frac{jt}{m}\rfloor+k_j-jt}$ and since $jt = m\lfloor\frac{jt}{m}\rfloor + k_j$, the exponent of the c term is also equal to zero. Hence $\frac{\beta^j}{y_j} = \frac{\delta^{k_j}}{x_{k_j}}$ which implies that $\{\frac{\delta^i}{x_i}\} = \{\frac{\beta^j}{y_j}\}$ which implies that $\frac{1}{m}\sum_{j=0}^{m-1}\frac{\beta^j}{y_j} \in \mathcal{O}_L$ which completes the proof. □

Applying the argument used in the proof of Theorem 2.5.25 we obtain:

Theorem 6.6.6. *Let m be an odd square free number, let K be a number field such that each prime number dividing m is unramified in K, and let L be a tamely ramified extension of K of degree m having the form $L = K(\delta)$ for some $\delta \in L$ such that $\delta^m \in K$. Let H be the Hopf algebra giving the unique almost classical Hopf-Galois structure on L/K. The ring of algebraic integers $\mathcal{O}_L$ is a free $\mathcal{A}_H$-module if and only if there exists $\beta \in \mathcal{O}_L$ such that*

1. *$L = K(\beta)$*
2. *$b = \beta^m \in \mathcal{O}_K$*
3. *The ideals $\prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}(b^k)}$ associated to b are principal with generators c_k such that*

$$y = \frac{1}{m}\sum_{k=0}^{m-1}\frac{\beta^k}{c_k} \in \mathcal{O}_L.$$

Furthermore in this case the element y is a free generator of $\mathcal{O}_L$ as an $\mathcal{A}_H$-module.

Bibliography

[AB18] Ali A Alabdali and Nigel P Byott. Counting Hopf–Galois structures on cyclic field extensions of squarefree degree. *Journal of Algebra*, 493:1–19, 2018.

[BCE18] Nigel P Byott, Lindsay N Childs, and G Griffith Elder. Scaffolds and generalized integral Galois module structure. In *Annales de l'Institut Fourier*, volume 68, pages 965–1010, 2018.

[BJ08] Werner Bley and Henri Johnston. Computing generators of free modules over orders in group algebras. *Journal of Algebra*, 320(2):836–852, 2008.

[Byo00] Nigel P Byott. Galois module structure and Kummer theory for Lubin-Tate formal groups. In *Algebraic Number Theory and Diophantine Analysis: Proceedings of the International Conference held in Graz, Austria, August 30 to September 5, 1998*. Walter de Gruyter, Berlin, 2000.

[Byo02] Nigel P Byott. Integral Hopf–Galois structures on degree p^2 extensions of p-adic fields. *Journal of Algebra*, 248(1):334–365, 2002.

[Chi00] Lindsay Childs. *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*. Number 80 of Mathematical Surveys and Monographs. American Mathematical Soc., 2000.

[CR81a] Charles W Curtis and Irving Reiner. Methods of representation theory with applications to finite groups and orders, vol. 1. *John Wiley & Sons, Inc., One Wiley Dr., Somerset, NJ 08873*, 1, 1981.

[CR81b] Charles W Curtis and Irving Reiner. Methods of representation theory with applications to finite groups and orders, vol. 2. *John Wiley & Sons, Inc., One Wiley Dr., Somerset, NJ 08873*, 2, 1981.

[DCR10] Ilaria Del Corso and Lorenzo Paolo Rossi. Normal integral bases for cyclic Kummer extensions. *Journal of Pure and Applied Algebra*, 214(4):385–391, 2010.

[DCR13] Ilaria Del Corso and Lorenzo Rossi. Normal integral bases and tameness conditions for Kummer extensions. *Acta Arithmetica*, 1(160):1–23, 2013.

[Frö83] Albrecht Fröhlich. *Galois module structure of algebraic integers*, volume 1 of A Series of Modern Surveys in Mathematics. Springer Science & Business Media, 1983.

[FT91] Albrecht Fröhlich and Martin J Taylor. *Algebraic number theory*, volume 27 of Cambridge studies in advanced Mathematics. Cambridge University Press, 1991.

[GA94] EJ Gómez Ayala. Bases normales d'entiers dans les extensions de Kummer de degré premier. *Journal de théorie des nombres de Bordeaux*, 6(1):95–116, 1994.

[GMR22] Daniel Gil-Muñoz and Anna Rio. Hopf-Galois module structure of quartic Galois extensions of $\mathbb{Q}$. *Journal of Pure and Applied Algebra*, 226(9):107045, 2022.

[GP87] Cornelius Greither and Bodo Pareigis. Hopf-Galois theory for separable field extensions. *Journal of Algebra*, (1):239–258, 1987.

[HGK81] Erich Hecke, Jay R Goldman, and R Kotzen. *Lectures on the theory of algebraic numbers*, volume 77 of Graduate Texts in Mathematics. Springer, 1981.

[Hil13] David Hilbert. *The theory of algebraic number fields*. Springer Science & Business Media, 2013.

[Ich04] Humio Ichimura. On the ring of integers of a tame Kummer extension over a number field. *Journal of Pure and Applied Algebra*, 187(1-3):169–182, 2004.

[Joh15] Henri Johnston. Explicit integral Galois module structure of weakly ramified extensions of local fields. *Proceedings of the American Mathematical Society*, 143(12):5059–5071, 2015.

[Koh98] Timothy Kohl. Classification of the Hopf-Galois structures on prime power radical extensions. *Journal of Algebra*, 207(2):525–546, 1998.

[Lan04] Serge Lang. *Algebra*, volume 211 of Graduate Texts in Mathematics. Springer Science & Business Media, 2004.

[Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322 of Grundlehren der mathematischen Wissenschaften. Springer Science & Business Media, 2013.

[Rom05] Steven Roman. *Field theory*, volume 158 of Graduate Texts in Mathematics. Springer Science & Business Media, 2005.

[Tho08] Lara Thomas. A valuation criterion for normal basis generators in equal positive characteristic. *Journal of Algebra*, 320(10):3811–3820, 2008.

[Tho10] Lara Thomas. On the Galois module structure of extensions of local fields. *Publications Mathematiques de Besançon*, pages 157–194, 2010.

[Tru11] Paul J Truman. Towards a generalisation of Noether's theorem to non-classical Hopf-Galois structures. *New York Journal of Mathematics*, 17:799–810, 2011.

[Tru20] Paul J Truman. Hopf-Galois module structure of tamely ramified radical extensions of prime degree. *Journal of Pure and Applied Algebra*, 224(5):106231, 2020.