SOME FAMILIES OF QUATERNION FIELDS AND THE SECOND CHINBURG CONJECTURE

By

JEFFREY JAMES HOOPER, B.Sc., M.Sc.

A Thesis
Submitted to the School of Graduate Studies
in Partial Fulfilment of the Requirements
for the Degree
Doctor of Philosophy

McMaster University

August, 1996

SOME FAMILIES OF QUATERNION FIELDS AND THE SECOND CHINBURG CONJECTURE

DOCTOR OF PHILOSOPHY (1996) MCMASTER UNIVERSITY

(Mathematics) Hamilton, Ontario

TITLE: Some Families of Quaternion Fields and the Second Chinburg Conjecture

AUTHOR: Jeffrey James Hooper

B.Sc., M.Sc.

SUPERVISOR: Professor V.P. Snaith

NUMBER OF PAGES: vi, 134

Abstract

Let N/K be a finite Galois extension of number fields with Galois group G. The second Chinburg conjecture asserts the equivalence in the locally free class group $CL(\mathbf{Z}[G])$ of the classes corresponding to two arithmetic invariants attached to the extension, namely the Fröhlich-Cassou-Noguès class $W_{N/K}$ and the second Chinburg invariant $\Omega(N/K, 2)$. Fröhlich originally formulated a conjectural equivalence of the class $W_{N/K}$ and the class $[\mathcal{O}_N]$ determined by the ring of integers in N, and this was subsequently verified by M. Taylor. The second Chinburg invariant $\Omega(N/K, 2)$ may be interpreted as a generalisation of the class $[\mathcal{O}_N]$ to wild extensions, and Chinburg showed that Fröhlich's conjecture for tame extensions implied Chinburg's conjecture for tame extensions.

More generally, the second Chinburg conjecture has been verified when G is absolutely abelian of odd conductor (C. Greither) and for several infinite families of wildly ramified quaternion fields (S. Kim). When N/K is wildly ramified and G is nonabelian, little further evidence for the conjecture is known.

In this thesis we consider some families of extensions $N/\mathbf{Q}$ with $G \cong Q_8$, the quaternion group of order 8, in which the prime 2 is totally ramified. In particular we consider those quaternion extensions containing a biquadratic subfield of the form $\mathbf{Q}(\sqrt{a}, \sqrt{b})$, where $a \equiv 2 \bmod 16$ and $b \equiv 3 \bmod 8$. We verify the second Chinburg conjecture for all such extensions.

We begin by localizing at the prime 2 and make use of a cohomological classification of a large class of cohomologically trivial 2-primary $\mathbf{Z}[Q_8]$-modules to explicitly compute the local second Chinburg invariant. Globally, we construct a projective $\mathbf{Z}[Q_8]$-module, X, that lies inside O_N, the ring of integers of N. We then work with Fröhlich's Hom-description of the class group and show that, in fact, $[X] = W_{N/\mathbf{Q}}$ in $CL(\mathbf{Z}[Q_8])$, where $[X]$ denotes the class of X. Combining this with the local information, and using congruence methods, we conclude that in $CL(\mathbf{Z}[Q_8])$,

$$\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}},$$

i.e., the second Chinburg conjecture holds for these extensions.

Combining this result with work of S. Kim, V. Snaith and M. Tran, this establishes the second Chinburg conjecture for all extensions $N/\mathbf{Q}$ having Galois group $G \cong Q_8$.

Contents

Chapter 1

Introduction

Perhaps the origin of Galois module structure is the so-called Normal Basis Theorem for a finite Galois extension L/K of fields. This asserts that as a K-vector space, the field L has a basis of the form $\{a^g\}$, where a is some fixed element of L and g runs through all elements of the Galois group $G = G(L/K)$. A basis of this special form is called a normal basis for L (with respect to K). An alternate way to state this result is that L is a free $K[G]$-module of rank one.

In case $N/\mathbf{Q}$ is a number field, with $G = Gal(N/\mathbf{Q})$, we can attempt to generalize this result. Inside N there are two obvious subrings that can be compared in a similar fashion, namely the ring $\mathcal{O}_N$ of integers of N and the ring $\mathbf{Z}$ of rational integers. Thus, a natural question arises as to whether $\mathcal{O}_N$ has a similar $\mathbf{Z}$-basis of the form $\{a^g\}$ for a fixed $a \in \mathcal{O}_N$ and with g running over G. When such a basis exists, it is commonly referred to as a normal integral basis, and the problem as to whether or not such a basis exists is called the normal integral basis problem. In terms of modules, the corresponding problem is to decide under what conditions $\mathcal{O}_N$ is a free $\mathbf{Z}[G]$-module.

As with most problems in number theory, a first approach is to attack the

problem locally and try to piece together the local information to achieve a global result. To this end, we denote by E/F a finite Galois extension of p-adic local fields with Galois group $G = G(E/F)$ and let $\mathcal{O}_E$ and $\mathcal{O}_F$ denote the respective valuation rings of E and F. In this setting a result of E. Noether (see [12, pp. 26-7]) states that $\mathcal{O}_E$ is free as an $\mathcal{O}_F[G]$-module precisely when the extension E/F is at most tamely ramified.

Returning to the number field situation, we say that the $\mathbf{Z}[G]$-module M is locally free if the $\mathbf{Q}[G]$-module $M \otimes_{\mathbf{Z}} \mathbf{Q}$ is free, and if each of the localisations $M \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a free $\mathbf{Q}_p[G]$-module. Noether's Theorem then implies that $\mathcal{O}_N$ is a locally free $\mathbf{Z}[G]$-module if and only if the extension $N/\mathbf{Q}$ is tame (meaning that each prime p is at most tamely ramified).

Clearly then, this last result implies that in order for $\mathcal{O}_N$ to have a normal integral basis, the extension $N/\mathbf{Q}$ must be tame. However, in this global setting the question remained as to whether or not every tame extension of number fields admitted a normal integral basis.

This question had, in fact, already been resolved in the abelian setting by a result due essentially to Hilbert in the late nineteenth century (cf. [12]). For abelian extensions one may use the Kronecker-Weber Theorem to show that for every tame extension N of $\mathbf{Q}$, the ring of integers $\mathcal{O}_N$ has a normal integral basis. Of course for nonabelian extensions, nothing as powerful as the Kronecker-Weber Theorem exists, making the corresponding problem more difficult. In 1969, J. Martinet [21] managed to prove the existence of a normal integral basis for all tame extensions $N/\mathbf{Q}$ having Galois group $Gal(N/\mathbf{Q}) \cong D_{2p}$, the dihedral group of order $2p$, where p is an odd prime.

Martinet then directed his attention at tame extensions $N/\mathbf{Q}$ for which the Galois group is isomorphic to Q_8, the quaternion group of order 8, and further progress came to an abrupt halt. He found that for Q_8 there are two possible

structures of locally free $\mathbf{Z}[Q_8]$-modules of rank one, and that each of these possibilities occurred as $\mathcal{O}_N$ for some such N. Hence he found examples of tame Galois extensions $N/\mathbf{Q}$ with $Gal(N/\mathbf{Q}) \cong Q_8$, and for which no normal integral basis exists.

This is not a satisfactory situation. Following the usual mathematical route, we would like to be able to describe the obstruction to the existence of such a basis for $\mathcal{O}_N$. To be plain, we ask: Why does a normal integral basis exist for some tame extensions $N/\mathbf{Q}$ and not for others, and in the case where no such basis exists, what is preventing its existence?

In order to proceed with such an inquiry, we are naturally led to look for ways in which we may classify the different isomorphism classes of locally free $\mathbf{Z}[G]$-modules that may occur. One standard approach is via a Grothendieck-type group, although in general such an approach can only be expected to classify modules up to stable isomorphism. So let $K_0(\mathbf{Z}[G])$ be the Grothendieck group generated by isomorphism classes of locally free $\mathbf{Z}[G]$-modules and with relations corresponding to short exact sequences. We use the notation (M) to denote the class in $K_0(\mathbf{Z}[G])$ corresponding to the locally free $\mathbf{Z}[G]$-module M. We define a homomorphism

$$rank : K_0(\mathbf{Z}[G]) \longrightarrow \mathbf{Z}$$

by demanding that, for each locally free $\mathbf{Z}[G]$-module M,

$$rank((M)) = rank_{\mathbf{Q}[G]}(M \otimes_{\mathbf{Z}} \mathbf{Q}).$$

The locally free class group, $\mathcal{CL}(\mathbf{Z}[G])$, is now defined to be the kernel of this homomorphism. The class in $\mathcal{CL}(\mathbf{Z}[G])$ determined by the locally free module M will be denoted by $[M]$. In particular, we have a short exact sequence of abelian groups of the form

$$0 \longrightarrow \mathcal{CL}(\mathbf{Z}[G]) \longrightarrow K_0(\mathbf{Z}[G]) \longrightarrow \mathbf{Z} \longrightarrow 0. \qquad (1.0.1)$$

There is a natural injection

$$\mathbf{Z} \longrightarrow K_0(\mathbf{Z}[G])$$

induced by sending a positive integer n to the class $((\mathbf{Z}[G])^n)$, and this clearly provides a splitting of (1.0.1). In particular, we may also view $\mathcal{CL}(\mathbf{Z}[G])$ as a quotient of $K_0(\mathbf{Z}[G])$.

These two groups and the homomorphism $rank$ give a fairly satisfactory classification of locally free $\mathbf{Z}[G]$-modules. Precisely, if X and Y are two locally free $\mathbf{Z}[G]$-modules which satisfy $rank(X) = rank(Y)$ and are such that $[X] = [Y] \in \mathcal{CL}(\mathbf{Z}[G])$, then X and Y are stably isomorphic, i.e. $X \oplus (\mathbf{Z}[G])^n \cong Y \oplus (\mathbf{Z}[G])^n$. In many cases, for example when G is abelian or of odd order, we have 'cancellation' in the sense that stably isomorphic locally free $\mathbf{Z}[G]$-modules are actually isomorphic.

For the moment we leave off this discussion in order to consider a connection between the classification of locally free $\mathbf{Z}[G]$-modules on the one hand, and objects of analytic origin on the other. If ρ is a character of G and we let $\Lambda_{\mathbf{Q}}(s,\rho)$ be the extended Artin L-function associated to ρ (see Section 1.3), then $\Lambda_{\mathbf{Q}}(s,\rho)$ satisfies a functional equation

$$\Lambda_{\mathbf{Q}}(1-s,\rho) = W_{\mathbf{Q}}(\rho)\,\Lambda_{\mathbf{Q}}(s,\overline{\rho}),$$

where $\overline{\rho}$ is the complex conjugate of ρ. The complex number of modulus 1 which occurs in this relation, $W_{\mathbf{Q}}(\rho)$, is called the Artin root number of ρ. When ρ is real-valued, and in particular if ρ is orthogonal or symplectic, it can be shown that $W_{\mathbf{Q}}(\rho) \in \{\pm 1\}$. Moreover, A. Fröhlich and J. Queyrut ([13]) have shown that in fact for an orthogonal representation ρ we actually have that $W_{\mathbf{Q}}(\rho) = 1$.

The entire discussion above generalizes naturally to the case of tame, relative Galois extensions N/K of number fields.

We return now to the difficulty encountered by Martinet during his examination of the normal integral basis problem for tame quaternion extensions of $\mathbf{Q}$. Let ρ_s denote the unique irreducible, symplectic representation of Q_8 and set $W_N = W_{\mathbf{Q}}(\rho_s)$. In the early 1970's Serre had the idea (cf. [12, p.12]) that perhaps we have $W_N = 1$ exactly when the ring of integers $\mathcal{O}_N$ has a normal integral basis. In [9] Fröhlich verified that this was indeed the case. The search then began to find a suitable generalisation of this fact for general tame extensions N/K.

Ph. Cassou-Noguès gave the appropriate generalisation, in the form of a class $W_{N/K}$ in $\mathcal{CL}(\mathbf{Z}[G])$, which is defined using only the values of Artin root numbers of symplectic representations (cf. [12] or [35]). After several explicit examples were computed (see for example [1] and [34]), Fröhlich conjectured that in $\mathcal{CL}(\mathbf{Z}[G])$ this analytic class, $W_{N/K}$, should in fact equal the class $[\mathcal{O}_N]$ of the ring of integers. In 1981, M. Taylor established this important connection:

Theorem 1.0.1 *([35]) Let N/K be a tame Galois extension of number fields with $G = Gal(N/K)$. Then*

$$[\mathcal{O}_N] = W_{N/K} \in \mathcal{CL}(\mathbf{Z}[G]). \qquad \square$$

Taylor's Theorem puts an end to the matter, at least in the case of tame extensions of number fields.

In the early 1980's, in connection with work on the multiplicative Galois module structure of S-units and Tate's formulation of the Stark conjectures, T. Chinburg ([3],[4]) introduced three elements, $\Omega(N/K, i)$ $(i = 1, 2, 3)$, of the class group $\mathcal{CL}(\mathbf{Z}[G])$ which are invariants of the extension, i.e. depend only

on the extension N/K. These invariants satisfy the basic relation

$$\Omega(N/K,2) = \Omega(N/K,1) + \Omega(N/K,3) \in \mathcal{CL}(\mathbf{Z}[G]). \qquad (1.0.2)$$

In fact, Chinburg was able to show that, in the case of a tame extension N/K of number fields, there is an equality

$$\Omega(N/K,2) = [\mathcal{O}_N] \in \mathcal{CL}(\mathbf{Z}[G]).$$

Moreover, since $\Omega(N/K,2)$ is defined for general extensions, without the tameness hypothesis, we may regard $\Omega(N/K,2)$ as a generalisation of $[\mathcal{O}_N]$ to wildly ramified extensions. In fact, the definition of the Cassou-Noguès-Fröhlich class $W_{N/K}$ can also be extended to the wild case. This idea of regarding $\Omega(N/K,2)$ as a generalisation of $[\mathcal{O}_N]$ led Chinburg to formulate the following conjectures:

Conjecture 1.0.2 *(Chinburg [4]) If N/K is a finite Galois extension of number fields, then in $\mathcal{CL}(\mathbf{Z}[G])$,*

$$(1) \quad \Omega(N/K,1) = 0;$$

$$(2) \quad \Omega(N/K,2) = W_{N/K};$$

$$(3) \quad \Omega(N/K,3) = W_{N/K}.$$

By equation (1.0.2) any two of these conjectured relationships implies the remaining one. Most of the work on these conjectures has therefore been concentrated on establishing the second and third of these equalities, which in the literature have come to be known as the second and third Chinburg conjectures.

In this thesis we establish the second Chinburg conjecture for certain quaternion extensions $N/\mathbf{Q}$ for which the prime 2 is totally ramified. Let us therefore pause to briefly discuss what has already been established regarding this conjecture.

As we remarked above, Chinburg showed in [4] that in the tame case conjecture (2) follows from Taylor's Theorem.

As regards further work in the case of wild extensions $N/\mathbf{Q}$, Chinburg [5] has verified several families of examples, and S. Kim [19], [20] has proved that this conjecture holds for all quaternion fields $N/\mathbf{Q}$ for which the prime 2 is not totally ramified. In his doctoral thesis ([37]), M. Tran has established the conjecture for an infinite family of quaternion fields where the prime 2 is totally ramified. The remaining quaternion extensions will be considered in this thesis.

In terms of results regarding the second Chinburg conjecture for general fields, we briefly mention two. Presently, the most powerful general result is that of D. Holland [17] who established that

$$\Omega(N/K,2) - W_{N/K} \in D(\mathcal{O}_K[G]).$$

This result provides the best evidence that the second Chinburg conjecture should hold for all extensions of number fields. More recently, C. Greither ([14]) has established the second conjecture for all absolutely abelian fields having odd conductor.

Other recent work has been done in the direction of extending the ideas of the Chinburg conjectures, in particular the third conjecture, to 'higher' Chinburg invariants. Chinburg, Kolster, Pappas and Snaith [6] have defined a sequence of 'higher' Chinburg invariants $\Omega_n(N/K)$ which are related to the algebraic K-groups of the ring of integers $\mathcal{O}_N$ in dimensions $2n$ and $2n+1$, as well as to values of L-functions at the special value $s = -n$. These new invariants are conjectured to satisfy relations similar to the original ones. In addition, D. Burns and M. Flach have independently defined similar invariants $\Omega_n(N/K)'$, which are also related to conjectures of Bloch-Kato, Kato, and

Fontaine and Perrin-Riou.

Now let us consider the results of this thesis in more detail. We write Q_8 for the quaternion group of order 8, which can be written in terms of generators and relations as

$$Q_8 = \left\{ x, y \mid x^4 = 1,\, x^2 = y^2,\, yxy^{-1} = x^{-1} \right\}.$$

If we then let $N/\mathbf{Q}$ be a quaternion field, (i.e. a Galois extension of $\mathbf{Q}$ with Galois group isomorphic to Q_8), then such a field contains a unique biquadratic subfield

$$E = \mathbf{Q}(\sqrt{d_1}\,,\, \sqrt{d_2}\,).$$

If in addition we demand that the prime 2 totally ramifies in N, then such extensions can be broken up into two families. For any such extension, either

$$d_1 \equiv 10 \pmod{16} \qquad \textit{and} \qquad d_2 \equiv 3 \pmod{8}$$

or

$$d_1 \equiv 2 \pmod{16} \qquad \textit{and} \qquad d_2 \equiv 3 \pmod{8}.$$

The second Chinburg conjecture has been verified by M. Tran [37] for the first family. Here we concentrate on the second.

The object of this thesis is to prove the following theorem.

Theorem 1.0.3 *Let $N/\mathbf{Q}$ be a quaternion field in which the prime 2 is totally ramified and whose biquadratic subfield E has the form $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$, where d_1 and d_2 satisfy*

$$d_1 \equiv 2 \pmod{16} \qquad \textit{and} \qquad d_2 \equiv 3 \pmod{8}.$$

Then

$$\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}} \in \mathcal{CL}(\mathbf{Z}[Q_8]). \qquad \square$$

Combining this theorem with the aforementioned work of Kim [20] and Tran [37], as well as that of Snaith [32], yields the following more general result.

Theorem 1.0.4 *For any quaternion field $N/\mathbf{Q}$, we have*

$$\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}} \in \mathcal{CL}(\mathbf{Z}[Q_8]) . \qquad \square$$

We now give a more detailed description of the contents of this thesis.

In Chapter 2 we begin outlining the definitions and important properties of the relevant background material needed. None of the material in this chapter is original, and we have omitted many of the proofs, referring the reader to the appropriate literature.

We begin in Section 2.1 with the definition and first properties of the locally free class group. We present this group using a Grothendieck construction and discuss the explicit description of its elements. Finally, since our results concern only the quaternion group of order 8, we close with a description of the class group of $\mathbf{Z}[Q_8]$.

The next section, Section 2.2, concentrates on a different description of the locally free class group, the Hom-description of Fröhlich. This new formulation provides a much more concrete description of elements as the equivalence classes of certain types of homomorphisms. In order to set notation, we start with a brief review of the definitions of the idèle and adèle rings. Next we introduce Fröhlich's Det construction and show how this construction gives information about elements of the class group. We also introduce the kernel group $D(\mathbf{Z}[G])$ and present a similar Hom-description of this group.

The focus of Section 2.3 is on analytic prerequisites and the construction of the class $W_{N/K}$ of Cassou-Noguès and Fröhlich. We start with a review of the extended Artin L-function for a complex representation ρ and its functional

equation, and show how the Artin root number $W_K(\rho)$ arises. This complex number of modulus one may actually be computed using local information, and so we next discuss local root numbers and local Gauss sums, and show how these local root numbers can be combined to compute the Artin root number. Finally, we use Fröhlich's Hom-description to construct the analytic root number class $W_{N/K}$ in the class group.

Section 2.4 centers on the definition of the second Chinburg invariant $\Omega(N/K, 2)$. We begin by outlining the construction of all three Chinburg invariants, since the three invariants are products of the same construction process. The formation of these invariants clarifies the way in which they are related. Following this, we introduce the notion of a local version of the second invariant and introduce a formula due to Kim, which shows how the local Chinburg invariants at wild primes may be combined to evaluate $\Omega(N/K, 2)$. We close this section by discussing the Chinburg conjectures, and we give some supporting evidence for the second conjecture.

In the final section of Chapter 2, we specialize to the case of quaternion fields. We introduce Hilbert symbols and show how these symbols may be used to classify quaternion fields. We outline Kim's result, which reduces us to considering only those which are totally ramified at the prime 2. We then point out Tran's result, and turn our attention to the infinite family of quaternion fields that will be of interest to us and the statement of our main theorem.

In Chapter 3, we concentrate on the local situation at the prime 2. We begin by considering the possible localisations $L/\mathbf{Q}_2$ at the prime 2. After giving explicit constructions of two local quaternion fields, we then prove that these are the only possibilities which can occur. Next we introduce the fundamental 2-extension, which represents the fundamental class in $H^2(Q_8; L^*)$ and use it

to construct an explicit 2-cocycle. The map is constructed in such a way as to be injective and we write M for its cokernel.

The proof of the main theorem is the focus of Chapter 4. In the first section, we use Kim's formula to compute the second Chinburg invariant. The local invariant which occurs incorporates information regarding the class of the cokernel M. We reduce the proof of the main theorem to a series of three propositions regarding the precise values of the classes which occur in Kim's formula.

In each of the remaining sections, we prove one of these three propositions, completing the proof of the main result.

Acknowledgements

I would like to take this opportunity to thank Professor Snaith for his supervision of this thesis. I would also like to thank Minh Tran for many helpful discussions.

I also want to thank my friends Boris Brauckmann, Eric Derbez, Spiro Daoussis, Franco Guerriero, Mike Pfau, Bob Stamicar, Paul Stephenson, Gavin Stuttard and Minh Tran for doing their utmost to increase the level of insanity within the department during the past four years.

Most importantly, I wish to thank my wife Christine, without whom this work would not have been possible. Her constant encouragement and endless patience have been a source of inspiration during the years.

This thesis was typeset using the LaTeX typesetting system.

Chapter 2

Background

This first chapter describes most of the background material necessary for an understanding of the proof of the main theorem. The chapter is by no means exhaustive, and we have referred the reader to the literature for many results whose proofs involve too much of a digression.

2.1 The Locally Free Class Group

In this section, we define the main group in which all of our computations and comparisons take place, namely the locally free class group $\mathcal{CL}(\mathcal{O}_K[G])$. Throughout this section, N/K will denote a finite Galois extension of number fields with Galois group $G = G(N/K)$.

We first recall the definition of locally free module. The $\mathcal{O}_K[G]$-module M is called **locally free** if $M \otimes_{\mathcal{O}_K} K$ is a free $K[G]$-module, while for each prime P of K, $M \otimes_{\mathcal{O}_K} \mathcal{O}_{K_P}$ is a free $\mathcal{O}_{K_P}[G]$-module. Furthermore, M is said to be **locally free of rank one** if each of the corresponding localizations of M are free modules on single generators. We will be considering $\mathbf{Z}[G]$-modules, and we note in passing that a finitely generated $\mathbf{Z}[G]$-module is locally free if and

only if it is projective.

Let $K_0(\mathcal{O}_K[G])$ be the Grothendieck group generated by all isomorphism classes of finitely generated, locally free $\mathcal{O}_K[G]$-modules and with relations corresponding to short exact sequences. Specifically, this means that in order to construct $K_0(\mathcal{O}_K[G])$, we take the free abelian group with one generator $\{M\}$ for each isomorphism class of finitely generated, locally free $\mathcal{O}_K[G]$-module M, and factor out by the subgroup generated by relations of the form

$$\{M_1\} + \{M_3\} = \{M_2\},$$

whenever there is an exact sequence of finitely generated, locally free $\mathcal{O}_K[G]$-modules of the form

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0.$$

Throughout the following discussion we will use the notation (M) to denote the class in $K_0(\mathcal{O}_K[G])$ corresponding to the locally free $\mathcal{O}_K[G]$-module M. We define a homomorphism

$$rank : K_0(\mathcal{O}_K[G]) \longrightarrow \mathbf{Z} \tag{2.1.3}$$

by demanding that, for each finitely generated, locally free $\mathcal{O}_K[G]$-module M,

$$rank((M)) = rank_{K[G]}(M \otimes_{\mathcal{O}_K} K).$$

Definition 2.1.1 *We define the* **locally free class group,** $\mathcal{CL}(\mathcal{O}_K[G])$ *to be the kernel of the homomorphism (2.1.3).*

The class in $\mathcal{CL}(\mathcal{O}_K[G])$ determined by the finitely generated, locally free module M will be denoted by $[M]$.

Note that in particular we have a short exact sequence of abelian groups of the form

$$0 \longrightarrow \mathcal{CL}(\mathcal{O}_K[G]) \longrightarrow K_0(\mathcal{O}_K[G]) \longrightarrow \mathbf{Z} \longrightarrow 0. \tag{2.1.4}$$

There is also a natural injection

$$\mathbf{Z} \longrightarrow K_0(\mathcal{O}_K[G])$$

induced by sending a positive integer n to the class $((\mathcal{O}_K[G])^n)$, and this clearly provides a splitting of (2.1.4). So we may also view $\mathcal{CL}(\mathcal{O}_K[G])$ as a quotient of $K_0(\mathcal{O}_K[G])$.

We note in passing that equality of classes in $\mathcal{CL}(\mathcal{O}_K[G])$ does not, in general imply that the corresponding modules are isomorphic. More precisely, if X and Y are two locally free $\mathcal{O}_K[G]$-modules which satisfy $rank(X) = rank(Y)$ and are such that $[X] = [Y] \in \mathcal{CL}(\mathcal{O}_K[G])$, then X and Y are stably isomorphic, i.e., $X \oplus (\mathcal{O}_K[G])^n \cong Y \oplus (\mathcal{O}_K[G])^n$.

As an alternative to this description, we may construct the class group in terms of generators and relations as follows. We consider the free abelian group $\mathcal{M}$ generated by the isomorphism classes of finitely generated, locally free $\mathcal{O}_K[G]$-modules and we define an equivalence relation, $\sim$, on $\mathcal{M}$ using the relations

(a) $(M_1) \sim (M_2)$ if there exist positive integers m and n such that

$$M_1 \oplus (\mathcal{O}_K[G])^m \cong M_2 \oplus (\mathcal{O}_K[G])^n$$

and

(b) $(M_1) + (M_3) \sim (M_2)$ whenever there exists an exact sequence of $\mathcal{O}_K[G]$-modules of the form

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0\,.$$

We then have

$$\mathcal{CL}(\mathcal{O}_K[G]) = \mathcal{M}/\sim\,.$$

Note that as a particular case of condition (b) above, we have that in $\mathcal{CL}(\mathcal{O}_K[G])$, $[M_1] + [M_2] = [M_1 \oplus M_2]$.

For the extensions considered in this thesis we have $K = \mathbf{Q}$ and $G \cong Q_8$, so that $\mathcal{O}_K = \mathbf{Z}$. In particular we will be doing all of our computations in the class group $\mathcal{CL}(\mathbf{Z}[Q_8])$. We end this section with an explicit description of this group. To be precise, we wish to describe an isomorphism of the form

$$n : \mathcal{CL}(\mathbf{Z}[Q_8]) \longrightarrow (\mathbf{Z}/4)^* \cong \mathbf{Z}/2 .$$

Although we will refrain from digressing to give the entire proof, we will explain the manner in which the element $n([M])$ is constructed.

To this end let M be a finitely generated, projective (i.e. locally free) $\mathbf{Z}[Q_8]$-module and denote by x^2 the element of order 2 in Q_8. We define two auxiliary modules M_+ and M_- by

$$M_+ = \{m \in M \mid x^2(m) = m\}$$

and

$$M_- = \{m \in M \mid x^2(m) = -m\} .$$

Then M_+ can be viewed in a natural way as a module over the ring

$$\mathbf{Z}[Q_8]/(x^2 - 1) \cong \mathbf{Z}[V] ,$$

where V is Klein's four group, and M_- is a module over the ring

$$\mathbf{Z}[Q_8]/(x^2 + 1) \cong \mathbf{H}_\mathbf{Z} ,$$

where by $\mathbf{H}_\mathbf{Z}$ we mean the ring of integral quaternions,

$$\mathbf{H}_\mathbf{Z} = \mathbf{Z}[i, j, k]/(i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j).$$

A proof of the following result can be found in [23].

Proposition 2.1.2 *Let R be the ring $\mathbf{Z}[V]$ or $\mathbf{H}_\mathbf{Z}$. Then every finitely generated, projective R-module is free.*

As a particular case we have that M_+ is a free $\mathbf{Z}[V]$-module and M_- is a free $\mathbf{H_Z}$-module.

Proposition 2.1.3 *Let M be a finitely generated, projective $\mathbf{Z}[Q_8]$-module. Then the map*

$$\psi_M \,:\, m + M_- \longmapsto (1+x^2)\,m$$

defines a $\mathbf{Z}[V]$-isomorphism

$$\psi_M \,:\, M/M_- \xrightarrow{\cong} M_+ \,.$$

Proof: First, since $x^2 \in Z(Q_8)$, the center of Q_8, every element of $\mathbf{Z}[V]$ commutes with $1+x^2$, so that ψ_M is indeed a $\mathbf{Z}[V]$-map. Also, it is clear that $(1+x^2)m = 0$ if and only if $x^2(m) = -m$, i.e. if and only if $m \in M_-$, which implies that ψ_M is injective.

It suffices then to prove surjectivity. For this it is enough to notice that M is projective over the ring $\mathbf{Z}[\{x^2\}] \cong \mathbf{Z}[\mathbf{Z}/2]$, so that $H^2(\{x^2\}; M)$ is trivial. But $H^2(\{x^2\}; M)$ is equal to

$$M^{\{x^2\}}/(1+x^2)M = M_+/(1+x^2)M \,.$$

Hence $M_+ = (1+x^2)M$ and ψ_M is surjective. □

We now choose a free $\mathbf{H_Z}$-basis $\{a_1, \ldots, a_k\}$ for M_-. By Proposition 2.1.3 we may choose $\alpha_1, \ldots, \alpha_k \in M$ so that

$$\{\alpha_1 + M_-, \ldots, \alpha_k + M_-\}$$

is a free $\mathbf{Z}[V]$-basis for $M/M_- \cong M_+$. Consider the set

$$\{(1-x^2)\alpha_1, \ldots, (1-x^2)\alpha_k\} \subset M_- \,.$$

Since these lie in M_-, we must be able to express them in terms of the basis $\{a_1, \ldots, a_k\}$. In particular, this means there exists a $k \times k$ matrix X in $M_k(\mathbf{H}_\mathbf{Z})$ such that as elements of M_-^k,

$$\begin{pmatrix} (1-x^2)\alpha_1 \\ \vdots \\ (1-x^2)\alpha_k \end{pmatrix} = X \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}.$$

We let

$$c : M_k(\mathbf{H}_\mathbf{Z}) \longrightarrow M_{2k}(\mathbf{Z}[i])$$

denote the usual complexification map. Finally, we define

$$n([M]) = det(c(X)) \ \ (modulo\ 4).$$

Theorem 2.1.4 *The above construction yields an element*

$$n([M]) \in (\mathbf{Z}/4)^* \cong \mathbf{Z}/2,$$

which depends only on $[M]$, the class of M in $\mathcal{CL}(\mathbf{Z}[Q_8])$, and defines an isomorphism

$$n : \mathcal{CL}(\mathbf{Z}[Q_8]) \longrightarrow (\mathbf{Z}/4)^* \cong \mathbf{Z}/2.$$

Proof: See [31, pp. 179-185]. □

2.2 The Hom Description of the Class Group

In this section, we discuss a different description of the class group of Section 2.1 in terms of homomorphisms and determinants, originally due to A. Fröhlich. This description will be used at several key places in the proof of Theorem 2.5.10. The material of this section is given in greater detail in [8, Vol. II,p. 329–342].

2.2.1 Adèles and Idèles

In order to fix notation, we begin by recalling some notions regarding adèles and idèles. Let K be a number field. In this section we consider a method of combining local information of elements of the various completions K_P at primes P of K. Throughout we use the convention that $\mathcal{O}_{K_P} = K_P$ whenever P is an Archimedean prime. The adèle ring $\mathbf{A}(K)$ of K is now defined to be the ring

$$\mathbf{A}(K) = \prod'_{P \text{ prime}} K_P,$$

where by $\prod'$ we mean that we take those elements of the full product ring for which almost all entries lie in the ring of integers, $\mathcal{O}_{K_P}$. The group of idèles, $J(K)$, is the group of units in $\mathbf{A}(K)$:

$$J(K) = \{(\lambda_P) \in \mathbf{A}(K) \mid \lambda_P \in K_P^* \textit{ and almost everywhere } \lambda_P \in \mathcal{O}_{K_P}^*\}.$$

Here, as usual, $\mathcal{O}_{K_P}^*$ denotes the multiplicative group of units in $\mathcal{O}_{K_P}$. The subgroup of unit idèles is the subgroup consisting of all idèles in which all entries lie in $\mathcal{O}_{K_P}^*$, i.e.

$$U(\mathcal{O}_K) = \prod_{P \text{ prime}} \mathcal{O}_{K_P}^*.$$

Suppose now that G is a finite group. The notions of adèles and idèles may be extended in a natural way to the group-rings $\mathcal{O}_K[G]$ and $K[G]$ by defining, in a similar manner,

$$\mathbf{A}(K[G]) = \prod'_{P \text{ prime}} K_P[G];$$

$$J(K[G]) = \{(\alpha_P) \in \mathbf{A}(K[G]) \mid \alpha_P \in K_P[G]^*;\ \alpha_P \in \mathcal{O}_{K_P}[G]^*,\ \textit{almost all } P\};$$

$$U(\mathcal{O}_K[G]) = \prod_{P \text{ prime}} \mathcal{O}_{K_P}[G]^*.$$

As in the case of the ordinary adèle ring, the weak product in the definition of $\mathbf{A}(K[G])$ means that we take those elements of the full product ring for which almost all entries lie in $\mathcal{O}_{K_p}[G]$.

We now consider the Galois action on these objects. To this end, suppose that E/K is a finite Galois extension with Galois group $G(E/K)$. The group $G(E/K)$ acts on the set of primes of E and hence acts upon each of the groups $J(E)$, $U(\mathcal{O}_E)$, $J(E[G])$ and $U(\mathcal{O}_E[G])$. In particular, we may use this action to define a continuous action of the absolute Galois group Ω_K on these groups by first projecting to $G(E/K)$.

Recall now that if K is any subfield of the complex numbers and G denotes an arbitrary group, then the K-**representation ring** of G, $R_K(G)$, is defined to be the free abelian group on the irreducible K-representations of G. This definition means that an element of $R_K(G)$ is a formal linear combination of the form $\sum_i n_i V_i$, where the n_i are integers and the V_i are the finitely many irreducible K-representations of G. For the properties of the representation ring that we need, we refer the reader to [8] or [31].

If we now return to the case considered above, in which G is a finite group and E/K is a finite Galois extension of number fields with Galois group $G(E/K)$, and now assume that the extension field E is large enough to contain all $|G|$-th roots of unity, then E is a splitting field for G. In this case $R_E(G) \cong R_{\mathbf{C}}(G)$ is also a $\mathbf{Z}[G]$-module. We may therefore consider the group of G-equivariant maps

$$Hom_{G(E/K)}(R(G), J(E)) \cong Hom_{\Omega_K}(R(G), J(E)).$$

where we use the notation $R(G)$ for the full representation ring $R_{\mathbf{C}}(G)$.

2.2.2 The Map Det and Fröhlich's Hom Description

We keep the notaion introduced in the previous paragraph. In particular, E/K is a finite Galois extension of number fields with Galois group G and E is large enough so as to contain all $|G|$-th roots of unity.

Now let M be an $\mathcal{O}_K[G]$-module of rank one which is locally free (cf. Section 2.1). We denote by x_0 the free generator of the $K[G]$-module $M \otimes_{\mathcal{O}_K} K$ and for each prime P of K we write x_P for the free generator of the $\mathcal{O}_{K_P}[G]$-module $M \otimes_{\mathcal{O}_K} \mathcal{O}_{K_P}$. Notice that $K[G]$ and $\mathcal{O}_{K_P}[G]$ are subrings of $K_P[G]$, so that we may compare the corresponding bases for the $K_P[G]$-module $M \otimes_{\mathcal{O}_K} K_P$. This means that for each P there exists a unit $\lambda_P \in K_P[G]^*$ defined by

$$\lambda_P \cdot x_0 = x_P \in M \otimes_{\mathcal{O}_K} K_P .$$

Moreover, for almost all P, λ_P will lie in $\mathcal{O}_{K_P}[G]^*$, and hence we obtain an idèle $(\lambda_P) \in J(K[G])$.

This sort of construction actually works in more generality. If M is a locally free module of rank n, a similar comparison of bases yields an invertible $n \times n$-matrix with adèlic entries,

$$(\lambda_P) \in GL_n(\mathbf{A}(K[G])) .$$

If we write, as usual, $K_1(R)$ for the first algebraic K-group of the ring R, then we may of course obtain from this (λ_P) an element

$$(\lambda_P) \in K_1(\mathbf{A}(K[G])) = \prod'_{P \text{ prime}} K_1(K_P[G]).$$

(Here the symbol $\prod'$ means that the given product is a weak product in the sense that almost all of the entries lie in $K_1(\mathcal{O}_{K_P}[G])$).

Suppose now that ρ is a representation of G,

$$\rho : G \longrightarrow GL_m(E) .$$

Such a map extends linearly to a map on $K_P[G]$ and hence to maps of both $GL_n(K_P[G])$ and $K_1(K_P[G])$. Applying the map ρ to each $\lambda_P \in GL_n(K_P[G])$, we obtain an invertible matrix

$$\rho(\lambda_P) \in M_{mn}(K_P \otimes_K E).$$

Similarly, we may apply ρ to each $\lambda_P \in K_1(K_P[G])$ to obtain an invertible matrix

$$\rho(\lambda_P) \in K_1(K_P \otimes_K E) \cong (K_P \otimes_K E)^*.$$

Since there is an isomorphism of rings

$$K_P \otimes_K E \cong \prod_{Q|P} E_Q,$$

we obtain an element

$$det(\rho(\lambda_P)) \in \prod_{Q|P} E_Q^*.$$

Finally, since $(\lambda_P) \in GL_n(\mathbf{A}(K[G]))$, we obtain an Ω_K-equivariant map, given by this element $det(\rho(\lambda_P))$ at the primes of E which divide P,

$$Det((\lambda_P)) \in Hom_{\Omega_K}(R(G), J(E)).$$

To summarize, this process constructs, for each finitely generated, locally free $\mathcal{O}_K[G]$-module M, a homomorphism $Det((\lambda_P))$ of the specified form. This construction depended upon the choices made as to the basis elements x_0 and x_P.

We now consider the way in which these choices affect the homomorphism obtained. For simplicity, we will only describe the situation for modules of rank one, the discussion being similar for modules of higher rank.

Suppose then that in lieu of x_P we select at each prime P a generator x'_P. These generators are related by an equation of the form $x'_P = u_P x_P$ for some

$u_P \in \mathcal{O}_{K_P}[G]^*$. Combining the u_P we obtain a unit idèle

$$u = (u_P) \in U(\mathcal{O}_K[G]),$$

so that the above homomorphism $Det((\lambda_P))$ will be adjusted by multiplication by the map

$$Det(u) \in Det(U(\mathcal{O}_K[G])) \subset Hom_{\Omega_K}(R(G), J(E)).$$

By a similar argument, changing x_0 to x_0' will change $Det((\lambda_P))$ by a function which lies in the group $Hom_{\Omega_K}(R(G), E^*)$. Note that the diagonal embedding of E^* into $J(E)$ induces an inclusion

$$Hom_{\Omega_K}(R(G), E^*) \subset Hom_{\Omega_K}(R(G), J(E)).$$

In particular, therefore, by factoring out these subgroups $Det(U(\mathcal{O}_K[G]))$ and $Hom_{\Omega_K}(R(G), E^*)$, we have associated to each finitely generated, locally free $\mathcal{O}_K[G]$-module M a well-defined element in

$$\frac{Hom_{\Omega_K}(R(G), J(E))}{Hom_{\Omega_K}(R(G), E^*) \cdot Det(U(\mathcal{O}_K[G]))}.$$

We will note the class in this factor group corresponding to the element $Det((\lambda_P))$ by $Det[M]$.

The following connection between this Det-construction and the class-group is essential to what follows. This connection, which is called the 'Hom-description', is originally due to Fröhlich.

Theorem 2.2.1 *[12, p. 20]) The element $Det[M]$ as just defined depends only on the class of M in $\mathcal{CL}(\mathcal{O}_K[G])$ and defines an isomorphism*

$$Det : \mathcal{CL}(\mathcal{O}_K[G]) \xrightarrow{\cong} \frac{Hom_{\Omega_K}(R(G), J(E))}{Hom_{\Omega_K}(R(G), E^*) \cdot Det(U(\mathcal{O}_K[G]))}$$

which sends the class of a finitely generated, locally free module, M, to the class of $Det((\lambda_P))$ as constructed above.

2.2.3 The Kernel Group

Here we briefly discuss a subgroup of the class group, the so-called Kernel group, $D(\mathcal{O}_K[G])$. The importance of this group lies in the fact that it measures the relationship between the class group $\mathcal{CL}(\mathcal{O}_K[G])$ of Section 2.1 and a corresponding class group for the maximal order in $K[G]$. We shall see that there is a similar Hom-description of this group as well. Recall that an $\mathcal{O}_K$-**order** Λ in $K[G]$ is a subring of $K[G]$ containing $\mathcal{O}_K$, which is a finitely generated, projective $\mathcal{O}_K$-module, and satisfies $K \otimes_{\mathcal{O}_K} \Lambda = K[G]$.

Suppose then that Λ denotes a **maximal** $\mathcal{O}_K$-**order** of $K[G]$ (i.e. maximal with respect to inclusion). By a Grothendieck-type construction similar to that of Definition 2.1.1 we may define $\mathcal{CL}(\Lambda)$, the class group of Λ. Extension of scalars from $\mathcal{O}_K[G]$ to Λ then defines a surjection (cf. [8, II p. 230])

$$\mathcal{CL}(\mathcal{O}_K[G]) \longrightarrow \mathcal{CL}(\Lambda)$$

and we define the **kernel group**, $D(\mathcal{O}_K[G])$, to be the kernel of this map. This group, $D(\mathcal{O}_K[G])$, is independent of the choice of the maximal order Λ used in its definition.

To describe the Hom-description of this group we need to introduce a subgroup

$$Hom^{+}_{\Omega_K}(R(G), \mathcal{O}_E^*) \subset Hom_{\Omega_K}(R(G), \mathcal{O}_E^*).$$

This subgroup is defined in the following manner. Suppose that the representation ρ is **symplectic**, i.e. that as a complex representation ρ has the form

$$\rho : G \longrightarrow GL_n(\mathbf{H}) \xrightarrow{c} GL_n(\mathbf{C}),$$

with c the complexification map. Then complex conjugation fixes ρ in $R(G)$,

and so if K is a subfield of $\mathbf{R}$, we have that for any function

$$f \in Hom_{\Omega_K}(R(G), E^*),$$

$f(\rho)$ lies in $\mathbf{R}$ for every Archimedean prime of E which divides $K \subset \mathbf{R}$. It therefore is sensible to define the subgroup $Hom^+_{\Omega_K}(R(G), E^*)$ to be the group

$$\{f \in Hom_{\Omega_K}(R(G), E^*) \mid f(\rho) > 0,\ \rho \ symplectic\}$$

where by $f(\rho) > 0$ we mean that $f(\rho)$ is positive under every Archimedean place of E which lies over a real place of K.

The subgroup $Hom^+_{\Omega_K}(R(G), \mathcal{O}_E^*)$ is then defined by

$$Hom^+_{\Omega_K}(R(G), \mathcal{O}_E^*) = \{f \in Hom^+_{\Omega_K}(R(G), E^*) \mid im(f) \subset \mathcal{O}_E^*\}.$$

Finally, the Hom-description of the kernel group is now given by

Theorem 2.2.2 *cf. ([8, II,p.334-] or [12]) The isomorphism of Theorem 2.2.1 induces an isomorphism*

$$Det : D(\mathcal{O}_K[G]) \xrightarrow{\cong} \frac{Hom_{\Omega_K}(R(G), U(\mathcal{O}_E))}{Hom^+_{\Omega_K}(R(G), \mathcal{O}_E^*) \cdot Det(U(\mathcal{O}_K[G]))}.$$

2.3 Analytic Elements

In this section, we recall the construction of the Artin L-Function $L_K(s, \rho)$ and use it to define the global Artin Root Number $W_K(\rho)$. We then consider the local situation and describe the related notions of local root number and local Gauss sum, and show how this local information may be pieced together to obtain information globally.

2.3.1 Artin L-Functions and Artin Root Numbers

Throughout this subsection we let N/K be a Galois extension of number fields and let

$$\rho : G(N/K) \longrightarrow GL(V)$$

be a complex representation of the Galois group $G(N/K)$.

Recall that if $P \lhd \mathcal{O}_K$ is a finite prime of K and Q is a prime of N lying above P, then the corresponding **decomposition group** of P is defined to be

$$D_P = \{g \in G(N/K) \,|\, g(Q) = Q\} \cong G(N_Q/K_P)$$

and this is well-defined up to conjugation in $G(N/K)$. With Q still fixed, the group D_P operates in a natural way on the residue class field $\overline{N}_Q = \mathcal{O}_N/Q$, and leaves the subfield $\overline{K}_P = \mathcal{O}_K/P$ fixed. Hence to each automorphism $\sigma \in D_P$ we may associate an automorphism $\overline{\sigma}$ of $\overline{N}_Q$ over $\overline{K}_P$. This defines a surjective homomorphism

$$D_P \longrightarrow G(\overline{N}_Q/\overline{K}_P)\,.$$

The kernel of this homomorphism, I_P, is called the **inertia group** of P. In particular we have an isomorphism

$$D_P/I_P \cong G(\overline{N}_Q/\overline{K}_P)\,,$$

and this last group is finite cyclic, generated by the Frobenius automorphism, F_P. We may pull this generator back to an automorphism $F_P \in D_P$, which is well-defined up to multiplication by elements of I_P. Of course, the image of F_P under ρ depends on this choice as well. However, if we let $V_P = V^{I_P}$ be the subspace of V fixed by the inertia group I_P, then F_P does determine a well-defined automorphism $F_P \in GL(V_P)$. We denote this automorphism by $\rho(F_P|V_P)$ in what follows.

With P, Q and ρ as above, we may restrict ρ to yield a local representation of the decomposition group,

$$Res^{G(N/K)}_{G(N_Q/K_P)}(\rho) \,:\, G(N_Q/K_P) \longrightarrow GL(V)\,.$$

We write $G_i(N_Q/K_P)$ for the ramification groups at P, where $G_0(N_Q/K_P) = I_P$ is the inertia group defined above. Recall (cf. [29, IV,§1]) that $G_i(N_Q/K_P)$ is defined to be the subgroup of $G(N_Q/K_P)$ consisting of all elements s which satisfy, for all $x \in \mathcal{O}_{N_Q}$,

$$v_{N_Q}(s(x) - x) \geq i + 1\,,$$

where v_{N_Q} denotes the normalised discrete valuation on N_Q. Only finitely many of these groups are nontrivial, and so we may consider their actions on V and combine this information to yield an invariant of ρ. Specifically, we define the **Artin conductor** of the local representation above to be

$$n(\rho, P) = \sum_{i=0}^{\infty} [G_0(N_Q/K_P) : G_i(N_Q/K_P)]^{-1} \left(dim(V) - dim(V^{G_i(N_Q/K_P)}) \right)\,.$$

Note that, for P unramified, all of the ramification groups $G_i(N_Q/K_P)$ $(i \geq 0)$ are trivial, and so the corresponding Artin conductor is 0. Since only finitely many primes P ramify, we may combine the conductors globally as the prime exponents of an ideal. We define the **Artin conductor ideal**, $f(\rho)$ by the product formula:

$$f(\rho) = \prod_{P \text{ prime}} P^{n(\rho,P)} \lhd \mathcal{O}_K\,.$$

Note that by the above remarks this is really only a finite product.

Finally, we recall that the **absolute norm** of P, denoted $N(P)$, is defined by setting $N(P) = |\mathcal{O}_K/P|$.

The Artin L-function $L_K(s, \rho)$ is defined as the meromorphic continuation

of the Euler product

$$\prod_{P \text{ prime}} \left(det\left(1 - N(P)^{-s}\,\rho(F_P \mid V_P)\right)\right)^{-1}$$

for $Re(s) > 1$. Such a continuation is of course unique.

Unfortunately, as it sits the Artin L-function doesn't satisfy a functional equation, i.e., an equation relating, for $s \in \mathbf{C}$, the value of L at $1-s$ to the value at s. In order to obtain such a relationship, we need to multiply $L_K(s,\rho)$ by some additional factors to obtain the extended Artin L-function $\Lambda_K(s,\rho)$. For details regarding these factors, see [22] or [32].

Theorem 2.3.1 *The extended Artin L-function, $\Lambda_K(s,\rho)$, is a meromorphic function of the complex variable s satisfying the functional equation*

$$\Lambda_K(1-s,\rho) = W_K(\rho)\,\Lambda_K(s,\overline{\rho})\,. \tag{2.3.5}$$

Brauer gave the first proof of this result in 1947. A similar functional equation had been established for abelian L-functions in 1917 by Hecke. See [22] for details. The factor $W_K(\rho)$ occuring in this functional equation is a complex number of modulus 1, called the **Artin root number** of ρ.

We close this section by listing several properties of $W_K(\rho)$ which will be needed later. Let G be a group, H a subgroup of G, and let $\rho : H \to GL(V)$ be a complex representation. We denote by $Ind_H^G(\rho)$ the representation **induced** on G by ρ. If K is another group, and $\varphi : K \to H$ is surjective, we write $Inf_H^K(\rho)$ for the **inflation** of ρ to K. For more details regarding induction and inflation, see Chapter 1 of [8, I].

Proposition 2.3.2 *The Artin root number, $W_K(\rho)$, satisfies the following properties (cf. [32], p. 25):*

(a) If $\rho_i : G(N/K) \longrightarrow GL(V_i)$, $i = 1,2$, *are complex representations, then*

$$W_K(\rho_1 \oplus \rho_2) = W_K(\rho_1)\, W_K(\rho_2);$$

(b) If $K \subset N \subset M$ *is a chain of Galois extensions of number fields and* $G(M/K) \to G(N/K)$ *is the canonical surjection then*

$$W_K(Inf_{G(N/K)}^{G(M/K)}(\rho)) = W_K(\rho);$$

(c) If $K \subset F \subset N$ *is a chain of Galois extensions of number fields and* $\rho : G(N/F) \longrightarrow GL(W)$ *is a complex representation then*

$$W_K(Ind_{G(N/F)}^{G(N/K)}(\rho)) = W_F(\rho).$$

2.3.2 Local Root Numbers and Local Gauss Sums

Here, we introduce the related notions of local root number and local Gauss sum, and show how these local pieces of information may be combined to yield the value of the Artin root number of Section 2.3.1.

We begin by recalling the definition of the additive character of a local field. Let p be a prime number and let $K/\mathbf{Q}_p$ denote an extension of local fields. Recall first that there is an isomorphism of groups

$$\mathbf{Q}/\mathbf{Z} \cong \bigoplus_{\ell \text{ prime}} \mathbf{Q}_\ell/\mathbf{Z}_\ell.$$

Using this isomorphism, we may define an injective homomorphism

$$u : \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow \mathbf{C}^*,$$

as follows. For $x \in \mathbf{Q}_p/\mathbf{Z}_p$, select a rational number r which satisfies $x - r \in \mathbf{Z}_p$. The map u is then defined by sending x to $exp(2\pi i r) \in \mathbf{C}^*$.

The **additive character** of K, ψ_K, is now defined to be the composition

$$\psi_K : K \longrightarrow \mathbf{Q}_p \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{u} \mathbf{C}^* ,$$

where the first map is the usual Trace map $Tr_{K/\mathbf{Q}_p}$ and the middle map is the canonical surjection. Also, we define the **codifferent** of K, $\mathcal{D}_K^{-1}$, to be the largest fractional ideal of K contained in the kernel of ψ_K.

Now let L/K denote a Galois extension of local fields with Galois group $G(L/K)$ and let

$$\theta : G(L/K) \longrightarrow \mathbf{C}^*$$

be a one-dimensional representation (i.e. a homomorphism). Since θ takes its values in an abelian group, it factors through the abelianisation $G(L/K)^{ab}$ of $G(L/K)$. Using the reciprocity isomorphism of local class field theory,

$$G(L/K)^{ab} \xrightarrow{\cong} K^*/\left(N_{L/K}(L^*)\right) ,$$

we may identify θ with a continuous homomorphism

$$\theta : K^* \longrightarrow \mathbf{C}^*$$

which sends $N_{L/K}(L^*)$ to 1.

If $n(\theta)$ is the local Artin conductor of θ (defined as in Section 2.3.1), and $\mathcal{M}_K$ denotes the maximal ideal of $\mathcal{O}_K$, we write

$$f(\theta) = \mathcal{M}_K^{n(\theta)}$$

and call $f(\theta)$ the **local Artin Conductor ideal** of θ. Let $\mathcal{D}_K$ denote the different of K and let c be a generator of the ideal $f(\theta)\mathcal{D}_K$. We define $\tau(\theta)$, the **local Gauss sum** associated to θ, by

$$\tau(\theta) = \sum_{x \in U_K^0/U_K^{n(\theta)}} \theta(x/c)\,\psi_K(x/c) .$$

Here U_K^0 is just U_K, and by U_K^n we mean the subgroup of U_K consisting of level-n units,

$$U_K^n = 1 + \mathcal{M}^n ,$$

where $\mathcal{M}$ denotes the maximal ideal in $\mathcal{O}_K$. It can be shown that this sum does not depend on the choice of generator c.

As in Section 2.3.1, we let $N(f(\theta))$ denote the absolute norm of the ideal $f(\theta)$ and as usual we write $\overline{\theta}$ for the representation conjugate to θ.

Proposition 2.3.3 *([22, p.30]) The local Gauss sum satisfies*

(a) $\tau(\theta)\overline{\tau(\theta)} = N(f(\theta))$ *; and*

(b)$\tau(\theta)\,\tau(\overline{\theta}) = \theta(-1)\,N(f(\theta))$.

We define the **abelian local root number** of θ, $W_K(\theta)$, as follows. For $K = \mathbf{R}$ or $\mathbf{C}$, we set

$$W_K(\theta) = \left(\sqrt{-1}\right)^{n(\theta)} ,$$

while for non-Archimedean K we set

$$W_K(\theta) = \frac{\tau(\overline{\theta})}{\sqrt{N(f(\theta))}} .$$

Although initially defined on one-dimensional representations, we may extend the definition to the entire representation ring.

Theorem 2.3.4 *Let L/K be a Galois extension of local fields. Then the abelian local root number, as defined above, extends uniquely to a homomorphism*

$$W_K : R(G(L/K)) \longrightarrow \mathbf{C}^* ,$$

called the **local root number homomorphism**, *which satisfies the following properties:*

(i) For every $z \in R(G(L/K))$, $|W_K(z)| = 1$.

(ii) If $\rho_i : G(N/K) \longrightarrow GL(V_i)$ are complex representations, then

$$W_K(\rho_1 \oplus \rho_2) = W_K(\rho_1)\, W_K(\rho_2);$$

(iii) If $K \subset N \subset M$ is a chain of Galois extensions of local fields and $G(M/K) \to G(N/K)$ is the canonical surjection then

$$W_K(Inf_{G(N/K)}^{G(M/K)}(\rho)) = W_K(\rho);$$

(iv) If $K \subset F \subset N$ is a chain of Galois extensions of local fields and $\rho : G(N/F) \longrightarrow GL(W)$ is a complex representation then

$$W_K(Ind_{G(N/F)}^{G(N/K)}(\rho)) = W_F(\rho).$$

We close this section by noting the connection between local root numbers and Artin root numbers. This relationship will be an important ingredient in Chapter 4.

Theorem 2.3.5 *(cf. [32, p. 27]) Let N/E be a Galois extension of number fields and let*

$$\rho : G(N/E) \longrightarrow GL(V)$$

be a complex Galois representation. For each place v of E, we choose a place w of N lying above v, and let $G(N_w/E_v)$ be the corresponding decomposition group. Then

$$W_E(\rho) = \prod_v W_{E_v}\left(Res_{G(N_w/E_v)}^{G(N/E)}(\rho)\right)$$

where the product runs over all places v of E.

Remark: It was Langlands who first conceived the idea that the Artin root number could be canonically factored into a product of local root numbers as in Theorem 2.3.5. Langlands announced his proof of Theorem 2.3.4, but apparently never published it. Dwork had previously proved the existence of

the local root number homomorphism up to sign. A complete existence proof was furnished by Deligne. For details, see [33].

2.3.3 The Artin Root Number Class

As in the previous section, we let N/K be a finite Galois extension of number fields with Galois group G, and let

$$\rho : G \longrightarrow GL(V)$$

be a finite-dimensional, complex representation of G.

In this section, we introduce a class in $\mathcal{CL}(\mathbf{Z}[G])$ constructed from the Artin root number $W_K(\rho)$ of Section 2.3.1. This construction was originally given for tamely-ramified extensions by Ph. Cassou-Noguès [1] and A. Fröhlich. We will outline a more general construction due to Fröhlich and later reformulated by T. Chinburg (see [5, p. 18]).

Our approach is via Fröhlich's Hom-description of Section 2.2. Specifically, we must construct from the Artin root number an $\Omega_{\mathbf{Q}}$-invariant homomorphism that maps the representation ring of G into the idèles of E. Before starting the construction, we should note that it is only sensible to use the value $W_K(\rho)$ when it is 'reasonable', in the sense that this value may actually be used to define an idèle of E.

Given the representation ρ above, the functional equation of Theorem 2.3.5 for the extended Artin L-function $\Lambda_K(s,\rho)$ defines the Artin root number $W_K(\rho)$. If ρ is fixed by complex conjugation then for each place v of K and each place w of N dividing v, the restriction of ρ to $G(N_w/K_v)$ is also fixed by complex conjugation. But Proposition 2.3.3 and the definition of the local root number for one-dimensional representations, along with Theorem 2.3.5

imply that

$$W_K(\rho) \in \{\pm 1\}. \tag{2.3.6}$$

Hence it makes sense to restrict our attention to considering representations which are fixed under complex conjugation. More generally, we may consider the subgroup R^- of $R(G)$ consisting of all elements fixed by complex conjugation.

Recall that a representation ρ is said to be **orthogonal** if it factors through the orthogonal group, or, equivalently, if it is the complexification of a real representation. It turns out that the subgroup R^- above is generated by the orthogonal and the symplectic representations (cf. Section 2.2.3).

The above discussion implies, in particular, that every irreducible symplectic representation ρ satisfies (2.3.6). Furthermore, A. Fröhlich and J. Queyrut ([13]) have shown that $W_K(\rho) = 1$ for every orthogonal representation ρ.

Because we have a reasonable amount of control over the values of $W_K(\rho)$ for irreducible, symplectic representations, we would like to piece together the information about these values to obtain a class in $\mathcal{CL}(\mathbf{Z}[G])$.

We let E be a large Galois extension of number fields, in the sense of Section 2.2.1. Then the absolute Galois group $\Omega_{\mathbf{Q}}$ acts transitively on the infinite places of E. We fix an infinite place v_∞.

We define a homomorphism

$$W'_{N/K} : R(G) \longrightarrow J(E)$$

as follows. For each irreducible representation ρ we define $W'_{N/K}(\rho)$ place by

place via the formula

$$\left(W'_{N/K}(\rho)\right)_v = \begin{cases} 1 & \textit{if } v \textit{ finite}; \\ 1 & \textit{if } \rho \textit{ not symplectic}; \\ \alpha^{-1}W_K(\alpha(\rho)) & \textit{if } \rho \textit{ symplectic and} \\ & v = \alpha^{-1}(v_\infty) \textit{ with } \alpha \in \Omega_{\mathbf{Q}}. \end{cases}$$

By construction it is clear that this local information does in fact define an idèle $W'_{N/K}(\rho) \in J(E)$. Moreover the components are clearly invariant under the action of $\Omega_{\mathbf{Q}}$, and so by extending to all of $R(G)$ we may define a homomorphism

$$W'_{N/K} \in Hom_{\Omega_{\mathbf{Q}}}(R(G), J(E)).$$

The Hom-description of Section 2.2.1 therefore allows us to define a class, $W_{N/K}$, in the class group by

$$W_{N/K} = [W'_{N/K}] \in \mathcal{CL}(\mathbf{Z}[G(N/K)]).$$

Note that since $W_K(\rho) \in \{\pm 1\}$ for symplectic representations, the above construction implies immediately that $2\,W_{N/K} = 0$ in $\mathcal{CL}(\mathbf{Z}[G(N/K)])$. Also, in the above construction we were forced to make a choice of infinite place v_∞. However, it is shown in [32] (proof of Proposition 2.2.1) that the class obtained is actually independent of this choice. To summarize:

Proposition 2.3.6 *The class $W_{N/K}$ constructed above does not depend on the choice of v_∞ made in its construction, and moreover satisfies*

$$2\,W_{N/K} = 0 \in \mathcal{CL}(\mathbf{Z}[G(N/K)]).$$

2.4 Chinburg Invariants

Let N/K be a finite Galois extension of number fields and denote by G the corresponding Galois group. In this section we introduce three class group

elements which were introduced by T. Chinburg (cf. [3] and [4]) in order to compare the additive $\mathbf{Z}[G]$-structure of $\mathcal{O}_N$ with the multiplicative $\mathbf{Z}[G]$-structure of the group $U_{N,S}$ of S-units of N, where S denotes a sufficiently large finite G-stable set of places of N.

2.4.1 Chinburg's Invariants

We begin by outlining the definitions of the three invariants, $\Omega(N/K, i)$, $i = 1, 2, 3$. Our explanation follows that in [2].

We begin by fixing some notation. Let N/K and G be as above. For each place v of N we denote by G_v the corresponding decomposition group of v in G, and note that if v is an infinite place we have $|G_v| = 1$ or 2. We denote by $S_\infty(N)$ the set of all infinite places of N, and we let S be a finite G-stable set of places of N chosen large enough so that

(A) S contains $S_\infty(N)$, along with all places of N which ramify over K;

(B) The subset $S_f = S \setminus S_\infty(N)$ of finite places of N in S is nonempty; and

(C) The S-class number of each subfield of N containing K is equal to 1.

As usual, we denote by N_v the completion of N at the place v, and by N_v^* the corresponding multiplicative group. If v is a non-Archimedean place of N we write U_v for the multiplicative group of units in the valuation ring of N_v. We let U_S denote the multiplicative group of S-units of N, i.e.

$$U_S = \{ a \in N^* \mid |a|_v = 1 \textit{ for all places } v \notin S \}.$$

The S-idèles of N, J_S, are defined to be

$$J_S = \prod_{v \in S} N_v^* \times \prod_{v \notin S} U_v .$$

We also denote by C the idèle class group of N.

Throughout this section we wish to consider the basic exact sequence

$$1 \longrightarrow U_S \longrightarrow J_S \longrightarrow C \longrightarrow 1\,. \tag{2.4.7}$$

Using $\mathcal{O}_N$, J_S and U_S, we will construct an 'approximating' exact sequence of the form

$$1 \longrightarrow U_S \longrightarrow J_{S,f} \longrightarrow C_{S,f} \longrightarrow 1\,, \tag{2.4.8}$$

which has the property that the $\mathbf{Z}[G]$-modules $J_{S,f}$ and $C_{S,f}$ are finitely generated, and such that the sequence 2.4.8 has the same cohomology as the original, (2.4.7).

This approximating sequence (2.4.8) will then be used to define elements $\Omega(N/K,1)$, $\Omega(N/K,2)$ and $\Omega(N/K,3)$ of the locally free class group $\mathcal{CL}(\mathbf{Z}[G])$, which are associated to the $\mathbf{Z}[G]$-module structure of the modules $C_{S,f}$, $J_{S,f}$ and U_S, respectively.

Although the results of this thesis involve only the invariant $\Omega(N/K,2)$, the definitions of these invariants are sufficiently intertwined that we shall include all three.

We begin, therefore, with the construction of the approximating sequence (2.4.8).

Lemma 2.4.1 *(cf. [2, p. 111] or [4, p. 953]) Enlarging S if necessary, there exist an element $\alpha \in U_S \cap K$ and a free $\mathcal{O}_K[G]$-submodule F of $\mathcal{O}_N$ of rank one which satisfy the following properties:*

(i) α is a non-unit at each place in S_f; and

(ii) $\alpha^3\mathcal{O}_N \subset F \subset \alpha^2\mathcal{O}_N$.

Moreover, for such α and F there is a filtration of the closure $\overline{1+F}$ of $1+F$ by the modules, for $m \geq 0$,

$$T(m) = \overline{(1+\alpha^m F)}/\overline{(1+\alpha^{m+1}F)}$$

where each $T(m)$ is $\mathbf{Z}[G]$-isomorphic to $F/\alpha F$. □

Corollary 2.4.2 *(cf. [2, p. 111]) The module $\overline{1+F}$ of Lemma 2.4.1 is a cohomologically trivial $\mathbf{Z}[G]$-module of finite index in $\prod_{v\in S_f} U_v$.* □

Lemma 2.4.3 *(cf. [2, p. 112] or [4, p. 353]) For each infinite place $v \in S_\infty(N)$, there exists a finitely generated $\mathbf{Z}[G_v]$-submodule W_v of N_v^* such that*

(i) $U_S \subset W_v$;

(ii) W_v/U_S is $\mathbf{Z}$-torsion free ; and

(iii) the injection $U_S \to W_v$ induces an isomorphism in G_v-cohomology.

Furthermore, the modules W_v may be chosen in a consistent fashion, so that for each $g \in G$ and for each place $v \in S_\infty(N)$, we have $g(W_v) = W_{g(v)}$.
□

Armed with these two results, we may now use the given place-by-place approximations for places of S to construct modules which approximate the S-idèles J_S. Namely, we define

$$J'_S = \left((\prod_{v\in S_f} N_v^*)/\overline{1+F} \right) \times \prod_{v\in S_\infty} N_v^*$$

and

$$J_{S,f} = \left((\prod_{v\in S_f} N_v^*)/\overline{1+F} \right) \times \prod_{v\in S_\infty} W_v .$$

Note that by sending $U_v \to 1$ for each $v \notin S$ and sending

$$\prod_{v\in S_f} N_v^* \longrightarrow \left((\prod_{v\in S_f} N_v^*)/\overline{1+F} \right)$$

under the canonical surjection, we may define a surjection

$$J_S \longrightarrow J'_S .$$

Similarly, there is an obvious injection induced from property (*iii*) of Lemma 2.4.3,

$$J_{S,f} \longrightarrow J'_S .$$

Also, using Corollary 2.4.2 and property (*iii*) of Lemma 2.4.1, we see that $J_{S,f}$ is a finitely generated $\mathbf{Z}[G]$-module which has the same cohomology as J_S. To see this last fact, note that by our underlying assumptions about S, for $v \notin S$ the place v is unramified, and hence ([29]) the $\mathbf{Z}[G_v]$-module U_v is cohomologically trivial.

Now consider the diagonal embedding

$$U_S \longrightarrow J_S .$$

By property (*i*) of Lemma 2.4.3, at each infinite place $v \in S_\infty$ we have a corresponding embedding $U_S \to W_v$. Also (cf. [2]) we have embeddings

$$U_S \longrightarrow \left((\prod_{v \in S_f} N_v^*)/\overline{1+F} \right) .$$

These embeddings may be combined to yield induced embeddings

$$U_S \longrightarrow J'_S$$

and

$$U_S \longrightarrow J_{S,f} .$$

We define C'_S and $C_{S,f}$ to be the respective cokernels. Then we have a commutative diagram of horizontal short exact sequences of the following form.

$$\begin{tikzcd}
0 \arrow[r] & U_S \arrow[r] \arrow[d] & J_S \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & U_S \arrow[r] & J'_S \arrow[r] & C'_S \arrow[r] & 0 \\
0 \arrow[r] & U_S \arrow[r] \arrow[u] & J_{S,f} \arrow[r] \arrow[u] & C_{S,f} \arrow[r] \arrow[u] & 0
\end{tikzcd} \tag{2.4.9}$$

Here all the vertical maps are natural projections and injections as above, and each induces isomorphisms in cohomology with respect to all subgroups of G.

In particular then, the bottom row in diagram (2.4.9) is a short exact sequence of $\mathbf{Z}[G]$-modules, each of which is finitely generated, and this sequence has the property that its cohomology is the same as that of the top sequence, which was our original basic sequence. This bottom row is the 'approximating' sequence we promised to construct.

We now continue with the actual construction of the Chinburg invariants, using the approximating sequence just constructed.

Let Y_S denote the additive group $Div_{\mathbf{Z}}(S)$, the group of $\mathbf{Z}$-divisors supported on the set S, and write X_S for $Div^0_{\mathbf{Z}}(S)$, the subgroup of Y_S consisting of those divisors having degree 0. Recall that by definition (cf. [4, p. 352]) Y_S is therefore the free abelian group on the set S and X_S is defined via the exact sequence

$$0 \longrightarrow X_S \longrightarrow Y_S \xrightarrow{\epsilon} \mathbf{Z} \longrightarrow 0\,, \tag{2.4.10}$$

where $\epsilon : Y_S \to \mathbf{Z}$ is defined at each $v \in S$ by $\epsilon(v) = 1$. In particular, each element $y \in Y_S$ is of the form $y = \sum_{v \in S} n_v v$ with $n_v \in \mathbf{Z}$ and $\epsilon(y) = \sum n_v$, so that $y \in X_S$ if and only if $\sum n_v = 0$.

The sequence (2.4.10) and the approximating sequence (2.4.8) may now be compared by using an exact commutative diagram of $\mathbf{Z}[G]$-modules of the following form.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & U_S \arrow[r] \arrow[d] & A_3 \arrow[r] \arrow[d] & B_3 \arrow[r] \arrow[d] & X_S \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & J_{S,f} \arrow[r] \arrow[d] & A_2 \arrow[r] \arrow[d] & B_2 \arrow[r] \arrow[d] & Y_S \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C_{S,f} \arrow[r] \arrow[d] & A_1 \arrow[r] \arrow[d] & B_1 \arrow[r] \arrow[d] & \mathbf{Z} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 & 0 &
\end{tikzcd} \tag{2.4.11}$$

Proposition 2.4.4 *(cf. [2]) The above diagram may be constructed in such a way that*

(i) The $\mathbf{Z}[G]$*-modules* A_i *and* B_i *are finitely generated and of finite projective dimension;*

(ii) The extension class

$$\alpha_{1,f} \in Ext^2_{\mathbf{Z}[G]}(\mathbf{Z}, C_{S,f}) = H^2(G; C_{S,f})$$

of the bottom sequence is the pull-back via diagram (2.4.9) of the canonical class in $H^2(G, C)$*;*

(iii) The extension class

$$\alpha_{2,f} \in Ext^2_{\mathbf{Z}[G]}(Y_S, J_{S,f})$$

of the middle row is the pull-back via diagram (2.4.9) of the class

$$\alpha_2 = \oplus_{v \in S_0} i_v^*(\alpha_v) \in \oplus_{v \in S_0} H^2(G_v, Y_S) = Ext^2_{\mathbf{Z}[G]}(Y_S, J_S)\,.$$

Here by S_0 we mean a set of representatives for the G-orbits of S, i_v^* is the map in cohomology induced by the injection

$$N_v \longrightarrow J_S\,,$$

and α_v denotes the canonical class in $H^2(G_v; N_v^*)$.

We may now define the invariants $\Omega(N/K, i)$. First notice that if X is a finitely generated $\mathbf{Z}[G]$-module of finite projective dimension, then there exist finitely generated, locally free $\mathbf{Z}[G]$-modules X_1 and X_2 such that the sequence

$$0 \longrightarrow X_1 \longrightarrow X_2 \longrightarrow X \longrightarrow 0 \tag{2.4.12}$$

is exact. One may then define a class $[X]$ in $\mathcal{CL}(\mathbf{Z}[G])$ by setting

$$[X] = [X_2] - [X_1]\,.$$

If

$$0 \longrightarrow X_1' \longrightarrow X_2' \longrightarrow X \longrightarrow 0$$

is another such short exact sequence, then Schanuel's Lemma ([25, Lemma 8.1]) implies that $X_1' \oplus X_2 \cong X_1 \oplus X_2'$, so that in $\mathcal{CL}(\mathbf{Z}[G])$,

$$[X_2] - [X_1] = [X_2'] - [X_1']\,.$$

Therefore the class $[X]$ constructed above is well-defined, i.e., is independent of the choices of X_1 and X_2 in the sequence (2.4.12).

Definition 2.4.5 *For any finite Galois extension N/K of number fields, we define the* **Chinburg invariants**, $\Omega(N/K, i)$, *by setting*

$$\Omega(N/K, i) = [A_i] - [B_i] \in \mathcal{CL}(\mathbf{Z}[G(N/K)])\,, \tag{2.4.13}$$

for $i = 1, 2, 3$.

Theorem 2.4.6 *([4]) The classes $\Omega(N/K,i)$ of Definition 2.4.5 depend only on the extension N/K, i.e. are independent of any of the choices made in their construction.* □

Finally, we note that in the diagram used in the construction of the invariants (2.4.11), the vertical sequences are short exact, and so applying this fact to the definition (2.4.13), we immediately deduce the following result.

Theorem 2.4.7 *([4]) For any finite Galois extension N/K of number fields,*

$$\Omega(N/K,2) = \Omega(N/K,1) + \Omega(N/K,3) \in C\mathcal{L}(\mathbf{Z}[G(N/K)]) . \square$$

2.4.2 Local Chinburg Invariants

Let L/K be a finite Galois extension of p-adic local fields with Galois group $G(L/K)$. In this section, we discuss the construction of a Chinburg-type invariant defined in this local situation. These local invariants will play a crucial role in the next section, where they will be used to give an alternative construction of the second Chinburg invariant, $\Omega(N/K,2)$, of Section 2.4.1.

We first recall that the Fundamental Theorem of local class field theory (cf. [32, Theorem 1.2.2]) gives a canonical isomorphism of the form

$$inv : H^2(G(L/K)\,;\,L^*) \xrightarrow{\cong} \mathbf{Z}/[L:K] .$$

(Throughout this section we view the group $\mathbf{Z}/[L:K]$ as the multiplicative group generated by $[L:K]^{-1}$.)

Recalling (cf. [26] or [16]) that the group $H^2(G(L/K);L^*)$ classifies 2-extensions, i.e. extensions of $\mathbf{Z}[G(L/K)]$-modules of the form

$$1 \longrightarrow L^* \longrightarrow A \longrightarrow B \longrightarrow \mathbf{Z} \longrightarrow 1 , \qquad (2.4.14)$$

we suppose that we have an extension of this form whose class

$$\alpha \in H^2(G(L/K); L^*)$$

corresponds to the generator $inv^{-1}([L:K]^{-1})$. Since $[L:K]^{-1}$ is a unit in $\mathbf{Z}/[L:K]$ the representative 2-extension 2.4.14 for the class α may be chosen so that the modules A and B are cohomologically trivial. In addition, the module B may be chosen to be finitely-generated and torsion free (and hence projective).

Suppose now that $U \subset L^*$ is a $\mathbf{Z}[G(L/K)]$-submodule which is cohomologically trivial. Then we may 'factor' out U as follows. Since U is cohomologically trivial, the short exact sequence

$$1 \longrightarrow U \longrightarrow L^* \longrightarrow L^*/U \longrightarrow 1$$

induces isomorphisms in Tate cohomology,

$$\hat{H}^n(G(L/K); L^*) \xrightarrow{\cong} \hat{H}^n(G(L/K); L^*/U)$$

and, in particular, an isomorphism

$$H^2(G(L/K); L^*) \xrightarrow{\cong} H^2(G(L/K); L^*/U).$$

This implies that the 2-extension

$$1 \longrightarrow L^*/U \longrightarrow A/U \longrightarrow B \longrightarrow \mathbf{Z} \longrightarrow 1$$

corresponds to the class

$$inv^{-1}([L:K]^{-1}) \in H^2(G(L/K); L^*/U) \cong \mathbf{Z}/[L:K].$$

In addition, if the module L^*/U is finitely generated, then we may also assume that A/U is finitely generated.

Recall from Section 2.4.1 that each finitely generated, cohomologically trivial $\mathbf{Z}[G(L/K)]$-module X gives rise to a well-defined class

$$[X] \in \mathcal{CL}(\mathbf{Z}[G(L/K)]),$$

so that in this way we obtain well-defined classes $[A/U]$ and $[B]$. The **local Chinburg invariant** $\Omega(L/K, U)$ is then defined to be

$$\Omega(L/K, U) = [A/U] - [B] \in \mathcal{CL}(\mathbf{Z}[G(L/K)]). \tag{2.4.15}$$

Proposition 2.4.8 *(cf. [32, p. 47]) The local Chinburg invariant $\Omega(L/K, U)$ does not depend on the choices of the $\mathbf{Z}[G(L/K)]$-modules A and B involved in its construction.*

2.4.3 Kim's Formula

We now introduce an alternative formula for computing the second Chinburg invariant introduced in Definition 2.4.5. Throughout this section N/K will denote a finite Galois extension of number fields with Galois group $G(N/K)$.

For each prime ideal P of $\mathcal{O}_K$, we fix a prime Q of $\mathcal{O}_N$ lying above P and write $G(N_Q/K_P)$ for the corresponding decomposition group. Recall that the prime P is said to be **tame** if each of the local extensions N_Q/K_P is at most tamely ramified. Otherwise we say that P is **wild**.

When P is tame, Noether's Theorem states that $\mathcal{O}_{N_Q}$ is a free module (of rank one) over the ring $\mathcal{O}_{K_P}[G(N_Q/K_P)]$ (cf. [12]). Of course for every P the Normal Basis Theorem says that N_Q, when viewed as a $K_P[G(N_Q/K_P)]$-module, is free of rank one. In addition, the corresponding free generator of N_Q may be chosen so as to lie in $\mathcal{O}_{N_Q}$. This allows us to construct an adèle $a = (a_P) \in \prod_P \mathcal{O}_{N_Q}$ by selecting for each P an element $a_P \in \mathcal{O}_{N_Q}$ such that

(a) $N_Q = K_P[G(N_Q/K_P)]\, a_P$ for every P; and

(b) $\mathcal{O}_{N_Q} = \mathcal{O}_{K_P}[G(N_Q/K_P)]\, a_P$ for every tame P.

Continuing to allow Q to denote our fixed prime above P, for each P we also have isomorphisms of the form

$$N \otimes_K K_P \cong \prod_{Q'|P} N_{Q'} \cong Ind_{G(N_Q/K_P)}^{G(N/K)}(N_Q)$$

and

$$\mathcal{O}_N \otimes_K \mathcal{O}_{K_P} \cong \prod_{Q'|P} \mathcal{O}_{N_{Q'}} \cong Ind_{G(N_Q/K_P)}^{G(N/K)}(\mathcal{O}_{N_Q}).$$

For each P, this permits us to rewrite

$$K_P[G(N/K)]\, a_P \cong \prod_{Q'|P} N_{Q'},$$

while for each tame P we may write

$$\mathcal{O}_{K_P}[G(N/K)]\, a_P \cong \prod_{Q'|P} \mathcal{O}_{N_{Q'}}.$$

In order to simplify notation, we write X_Q for $\mathcal{O}_{K_P}[G(N_Q/K_P)]\, a_P$, so that for tame P, condition (b) above implies that $X_Q = \mathcal{O}_{N_Q}$. Of course this need not be the case if P is wild, where we only know that $X_Q \subset N_Q$. In addition, we define $X = \mathcal{O}_K[G(N/K)]\, a$. By this we mean that X is the intersection of N with the product $\prod_P X_P$ of all of the P-completions of X. Here both N and $\prod_P X_P$ are viewed as subgroups of the adèles, so that such an intersection makes sense.

This construction implies in particular that X is a locally free module over $\mathcal{O}_K[G(N/K)]$, whose completion at P is given by

$$X_P = \mathcal{O}_{K_P}[G(N/K)]\, a_P = Ind_{G(N_Q/K_P)}^{G(N/K)}(X_Q).$$

By replacing X by a suitable integer multiple mX if necessary, we may also assume that for every wildly ramified extension N_Q/K_P, the Q-adic exponential

map gives an isomorphism

$$exp_Q : X_Q \xrightarrow{\cong} 1 + X_Q \subset \mathcal{O}^*_{N_Q}. \tag{2.4.16}$$

Because X is locally free as an $\mathcal{O}_K[G(N/K)]$-module, it is cohomologically trivial. In particular, as in Section 2.4.1 X defines a class in $\mathcal{CL}(\mathbf{Z}[G(N/K)])$. Moreover, for each P the module X_Q is also cohomologically trivial, and so for wild P the isomorphism (2.4.16) implies that $1 + X_Q$ is cohomologically trivial as well. Hence, for wild P it is sensible to consider the local Chinburg invariant $\Omega(N_Q/K_P, 1 + X_Q)$ as defined by (2.4.15).

The following formula is due to S. Kim, who made explicit use of several results of Chinburg [4] in order to derive it.

Proposition 2.4.9 *([19]) Let N/K be a finite Galois extension of number fields with Galois group $G(N/K)$. Then, in $\mathcal{CL}(\mathbf{Z}[G(N/K)])$,*

$$\Omega(N/K, 2) = [X] + \sum_{P \text{ wild}} Ind_{G(N_Q/K_P)}^{G(N/K)}(\Omega(N_Q/K_P, 1 + X_Q)).$$

We note that as a consequence of this Proposition, the computation of $\Omega(N/K, 2)$ is independent of the choice of locally free $\mathcal{O}_K[G(N/K)]$-module X, provided only that X satisfy conditions (a) and (b) above.

2.4.4 Chinburg's Conjectures

In the early 1980's T. Chinburg introduced the three classes, $\Omega(N/K, i) \in \mathcal{CL}(\mathbf{Z}[G])$ $(i = 1, 2, 3)$ which were constructed in Section 2.4.1 and went on to show that, in the case of a tame extension N/K of number fields, there is an equality

$$\Omega(N/K, 2) = [\mathcal{O}_N] \in \mathcal{CL}(\mathbf{Z}[G]).$$

Previously, M. Taylor had proven the following result.

Theorem 2.4.10 *([35]) Let N/K be a tame Galois extension of number fields with $G = Gal(N/K)$. Then*

$$[\mathcal{O}_N] = W_{N/K} \in \mathcal{CL}(\mathbb{Z}[G]). \qquad \square$$

This result had originally been conjectured by Fröhlich.

Since $\Omega(N/K, 2)$ is defined for general extensions, without the tameness hypothesis, Chinburg had the idea that perhaps we should regard $\Omega(N/K, 2)$ as a generalisation of $[\mathcal{O}_N]$ to wildly ramified extensions. This quite naturally led Chinburg to formulate the following conjectures:

Conjecture 2.4.11 *(Chinburg [4]) Let N/K be a finite Galois extension of number fields. Then in $\mathcal{CL}(\mathbb{Z}[G])$,*

$$(1) \quad \Omega(N/K, 1) = 0;$$

$$(2) \quad \Omega(N/K, 2) = W_{N/K};$$

$$(3) \quad \Omega(N/K, 3) = W_{N/K}.$$

These three conjectures have come to commonly be known, respectively, as the first, second and third **Chinburg conjectures**. However, because the second conjecture extends Taylor's Theorem (2.4.10), and thus the conjecture of Fröhlich, it is sometimes referred to as the Fröhlich-Chinburg conjecture.

Since the three Chinburg invariants are related (cf. Theorem 2.4.7), any two of the conjectured relations (1)–(3) implies the remaining one. Much of the work on these conjectures has therefore been concentrated on verifying the second and third conjectures.

Because the focus of this thesis is on verifying some cases of the second of these conjectures only, henceforth we will restrict our attention to this conjecture. For an explanation of known results for the third Chinburg conjecture,

the reader should consult [2, §4.2] and [15]. The first of these also outlines some of what has been verified in the function field case.

Regarding the second Chinburg conjecture, some further work has been done in the direction of wild extensions $N/\mathbf{Q}$, although in these cases computational difficulties arise. Chinburg [5] has verified several families of examples, and S. Kim [19], [20] has proved that this conjecture holds for all quaternion fields $N/\mathbf{Q}$ for which the prime 2 is not totally ramified. In addition, in his doctoral thesis ([37]), M. Tran has established the conjecture for an infinite family of quaternion fields where the prime 2 is totally ramified. The remaining quaternion extensions will be considered in the next chapter.

The strongest general result is that of D. Holland [17] who used the idea of canonical factorisation to establish that

$$\Omega(N/K,2) - W_{N/K} \in D(\mathcal{O}_K[G]).$$

Since there exist some wildly ramified extensions N/K for which the class $W_{N/K}$ lies outside the kernel group, this result provides the best evidence that the second Chinburg conjecture should hold for all extensions of number fields. Note that Holland's result establishes a weaker version of Conjecture (2), in that we have an equality

$$\Omega(N/K,2) = W_{N/K} \in \mathcal{CL}(\mathbf{Z}[G])/D(\mathcal{O}_K[G]).$$

More recently, C. Greither ([14]) has established the original version of the second conjecture for all absolutely abelian fields having odd conductor.

2.5 Quaternion Extensions

We now seek to establish the underlying setting for our results in Chapters 3 and 4. In this section, we introduce Hilbert symbols and use them to classify

the extensions of interest, namely those quaternion extensions of $\mathbf{Q}$ for which the prime 2 is totally ramified. With this notation, we can state our main theorem and discuss the approach that the proof will take in the following two chapters.

Throughout this section, we will write Q_8 for the quaternion group of order 8, which we write in terms of generators and relations as

$$Q_8 = \left\{ x, y \mid x^4 = 1,\, x^2 = y^2,\, yxy^{-1} = x^{-1} \right\}. \tag{2.5.17}$$

We now let $N/\mathbf{Q}$ be a quaternion field. Then N is a Galois extension of $\mathbf{Q}$ with Galois group isomorphic to Q_8. We will usually identify $Gal(N/\mathbf{Q})$ with the group Q_8 as in equation (2.5.17). We note in particular that we therefore write x^2 for the unique element of order 2 in $Gal(N/\mathbf{Q})$.

Every quaternion field contains a unique biquadratic subfield

$$E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2}).$$

with d_1 and d_2 nonsquare. E is the field fixed under the automorphism x^2. We shall see that the behaviour of primes in N can be expressed in terms of conditions on the possible values of the d_i.

2.5.1 Hilbert Symbols

The purpose of this section is to introduce the Hilbert symbol and discuss its main properties. Additional details and omitted proofs may be found in [28, Ch.III] or [24, III,§5].

We begin with some definitions. Throughout this section we shall use the notation k to refer either to the field $\mathbf{R}$ of real numbers or to the field $\mathbf{Q}_p$ of p-adic numbers. We let V be the set consisting of all rational prime numbers p, along with the additional symbol ∞.

Definition 2.5.1 *Let $v \in V$. We take $k = \mathbf{Q}_p$ if $v = p$, and $k = \mathbf{R}$ if $v = \infty$. The* **Hilbert symbol** *at v is the map*

$$(\cdot,\cdot)_v : k^* \times k^* \longrightarrow \{\pm 1\}$$

defined by setting, for $a, b \in k^*$, $(a,b)_v = 1$ when the equation $z^2 = ax^2 + by^2$ has a nontrivial solution $(0,0,0) \neq (z,x,y) \in k^3$, and $(a,b)_v = -1$ otherwise.

It is clear from the definition that the value $(a,b)_v$ does not change when either a or b are multiplied by squares, so that we may actually view $(\cdot,\cdot)$ as a map

$$(\cdot,\cdot)_v : k^*/(k^*)^2 \times k^*/(k^*)^2 \longrightarrow \{\pm 1\}.$$

Proposition 2.5.2 *(cf. [28, p.19]) Let v and k be as in Definition 2.5.1 and let $a, b \in k^*$. We write N_b for the subgroup of k^* consisting of norms of elements of $k(\sqrt{b})^*$. Then $(a,b)_v = 1$ if and only if $a \in N_b$.*

By local class field theory,

$$k^*/N_b \cong Gal(k(\sqrt{b})/k)^{ab} \cong \{\pm 1\},$$

so that this result should not seem surprising.

Theorem 2.5.3 *([28, p.19-20]) The Hilbert symbol is a nondegenerate, symmetric bilinear form on the $\mathbf{F}_2$-vector space $k^*/(k^*)^2$, satisfying the following relations, where for simplicity we suppress subscripts:*

(i) $(a, c^2) = 1$;

(ii) $(a, -a) = 1$ *and* $(a, 1-a) = 1$;

(iii) if $(a,b) = 1$, *then* $(aa', b) = (a', b)$; *and*

(iv) $(a,b) = (a, -ab) = (a, (1-a)b)$.

Globally, these symbols tie together to give the following product formula of Hilbert:

Theorem 2.5.4 *([28, p.23]) Let $a, b \in \mathbf{Q}^*$. Then for all but finitely many v we have $(a,b)_v = 1$ and*

$$\prod_{v \in V} (a,b)_v = 1 .$$

We are going to use the Hilbert symbol to classify quaternion fields. In order to do this, we need an easier way to evaluate these symbols explicitly, especially at the prime 2.

Proposition 2.5.5 *([24, p.54]) Let $v = 2$, so that $k = \mathbf{Q}_2$, and suppose that $a, b \in U_{\mathbf{Q}_2}{}^*$. Then*

$$(a,2)_2 = (-1)^{(a^2-1)/8} = \begin{cases} 1 & if\ a \equiv \pm 1\ mod\ 8 \\ -1 & if\ a \equiv \pm 3\ mod\ 8 \end{cases} ;\ and$$

$$(a,b)_2 = (-1)^{((a-1)/2)((b-1)/2)} = 1 \quad unless\ a \equiv b \equiv 3\ mod\ 4 .$$

As a particular case of this proposition, we see that for a odd,

$$(a,-1)_2 = \begin{cases} 1 & if\ a \equiv 1\ mod\ 4 \\ -1 & if\ a \equiv -1\ mod\ 4 \end{cases} . \tag{2.5.18}$$

2.5.2 Classifying Quaternion Fields

We are now going to use the Hilbert symbol of the previous section in order to classify those quaternion fields for which the prime 2 is totally ramified. For our purposes, the most important result is the following.

Recall that if N is a quaternion field, then N contains a unique biquadratic subfield $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$, namely the field fixed under the element $x^2 \in Q_8$.

Proposition 2.5.6 *([23, p.529];[12, p.49]) Let E be the biquadratic field $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$. Then $E \subset N$ for some extension N with $Gal(N/\mathbf{Q}) \cong Q_8$ if and only if*

$$(d_1, d_2)_p\, (-1, d_1)_p\, (-1, d_2)_p = 1$$

for every prime p.

This result is extremely useful in narrowing the possible quaternion fields, by restricting the possibilities for the biquadratic subfield E. To illustrate, we use this result to determine the possible biquadratic fields E which can be embedded in quaternion fields which are totally ramified at the prime 2. First note that the biquadratic field E contains precisely three quadratic subfields, namely the subfields $\mathbf{Q}(\sqrt{d_1})$, $\mathbf{Q}(\sqrt{d_2})$, and $\mathbf{Q}(\sqrt{d_3}) = \mathbf{Q}(\sqrt{d_1 d_2})$. These are exactly the fields fixed by the automorphisms of order four: x, y, and xy.

Proposition 2.5.7 *Suppose that N is a quaternion field and that the prime 2 is totally ramified in N. If $E = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ is the unique biquadratic subfield, then either*

$$d_1 \equiv 10 \pmod{16} \qquad \textit{and} \qquad d_2 \equiv 3 \pmod{8}$$

or

$$d_1 \equiv 2 \pmod{16} \qquad \textit{and} \qquad d_2 \equiv 3 \pmod{8}.$$

Proof: Let d_1, d_2 and d_3 be as in the discussion above, and assume without loss of generality that these are squarefree.

We start with a few comments regarding the localisation $L/\mathbf{Q}_2$ at 2. Since by hypothesis this extension is totally ramified, the decomposition group D_2 is all of Q_8, and hence

$$Gal(L/\mathbf{Q}_2) \cong D_2 = Gal(N/\mathbf{Q}) \cong Q_8\,,$$

so that L is therefore a quaternion extension of $\mathbf{Q}_2$. In particular, each of the quadratic completions $\mathbf{Q}_2(\sqrt{d_i})$ must remain distinct from one another, as well as distinct from $\mathbf{Q}_2$.

In addition, note that squares in $\mathbf{Z}$ have the form $4^n u$ with $u \equiv 1 \bmod 8$. Hence for d_i odd, we may only determine d_i modulo 8, while even d_i can be

determined modulo 16. This is due to the fact that not every integer which is congruent to 1 modulo 8 need be a square (for example, 17). Upon completing at 2, however, this problem disappears. In fact (cf. [28]), every element $u \in \mathbf{Z}_2^*$ which satisfies $u \equiv 1 \bmod 8$ is actually a square. We will use this fact to eliminate possibilities over N. More precisely, we will show in a moment that exactly two of the d_i are even. The above comments imply that these two even d_i's cannot be congruent mod 16, since these would collapse to the same quadratic extension upon completing at 2.

We now consider the possible d_i which may occur. By the above remarks, we cannot have any of the d_i congruent to 1 mod 8, since in that case $\mathbf{Q}_2(\sqrt{d_i}) = \mathbf{Q}_2$. Also, $d_i \not\equiv 5 \bmod 8$, since for such an extension the prime 2 decomposes. Of course, since the d_i are assumed squarefree, we may not have $d_i \equiv 0, 4 \bmod 8$. Therefore, modulo 8 we have only the possible values 2, 3, 6, or 7 for the d_i.

It is clear that we cannot have all three of the d_i even. We also notice that no two of the d_i can be odd. To see this, we suppose for sake of argument that d_1 and d_2 are odd. Then, since $d_1 \equiv d_2 \equiv 3 \bmod 4$, Proposition 2.5.5 and equation (2.5.18) imply that we have

$$(d_1, d_2)_2\,(-1, d_1)_2\,(-1, d_2)_2 = -1\,,$$

which contradicts Proposition 2.5.6.

Therefore one of the d_i, say d_2, is $\equiv 3 \bmod 4$, while the others, d_1 and d_3 are even. We write $d_1 = 2u_1$ and $d_3 = 2u_3$ with u_1 and u_3 odd.

Next we notice that we in fact have $d_2 \equiv 3 \bmod 8$. This follows from the following computation. We note that by Propositions 2.5.5 and 2.5.6,

$$\begin{aligned} 1 &= (d_1, d_2)_2\,(-1, d_1)_2\,(-1, d_2)_2 \\ &= (2, d_2)_2\,(u_1, d_2)_2\,(-1, 2)_2\,(-1, u_1)_2\,(-1, d_2)_2\,. \end{aligned}$$

We compute that $(-1, d_2)_2 = -1$, $(-1, 2)_2 = 1$, and moreover that

$$(u_1, d_2)_2 (-1, u_1)_2 = 1 ,$$

so that we are reduced to the condition that $(2, d_2)_2 = -1$. But this can only happen when $d_2 \equiv 3$ modulo 8.

Now we restrict the possibilities for u_1 and u_3. We claim that it cannot be the case that $u_1 \equiv u_3$ mod 4. Indeed, if this relation holds, then $u_1 u_3 \equiv 1$ mod 4 as well. But there exists an odd integer c with the property that $c^2 d_2 = u_1 u_3$. Looking at this equation mod 8, we see that $c^2 \equiv 1$ and so

$$d_2 \equiv u_1 u_3 \quad (mod\ 8) .$$

This contradicts the fact that $d_2 \equiv 3$ mod 8.

Therefore we may assume that $d_1 \equiv 2$ mod 8 and $d_3 \equiv 6$ mod 8. Thus we are reduced to the possibilities in the statement of the proposition. □

2.5.3 The Main Theorem

We now discuss the classification in the previous section and its relation to the results of this thesis.

We first recall the result of Kim

Theorem 2.5.8 *(Kim [20]) Let N be a quaternion field in which the prime 2 is not totally ramified. Then*

$$\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}} \in \mathcal{CL}(\mathbf{Z}[Q_8]) .$$

Recall, from the classification of totally ramified quaternion extensions in Proposition 2.5.7, that quaternion fields where the prime 2 is totally ramified can be divided into two infinite families. In his doctoral thesis, Tran proved the following:

Theorem 2.5.9 *(Tran [37]) Let N be a quaternion field which contains a biquadratic subfield $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ with $d_1 \equiv 10 \bmod 16$ and $d_2 \equiv 3 \bmod 8$, so that the prime 2 is totally ramified. Then*

$$\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}} \in \mathcal{CL}(\mathbf{Z}[Q_8]).$$

Tran's theorem leaves only one family of quaternion fields for which the second Chinburg conjecture remains to be verified, and this verification is the object of this thesis. The remaining chapters of this thesis are devoted to the proof of the following theorem.

Theorem 2.5.10 *Let N be a quaternion field which contains a biquadratic subfield $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ with $d_1 \equiv 2 \bmod 16$ and $d_2 \equiv 3 \bmod 8$, so that the prime 2 is totally ramified. Then*

$$\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}} \in \mathcal{CL}(\mathbf{Z}[Q_8]).$$

Finally, we note that this result, along with the theorems of Kim and Tran give the following complete result.

Theorem 2.5.11 *Let N be a quaternion field. Then*

$$\Omega(N/\mathbf{Q}, 2) = W_{N/\mathbf{Q}} \in \mathcal{CL}(\mathbf{Z}[Q_8]).$$

Chapter 3

The Local Situation

In this chapter, we begin our progress toward the proof of Theorem 2.5.10, which will be given in Chapter 4. Before we get to the proof itself, however, we need to first explore some facts regarding the situation when we localize at the prime 2.

Locally, by the results of Section 2.5.2, we see that the completion of N at 2 is quaternion over $\mathbf{Q}_2$. In Section 3.1 we first examine this completion and show that for the quaternion fields of interest, there are precisely two nonisomorphic local quaternion extensions which occur. We give explicit constructions for both fields.

We then digress slightly in order to discuss the fundamental 2-extension and use this extension to construct an explicit 2-cocycle for the canonical generator of $H^2(Q_8, L^*)$.

Finally, we show that with suitable choices, this cocycle is actually injective. This simplifies the considerations of Chapter 4.

Throughout the remainder of this thesis, we will let $N/\mathbf{Q}$ be a quaternion extension of the type outlined in the statement of Theorem 2.5.10. As noted

in (2.5.17), we will write Q_8 explicitly in terms of generators and relations as

$$Q_8 = \left\{ x, y \mid x^4 = 1,\, x^2 = y^2,\, yxy^{-1} = x^{-1} \right\}.$$

3.1 The Two Local Extensions

If we localize the biquadratic subfield $\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ at the prime 2 we obtain the biquadratic extension $E = \mathbf{Q}_2(\sqrt{2}, \sqrt{3})$ of $\mathbf{Q}_2$. We must therefore examine this local biquadratic extension E and determine the possible quaternion extensions which contain it.

Our starting point will be a theorem due to E. Witt giving a precise description of these quaternion extensions.

Theorem 3.1.1 *(E. Witt) Let K be a field and let $u, v \in K \setminus K^2$ be such that $uv \notin K^2$. Then the following statements are equivalent.*

(i) The biquadratic extension $K(\sqrt{u}, \sqrt{v})$ of K admits a quaternion extension over K.

(ii) The quadratic form $Q(X_1, X_2, X_3) = uX_1^2 + vX_2^2 + (1/uv)X_3^2$ is equivalent to the diagonal quadratic form $Y_1^2 + Y_2^2 + Y_3^2$, with an equivalence given by

$$X_i = \sum_{i,j=1} p_{ij} Y_j\,, \qquad P = (p_{ij}) \text{ with } \det(P) = 1\,.$$

When these conditions hold, the quaternion extensions over K that contain $K(\sqrt{u}, \sqrt{v})$ are given by

$$L = K\left(\sqrt{r\left(1 + p_{11}\sqrt{u} + p_{22}\sqrt{v} + p_{33}\left(\frac{1}{\sqrt{uv}}\right)\right)}\right),$$

where $r \in K^*$.

Proof: A proof may be found in [18]. □

Using Witt's Theorem, we see immediately that the existence of a quaternion extension containing $\mathbf{Q}_2(\sqrt{2},\sqrt{3})$ is equivalent to the existence of a 3×3 matrix P with entries in $\mathbf{Q}_2$ satisfying

$$P^T DP = I \quad \text{and} \quad \det(P) = 1\,,$$

where P^T denotes the transpose of P, $D = \mathrm{diag}(2,3,1/6)$, and I is the 3×3 identity matrix.

We choose P to be the matrix

$$P = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 & 0 \\ -1/3 & 1/3 & -1/3 \\ -1 & 1 & 2 \end{pmatrix}.$$

Then

$$\begin{aligned} P^T DP &= \begin{pmatrix} 1/2 & -1/3 & -1 \\ 1/2 & 1/3 & 1 \\ 0 & -1/3 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1/6 \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 & 0 \\ -1/3 & 1/3 & -1/3 \\ -1 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 & -1/6 \\ 1 & 1 & 1/6 \\ 0 & -1 & 1/3 \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1/6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

and

$$det(P) = (1/2)\begin{vmatrix} 1/3 & -1/3 \\ 1 & 2 \end{vmatrix} - (1/2)\begin{vmatrix} -1/3 & -1/3 \\ -1 & 2 \end{vmatrix} = 2/3 + 1/3 = 1\,.$$

We now set

$$\begin{aligned} \alpha_{\pm}^2 &= \pm(1 + p_{11}\sqrt{u} + p_{22}\sqrt{v} + p_{33}(1/\sqrt{uv})) \\ &= \pm(1 + (1/2)\sqrt{2} + (1/3)\sqrt{3} + (1/3)\sqrt{6}) \\ &= \pm(\sqrt{6}/6)\,(1+\sqrt{2})\,(\sqrt{2}+\sqrt{3}). \end{aligned}$$

Witt's Theorem now implies that every quaternion extension of $\mathbf{Q}_2$ containing $\mathbf{Q}_2(\sqrt{2},\sqrt{3})$ has the form $L = \mathbf{Q}_2(\sqrt{r\alpha_+^2})$ for some $r \in \mathbf{Q}_2^*$. We take $r = \pm 1$ and set $L_\pm = \mathbf{Q}_2(\alpha_\pm)$.

In [18] it is shown that there are precisely two non-isomorphic quaternion extensions of $\mathbf{Q}_2$ which contain $E = \mathbf{Q}_2(\sqrt{2},\sqrt{3})$, and that for $r, s \in \mathbf{Q}_2^*$,

$$\mathbf{Q}_2(\sqrt{r\alpha_+^2}) \cong \mathbf{Q}_2(\sqrt{s\alpha_+^2})$$

if and only if $r/s \in (\mathbf{Q}_2^*)^2$. Since $-1 \notin (\mathbf{Q}_2^*)^2$, these observations prove the following lemma.

Lemma 3.1.2 *The extensions $L_\pm/\mathbf{Q}_2$ constructed above are precisely the two non-isomorphic quaternion extensions of $\mathbf{Q}_2$ which contain the biquadratic subfield $E = \mathbf{Q}_2(\sqrt{2},\sqrt{3})$.* □

Notation: We label the subextensions of $L_\pm$ as follows. We let $K_2 = \mathbf{Q}_2(\sqrt{2})$, $K_3 = \mathbf{Q}_2(\sqrt{3})$, $K_6 = \mathbf{Q}_2(\sqrt{6})$ and, as above, $E = \mathbf{Q}_2(\sqrt{2},\sqrt{3})$. As usual, we let π_H denote a prime (or uniformising) element for the local field H (i.e. so that $v_H(\pi_H) = 1$). Writing $\pi_i = \pi_{K_i}$ we choose $\pi_2 = \sqrt{2}$, $\pi_3 = 1 + \sqrt{3}$ and $\pi_6 = \sqrt{6}$. For the field E, our choice of prime will be

$$\pi_E = 1 + \pi_3/\pi_2 = 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{6}}{2}.$$

Finally, we choose

$$\pi_{L_\pm} = 1 + \pi_E \alpha_\pm .$$

Lemma 3.1.3 *(a) Let $a, b, c, d \in \mathbf{Q}_2$ and set $z = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in E$. Then*

$$N_{E/\mathbf{Q}_2}(z) = (a^2 + 2b^2 - 3c^2 - 6d^2)^2 - 2(2ab - 6cd)^2 .$$

(b) Let $L = L_\pm$ and $\alpha = \alpha_\pm$. The element π_L defined above is a prime element of L.

Proof: (a) follows from the computation:

$$\begin{aligned} N_{E/\mathbf{Q}_2}(z) &= N_{K_2/\mathbf{Q}_2} N_{E/K_2}(a + b\sqrt{2} + \sqrt{3}(c + d\sqrt{2})) \\ &= N_{K_2/\mathbf{Q}_2}((a + b\sqrt{2})^2 - 3(c + d\sqrt{2})^2) \\ &= N_{K_2/\mathbf{Q}_2}((a^2 + 2b^2 - 3c^2 - 6d^2) + (2ab - 6cd)\sqrt{2}) \\ &= (a^2 + 2b^2 - 3c^2 - 6d^2)^2 - 2(2ab - 6cd)^2 . \end{aligned}$$

(b) We prove the result for $L = L_+$, the case $L = L_-$ being similar.

We first recall that for the tower of fields $\mathbf{Q}_2 \subset K_2 \subset E \subset L$, we have a commutative diagram of the form

$$\begin{tikzcd} L \arrow[r, "N_{L/E}"] \arrow[d, "v_L"] & E \arrow[r, "N_{E/K_2}"] \arrow[d, "v_E"] & K_2 \arrow[r, "N_{K_2/\mathbf{Q}_2}"] \arrow[d, "v_{K_2}"] & \mathbf{Q}_2 \arrow[d, "v_{\mathbf{Q}_2}"] \\ \mathbf{Z} \arrow[r, "f_{L/E} = 1"] & \mathbf{Z} \arrow[r, "f_{E/K_2} = 1"] & \mathbf{Z} \arrow[r, "f_{K_2/\mathbf{Q}_2} = 1"] & \mathbf{Z} \end{tikzcd} \tag{3.1.19}$$

Hence we compute (with $\alpha = \alpha_+$)

$$\begin{aligned} & v_L(\pi_L) = v_E(1 - \pi_E^2 \alpha^2) \\ & = v_E\left[1 - (3 + \sqrt{2} + \sqrt{3} + \sqrt{6})\,(1 + (1/2)\sqrt{2} + (1/3)\sqrt{3} + (1/3)\sqrt{6})\right] \\ & = v_E\left[-6 - \tfrac{9}{2}\sqrt{2} - \tfrac{11}{3}\sqrt{3} - \tfrac{17}{6}\sqrt{6}\right] \\ & = v_{\mathbf{Q}_2} \cdot N_{E/\mathbf{Q}_2}\left[-6 - (9/2)\sqrt{2} - (11/3)\sqrt{3} - (17/6)\sqrt{6}\right] \\ & = v_{\mathbf{Q}_2}\left[(6^2 + 2(9/2)^2 - 3(11/3)^2 - 6(17/6)^2)^2 \right. \\ & \qquad \left. -2\,(2(6)(9/2) - 6(11/3)(17/6))^2\right] \\ & = v_{\mathbf{Q}_2}\left[(1/36)(-72)^2 - (2/9)(-25)^2\right] \end{aligned}$$

$$
\begin{aligned}
&= v_{\mathbf{Q}_2}[144-(2/9)(625)] \\
&= v_{\mathbf{Q}_2}[2((81)(8)-625)/9] \\
&= v_{\mathbf{Q}_2}(2)+v_{\mathbf{Q}_2}((81)(8)-625)-v_{\mathbf{Q}_2}(9) \\
&= 1+0-0=1\,,
\end{aligned}
$$

as claimed. □

We now consider the Galois action of the group Q_8 on these extensions.

Lemma 3.1.4 *Let $L = L_\pm$ and $\alpha = \alpha_\pm$. Then the Galois action of Q_8 on $L/\mathbf{Q}_2$ is given by the formulae:*

$$
\begin{aligned}
x(\sqrt{2}) &= -\sqrt{2} & y(\sqrt{2}) &= \sqrt{2} \\
x(\sqrt{3}) &= \sqrt{3} & y(\sqrt{3}) &= -\sqrt{3} \\
x(\alpha) &= (\sqrt{2}-1)(\sqrt{3}-\sqrt{2})\,\alpha & y(\alpha) &= (\sqrt{3}-\sqrt{2})\,\alpha
\end{aligned}
$$

Proof: It suffices to check that the defining relations for Q_8 hold for the action on α. First note that

$$
\begin{aligned}
x^2(\alpha) &= x((\sqrt{2}-1)(\sqrt{3}-\sqrt{2})\,\alpha) \\
&= x((\sqrt{2}-1))\,x((\sqrt{3}-\sqrt{2}))\,x(\alpha) \\
&= (-\sqrt{2}-1)(\sqrt{3}+\sqrt{2})(\sqrt{2}-1)(\sqrt{3}-\sqrt{2})\,\alpha \\
&= (-\sqrt{2}-1)(\sqrt{2}-1)(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2})\,\alpha \\
&= -\alpha
\end{aligned}
$$

and

$$
\begin{aligned}
y^2(\alpha) &= y((\sqrt{3}-\sqrt{2})\,\alpha) \\
&= y((\sqrt{3}-\sqrt{2}))\,y(\alpha) \\
&= (-\sqrt{3}-\sqrt{2})(\sqrt{3}-\sqrt{2})\,\alpha \\
&= -\alpha
\end{aligned}
$$

so that on L, we have $x^2 = y^2$ and $y^4 = 1$. Finally, we compute that $yxy = x$

on L:

$$\begin{aligned} yxy(\alpha) &= yx\left[(\sqrt{3}-\sqrt{2})\,\alpha\right] \\ &= y\left[x(\sqrt{3}-\sqrt{2})\,x(\alpha)\right] \\ &= y\left[(\sqrt{3}+\sqrt{2})\,(\sqrt{2}-1)\,(\sqrt{3}-\sqrt{2})\,\alpha\right] \\ &= y(\sqrt{2}-1)\,y(\alpha) \\ &= (\sqrt{2}-1)\,(\sqrt{3}-\sqrt{2})\,\alpha \\ &= x(\alpha)\,. \end{aligned}$$

□

3.2 The Fundamental 2-Extension

Throughout this subsection, we let $L = L_{\pm}$. Let $\mathbf{Q}_{2,nr}$ denote the maximal unramified extension of $\mathbf{Q}_2$ and let F denote the Frobenius automorphism of $\mathbf{Q}_{2,nr}/\mathbf{Q}_2$. We write L_0 for the compositum $L \cdot \mathbf{Q}_{2,nr}$. Note that since L is totally ramified over $\mathbf{Q}_2$, we have that $L \cap \mathbf{Q}_{2,nr} = \mathbf{Q}_2$.

There is an isomorphism (cf. [32, Ch.1] or [31, Ch.7])

$$\lambda : L \otimes_{\mathbf{Q}_2} \mathbf{Q}_{2,nr} \longrightarrow L_0 \tag{3.2.20}$$

given by setting $\lambda(z \otimes w) = zw$.

From the construction in [31, Ch.7], the fundamental class of the extension $L/\mathbf{Q}_2$ is represented by a 2-extension of the form

$$1 \longrightarrow L^* \xrightarrow{i} (L \otimes_{\mathbf{Q}_2} \mathbf{Q}_{2,nr})^* \xrightarrow{(1\otimes F)/1} (L \otimes_{\mathbf{Q}_2} \mathbf{Q}_{2,nr})^* \xrightarrow{\omega} \mathbf{Z} \longrightarrow 0\,, \tag{3.2.21}$$

where the maps are defined as follows.

For $z \in L^*$ we set $i(z) = z \otimes 1$. For $z \in L^*$ and $w \in \mathbf{Q}_{2,nr}^*$, the map

$$1 \otimes F : (L \otimes_{\mathbf{Q}_2} \mathbf{Q}_{2,nr})^* \longrightarrow (L \otimes_{\mathbf{Q}_2} \mathbf{Q}_{2,nr})^*$$

is given by

$$(1 \otimes F)\,(z \otimes w) = z \otimes F(w)\,.$$

Finally, the map ω is given by composing

$$\omega = v_{L_0} \cdot \lambda \,:\, (L \otimes_{\mathbf{Q}_2} \mathbf{Q}_{2,nr})^* \longrightarrow L_0^* \longrightarrow \mathbf{Z}\,.$$

By [32, Lemma 1.2.7] the sequence (3.2.21) is exact.

We now use the map (3.2.20) to determine the Galois action on L_0. Following [31, p.303], we have a map, given by restriction to the intersection $L \cap \mathbf{Q}_{2,nr} = \mathbf{Q}_2$:

$$h \,:\, G(\mathbf{Q}_{2,nr}/\mathbf{Q}_2) \times G(L/\mathbf{Q}_2) \longrightarrow G(L \cap \mathbf{Q}_{2,nr}/\mathbf{Q}_2) = 1$$

given by

$$h(F^i, z) = (F^i \,|\, \mathbf{Q}_2)\,(z \,|\, \mathbf{Q}_2)^{-1}\,,$$

where $(a \,|\, H)$ denotes the restriction of the map a to the field H. Since each of $(F^i \,|\, \mathbf{Q}_2)$ and $(z \,|\, \mathbf{Q}_2)$ is trivial, we may choose for each i and each $z \in G(L/\mathbf{Q}_2)$ an element of $G(L_0/\mathbf{Q}_2)$ which equals F^i on $\mathbf{Q}_{2,nr}$ and equals z on L. In other words, we have an isomorphism

$$G(\mathbf{Q}_{2,nr}/\mathbf{Q}_2) \times G(L/\mathbf{Q}_2) \xrightarrow{\cong} G(L_0/\mathbf{Q}_2)\,.$$

In particular, we may define an element $F_0 \in G(L_0/\mathbf{Q}_2)$ by demanding that $(F_0 \,|\, \mathbf{Q}_{2,nr}) = F$ and $(F_0 \,|\, L) = 1$.

Using the sequence (3.2.21) and the following commutative diagram (cf. [31, Lemma 7.1.15])

$$\begin{tikzcd}
L^* \arrow[r] \arrow[d, "1"] & (L \otimes_{\mathbf{Q}_2} \mathbf{Q}_{2,nr})^* \arrow[r, "(1 \otimes F)/1"] \arrow[d, "\lambda"] & (L \otimes_{\mathbf{Q}_2} \mathbf{Q}_{2,nr})^* \arrow[r, "\omega"] \arrow[d, "\lambda"] & \mathbf{Z} \arrow[d, "1"] \\
L^* \arrow[r] & L_0^* \arrow[r, "F_0/1"] & L_0^* \arrow[r, "v_{L_0}"] & \mathbf{Z}
\end{tikzcd} \qquad (3.2.22)$$

where the outside maps are identities and the middle maps are the isomorphism λ, we see that we may also use the lower sequence as a representative for the fundamental class of $L/\mathbf{Q}_2$. We note in passing that the map $F_0/1$ is given by $(F_0/1)(z) = F_0(z)/z$. This map therefore sends every element of L to 1, and acts as $F(z)/z$ for $z \in \mathbf{Q}_{2,nr}$.

3.2.1 Constructing the 2-Cocycle

We want to construct a commutative diagram of $\mathbf{Z}[Q_8]$-modules of the form

$$\begin{tikzcd}
Ker(d) \arrow[r] \arrow[d, "k"] & \mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8] \arrow[r, "d"] \arrow[d, "j"] & \mathbf{Z}[Q_8] \arrow[r, "\varepsilon"] \arrow[d, "i"] & \mathbf{Z} \arrow[d, "1"] \\
L_{\pm}^{*} \arrow[r] & L_0^{*} \arrow[r, "F_0/1"] & L_0^{*} \arrow[r, "\varepsilon"] & \mathbf{Z}
\end{tikzcd} \tag{3.2.23}$$

The top row in this diagram is the beginning of the standard, periodic $\mathbf{Z}[Q_8]$-resolution of $\mathbf{Z}$. The $\mathbf{Z}[Q_8]$-map ϵ is given by $\epsilon(1) = 1$. If b and b' denote the two free generators of $\mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8]$, then the map d is given by

$$d(b) = x - 1 \quad \text{and} \quad d(b') = y - 1\,.$$

As noted in [32, p.139], $Ker(d)$ is the $\mathbf{Z}[Q_8]$-submodule of $\mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8]$ generated by

$$c_1 = (1+x)b - (1+y)b'$$

and

$$c_2 = (xy+1)b + (x-1)b'\,.$$

We also note that as an abelian group, $Ker(d)$ is free of $\mathbf{Z}$-rank 9. The bottom row in the above diagram is the 2-extension constructed in diagram (3.2.22).

The vertical maps in this diagram are constructed as follows. First we define the $\mathbf{Z}[Q_8]$-map i by

$$i(1) = \pi_L \in L_0^*.$$

Commutativity of the right hand square is then obvious, since π_L is a prime element for L_0.

In order to construct j, we first notice that

$$\begin{aligned} i \cdot d(b) &= i(x-1) \\ &= (x-1)\, i(1) \\ &= (x-1)(\pi_L) = x(\pi_L)/\pi_L. \end{aligned}$$

Similarly, we have $i \cdot d(b') = y(\pi_L)/\pi_L$.

Since $v_{L_0}(x(\pi_L)) = v_{L_0}(y(\pi_L)) = v_{L_0}(\pi_L) = 1$, exactness of the lower row in (3.2.23) implies that there exist elements $t_1, t_2 \in L_0^*$ such that

$$(F_0/1)(t_1) = \frac{F_0(t_1)}{t_1} = \frac{y(\pi_L)}{\pi_L} \tag{3.2.24}$$

and

$$(F_0/1)(t_2) = \frac{F_0(t_2)}{t_2} = \frac{x(\pi_L)}{\pi_L}. \tag{3.2.25}$$

Once we have made appropriate choices for these elements $t_1, t_2 \in L_0^*$, we may fill in the diagram to make the middle square commute, i.e., we may define

$$j(b) = t_2 \quad \text{and} \quad j(b') = t_1.$$

Finally, the map k on the left is defined by simply restricting j to $Ker(d)$. There is only one minor item to check.

Lemma 3.2.1 *With the notation introduced above, $k(Ker(d)) \subset L^*$.*

Proof: We compute that

$$\begin{aligned}
(F_0/1)\cdot j(c_1) &= (F_0/1)\cdot j((1+x)b-(1+y)b') \\
&= (F_0/1)\left[t_2\, x(t_2)t_1^{-1}\, y(t_1)^{-1}\right] \\
&= F_0(t_2)\, t_2^{-1}\, F_0(x(t_2))\, x(t_2)^{-1}\, t_1\, F_0(t_1)^{-1}\, y(t_1)\, F_0(y(t_1)^{-1} \\
&= F_0(t_2)\, t_2^{-1}\, x(F_0(t_2)\, t_2^{-1})\, t_1\, F_0(t_1)^{-1}\, y(t_1\, F_0(t_1)^{-1}) \\
&= x(\pi_L)\, \pi_L^{-1}\, x(x(\pi_L)\, \pi_L^{-1})\, \pi_L\, y(\pi_L)^{-1}\, y(\pi_L\, y(\pi_L)^{-1}) \\
&= x(\pi_L)\, \pi_L^{-1}\, x^2(\pi_L)\, x(\pi_L)^{-1}\, \pi_L\, y(\pi_L)^{-1}\, y(\pi_L)\, y^2(\pi_L)^{-1} \\
&= 1\,,
\end{aligned}$$

since $x^2 = y^2$ on L. Likewise, since $xyx = y$ on L,

$$\begin{aligned}
(F_0/1)\cdot j(c_2) &= (F_0/1)\cdot j((xy+1)b+(x-1)b') \\
&= (F_0/1)\left[t_2\, xy(t_2)\, x(t_1)\, t_1^{-1}\right] \\
&= F_0(t_2)\, t_2^{-1}\, F_0(xy(t_2))\, xy(t_2)^{-1} \\
&\qquad \cdot F_0(x(t_1))\, x(t_1)^{-1}\, t_1\, F_0(t_1)^{-1} \\
&= F_0(t_2)\, t_2^{-1}\, xy(F_0(t_2)\, t_2^{-1})\, x(F_0(t_1)\, t_1^{-1})\, t_1\, F_0(t_1)^{-1} \\
&= x(\pi_L)\, \pi_L^{-1}\, xy(x(\pi_L)\, \pi_L^{-1})\, x(y(\pi_L)\, \pi_L^{-1})\, \pi_L\, y(\pi_L)^{-1} \\
&= x(\pi_L)\, \pi_L^{-1}\, xyx(\pi_L)\, xy(\pi_L)^{-1}\, xy(\pi_L)\, x(\pi_L)^{-1}\, \pi_L\, y(\pi_L)^{-1} \\
&= 1\,.
\end{aligned}$$

Hence, by exactness of the bottom row, we see that $j(c_1)$ and $j(c_2)$ lie in L^*, as required. □

3.2.2 Choosing the elements t_1 and t_2

We are going to try to make choices of the elements t_1 and t_2 so as to optimize the resulting map k in diagram (3.2.23), in the sense that our computations will be as simple as possible. For us it will turn out that with suitable choices, the resulting k will be injective and have finite cokernel.

We begin by discussing a method of filtering the fundamental 2-extension to derive similar such sequences for the unit groups of level n for $n \geq 0$. This is done in full generality in [32, pp.137-9]. Consider the following commutative diagram.

$$\begin{tikzcd}
L^* \arrow[r] \arrow[d, "v"] & L_0^* \arrow[r, "F_0/1"] \arrow[d, "v"] & L_0^* \arrow[r, "v"] \arrow[d, "v"] & \mathbf{Z} \arrow[d, "1"] \\
\mathbf{Z} \arrow[r, "1"] & \mathbf{Z} \arrow[r, "0"] & \mathbf{Z} \arrow[r, "1"] & \mathbf{Z}
\end{tikzcd} \tag{3.2.26}$$

Here the maps denoted v are the appropriate valuation maps. The lower sequence is trivially exact and the vertical maps are all surjective, so we obtain a short exact kernel sequence

$$\{1\} \longrightarrow \mathcal{O}_L^* \longrightarrow \mathcal{O}_{L_0}^* \xrightarrow{F_0/1} \mathcal{O}_{L_0}^* \longrightarrow 0\,.$$

Exactness of this sequence follows from the Snake lemma or from the following simple observations. Exactness at the first two terms is a trivial diagram chase. For the final term, if $w \in \mathcal{O}_{L_0}^*$, then viewed as an element of L_0^*, it clearly lies in the image of $F_0/1$. Let w' be any preimage and let $m = v_{L_0}(w')$. If $m = 0$ then we have $w' \in \mathcal{O}_{L_0}^*$, as required. Otherwise, select $z \in L^*$ with $v_L(z) = -m$. Then $(F_0/1)(z) = 1$, so that $(F_0/1)(zw') = w$ and $v_{L_0}(zw') = 0$, meaning that zw' is our required preimage of w in $\mathcal{O}_{L_0}^*$.

We now consider the following commutative diagram of horizontal short exact sequences and vertical quotient maps.

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_L^* \arrow[r] \arrow[d] & \mathcal{O}_{L_0}^* \arrow[r, "F_0/1"] \arrow[d] & \mathcal{O}_{L_0}^* \arrow[r, "v"] \arrow[d] & 0 \\
1 \arrow[r] & \overline{L}^* \arrow[r] & \overline{L_0}^* \arrow[r, "F_0/1"] & \overline{L_0}^* \arrow[r, "v"] & 0
\end{tikzcd}$$

Here the lower sequence is short exact. This follows from the fact that the Frobenius, $F_0 : L_0^* \longrightarrow L_0^*$, is an automorphism and hence restricts to an automorphism of $\mathcal{O}_{L_0}^*$ and induces an automorphism of $\overline{L_0}^*$. Because of this fact, we can easily solve the equation

$$F_0(\overline{u})/\overline{u} = \overline{v}$$

for $\overline{u} \in \overline{L_0}^*$, given an element $\overline{v} \in \overline{L_0}^*$, since we may pull $\overline{v}$ back to an element $v \in \mathcal{O}_{L_0}^*$ and solve for $u \in \mathcal{O}_{L_0}^*$. Exactness at the middle term follows from the observation that the fixed field of F_0 acting on $\overline{L_0}$ is $\overline{L}$, so that the image of $\overline{L}^*$ in $\overline{L_0}^*$ is precisely the kernel of the map $F_0/1$. (Of course in our case, $\overline{L}$ is the field of order two, so that here $\overline{L}^* = \{1\}$).

Applying the Snake Lemma to this diagram, we obtain a short exact sequence

$$\{1\} \longrightarrow U_L^1 = \mathcal{O}_L^* \longrightarrow U_{L_0}^1 \xrightarrow{F_0/1} U_{L_0}^1 \longrightarrow 0$$

of level-one unit groups. Recalling that (cf. [29, IV,Prop. 6]) we have an isomorphism of groups of the form $U_L^1/U_L^2 \cong \overline{L}$ (and similarly for L_0), we are led to construct another commutative diagram of horizontal short exact sequences and vertical quotient maps:

$$\begin{tikzcd}
1 \arrow[r] & U_L^1 \arrow[r] \arrow[d] & U_{L_0}^1 \arrow[r, "F_0/1"] \arrow[d] & U_{L_0}^1 \arrow[r] \arrow[d] & 0 \\
1 \arrow[r] & \overline{L} \arrow[r] & \overline{L_0} \arrow[r, "F_0/1"] & \overline{L_0} \arrow[r] & 0
\end{tikzcd}$$

Again we obtain, via the Snake Lemma, a short exact kernel sequence

$$\{1\} \longrightarrow U_L^2 \longrightarrow U_{L_0}^2 \xrightarrow{F_0/1} U_{L_0}^2 \longrightarrow 0\,.$$

Since for each $n \geq 1$ there exists a similar group isomorphism, $U_L^n/U_L^{n+1} \cong \overline{L}$, we may inductively arrive at the following result.

Proposition 3.2.2 *The fundamental 2-extension (3.2.21) induces exact sequences, for all $n \geq 0$,*

$$\{1\} \longrightarrow U_L^n \longrightarrow U_{L_0}^n \xrightarrow{F_0/1} U_{L_0}^n \longrightarrow 0\,.$$

This proposition is extremely useful in that it allows us to narrow our search for appropriate elements t_1 and t_2.

Lemma 3.2.3 *The elements $x(\pi_L)/\pi_L$ and $y(\pi_L)/\pi_L$ in equations (3.2.24) and (3.2.25) satisfy (modulo $\pi_L^{19}\mathcal{O}_L$)*

$$\frac{x(\pi_L)}{\pi_L} \equiv 1 + \pi_L^3 + \pi_L^4 + \pi_L^5 + \pi_L^6 + \pi_L^7 + \pi_L^8 + \pi_L^9 + \pi_L^{10} + \pi_L^{11} + \pi_L^{12} + \pi_L^{16} + \pi_L^{17} + \pi_L^{18}$$

and

$$\frac{y(\pi_L)}{\pi_L} \equiv 1 + \pi_L + \pi_L^2 + \pi_L^3 + \pi_L^4 + \pi_L^8 + \pi_L^{18}\,.$$

Proof: The proof is entirely computational. We just give an idea as to how the computation is done. We use diagram (2.1.3) and Lemma 3.1.3 to compute $v_L(x(\pi_L) - \pi_L)$ as follows:

$$\begin{aligned} v_L(x(\pi_L) - \pi_L) &= v_L\left[x(\pi_E)x(\alpha) - \pi_E\alpha\right] \\ &= v_L\Big[(1 - (1/2)\sqrt{2} - (1/2)\sqrt{6})\,(\sqrt{2} - 1)\,(\sqrt{3} - \sqrt{2}) \\ &\qquad -(1 + (1/2)\sqrt{2} + (1/2)\sqrt{6})\Big] + v_L(\alpha)\,. \end{aligned}$$

Now,

$$\begin{aligned} v_L(\alpha) &= v_E(-\alpha^2) \\ &= v_E\left[-1 - (1/2)\sqrt{2} - (1/3)\sqrt{3} - (1/3)\sqrt{6}\right] \\ &= v_{\mathbf{Q}_2}\left[(1 + 2(1/4) - 3(1/9) - 6(1/9))^2\right. \\ &\qquad \left. - 2(2(-1)\,(1/2) - 6(1/3)\,(1/3))^2\right] \\ &= v_{\mathbf{Q}_2}\left[(1/2)^2 - 2(1/3)^2\right] \\ &= v_{\mathbf{Q}_2}\left[(9 - 8)/36\right] = v_{\mathbf{Q}_2}\left[1/36\right] = -2\,, \end{aligned}$$

while

$$\begin{aligned} v_L\Big[(1 - (1/2)\sqrt{2} &\quad - (1/2)\sqrt{6})\,(\sqrt{2} - 1)\,(\sqrt{3} - \sqrt{2}) - \pi_E\Big] \\ &= v_L\left[-7 + 3\sqrt{2} - 3\sqrt{3} + 2\sqrt{6}\right] \\ &= v_E\left[(-7 + 3\sqrt{2} - 3\sqrt{3} + 2\sqrt{6})^2\right] \\ &= v_E\Big[(49 + 18 + 27 + 24) + (-42 - 36)\sqrt{2} \\ &\qquad +(24 + 42)\sqrt{3} + (-28 - 18)\sqrt{6}\Big] \\ &= v_E\left[118 - 78\sqrt{2} + 66\sqrt{3} - 46\sqrt{6}\right] \\ &= v_{\mathbf{Q}_2}\left[((118)^2 + 2(78)^2 - 3(66)^2 - 6(46)^2)^2\right. \\ &\qquad \left. -2(2(118)\,(-78) - 6(66)\,(-46))^2\right] \\ &= v_{\mathbf{Q}_2}\left[(13924 + 12168 - 13068 - 12696)^2\right. \\ &\qquad \left. -2(-18408 + 18216)^2\right] \\ &= v_{\mathbf{Q}_2}\left[(328)^2 - 2(192)^2\right] \\ &= v_{\mathbf{Q}_2}\left[((8)\,(41))^2 - 2((64)\,(3))^2\right] \\ &= v_{\mathbf{Q}_2}(64) + v_{\mathbf{Q}_2}\left[(41)^2 - 2(64)\,(9)\right] = 6 + 0 = 6\,. \end{aligned}$$

This implies that $v_L(x(\pi_L) - \pi_L) = 4$, so that

$$\frac{x(\pi_L)}{\pi_L} = 1 + \pi_L^3 u$$

for some $u \in \mathcal{O}_L^*$.

We derive the next term in this expansion by computing the expression $v_L(x(\pi_L) - \pi_L - \pi_L^3)$ as above. Repeated computations (using Maple) give the stated result. The same method applied to $y(\pi_L)/\pi_L$ produces the second congruence. □

Lemma 3.2.4 *The element t_1 in equation (3.2.24) may be chosen to lie in $U_{L_0}^1$.*

Proof: By the previous lemma we have that $y(\pi_L)/\pi_L \in U_L^1 \subset U_{L_0}^1$. We must solve the equation $F_0(t_1)/t_1 = y(\pi_L)/\pi_L$. Applying Proposition 3.2.2 we have the short exact sequence

$$\{1\} \longrightarrow U_L^1 \longrightarrow U_{L_0}^1 \xrightarrow{F_0/1} U_{L_0}^1 \longrightarrow 0\,,$$

and exactness at the right hand term implies that there exists an element $u \in U_{L_0}^1$ satisfying $F_0(u)/u = y(\pi_L)/\pi_L$. Therefore we may choose $t_1 = u$, as required. □

Similarly, since $x(\pi_L)/\pi_L \in U_L^3 \subset U_{L_0}^3$, Proposition 3.2.2 with $n = 3$ gives

Lemma 3.2.5 *The element t_2, as defined in equation (3.2.25), may be chosen to lie in $U_{L_0}^3$.* □

We now choose the elements t_1 and t_2 with a little more care. In order to ease notation, we set $\pi = \pi_L$. Let ξ denote a primitive cube root of unity lying

in $\mathbf{Q}_{2,nr}$ and let ω be a primitive root of unity of odd order lying in $\mathbf{Q}_{2,nr}$, satisfying

$$\omega^2 + \omega \equiv \xi^2 \ (modulo\ 2\mathcal{O}_L).$$

We have the following result.

Lemma 3.2.6 *The element t_1 in equation (3.2.24) may be chosen to satisfy*

$$t_1 = \prod_{m=1}^{19} (1 + c_m \pi^m)(1 + u\pi^{20}),$$

with $u \in \mathcal{O}_{L_0}$ and where each c_m is a root of unity lying in $\mathbf{Q}_{2,nr}$. Moreover, in this expression we may take $c_1 = c_3 = c_5 = \xi$.

Proof: Since $t_1 \in U^1_{L_0}$, we may write t_1 in the above product form with the coefficients c_m as stated. In the factor $(1 + u\pi^{20})$, however, we must allow $u \in \mathcal{O}_{L_0}$ in order to have equality. Recall that the map F_0 acts trivially on elements of L and acts as the Frobenius F on elements of $\mathbf{Q}_{2,nr}$.

We need to verify that the elements c_1, c_3 and c_5 may be chosen to have the stated values. To do so, we clearly need only compute modulo $\pi^6\mathcal{O}_{L_0}$. We set

$$t = (1 + \xi\pi)(1 + c_2\pi^2)(1 + \xi\pi^3)(1 + c_4\pi^4)(1 + \xi\pi^5) + z$$

where $z \in \pi^6\mathcal{O}_{L_0}$, and show that t satisfies the required equation mod $\pi^6\mathcal{O}_{L_0}$. Rewriting equation (3.2.24) in the form

$$F_0(t) = t\,\frac{y(\pi)}{\pi},$$

we compute both sides mod $\pi^6\mathcal{O}_{L_0}$. We see that

$$\begin{aligned} F_0(t) &\equiv F_0((1 + \xi\pi)(1 + c_2\pi^2)(1 + \xi\pi^3)(1 + c_4\pi^4)(1 + \xi\pi^5)) \\ &\equiv (1 + \xi^2\pi)(1 + c_2^2\pi^2)(1 + \xi^2\pi^3)(1 + c_4^2\pi^4)(1 + \xi^2\pi^5) \\ &\equiv 1 + \xi^2\pi + c_2^2\pi^2 + (\xi^2c_2^2 + \xi^2)\pi^3 + (c_4^2 + \xi)\pi^4 \\ &\qquad + (\xi^2 + \xi^2c_2^2 + \xi^2c_4^2)\pi^5. \end{aligned}$$

Similarly,

$$\begin{aligned} t &\equiv (1+\xi\pi)(1+c_2\pi^2)(1+\xi\pi^3)(1+c_4\pi^4)(1+\xi\pi^5) \\ &\equiv 1+\xi\pi+c_2\pi^2+(\xi c_2+\xi)\pi^3+(c_4+\xi^2)\pi^4 \\ &\qquad +(\xi+\xi c_2+\xi c_4)\pi^5, \end{aligned}$$

so that

$$\begin{aligned} t\,y(\pi)/\pi &\equiv t(1+\pi+\pi^2+\pi^3+\pi^4) \\ &\equiv 1+(1+\xi)\pi+(1+\xi+c_2)\pi^2+(1+c_2+\xi c_2)\pi^3 \\ &\qquad +(\xi+c_2+\xi c_2+c_4)\pi^4+(1+c_2+c_4+\xi c_4)\pi^5. \end{aligned}$$

Here we have used the fact that $2 \in \pi^8\mathcal{O}_L$. Hence we see that

$$\begin{aligned} t\,y(\pi)/\pi - F_0(t) &\equiv 1+(1+\xi-\xi^2)\pi+(1+\xi+c_2-c_2^2)\pi^2 \\ &\quad +(1+c_2+\xi c_2-\xi^2c_2^2-\xi^2)\pi^3+(\xi+c_2+\xi c_2+c_4-c_4^2-\xi)\pi^4 \\ &\quad +(1+c_2+c_4+\xi c_4-\xi^2-\xi^2c_2^2-\xi^2c_4^2)\pi^5 \\ &\equiv 1+(\xi^2+c_2+c_2^2)\pi^2+(c_2+\xi c_2+\xi^2c_2^2+\xi)\pi^3 \\ &\quad +(c_2+\xi c_2+c_4+c_4^2)\pi^4+(c_2+c_4+\xi c_4+\xi+\xi^2c_2^2+\xi^2c_4^2)\pi^5. \end{aligned}$$

Now, this element must be trivial, so that the coefficients must be 0 mod $2\mathcal{O}_{L_0}$. Therefore, working mod 2, we see first of all that

$$c_2^2+c_2 \equiv -\xi^2 \equiv \xi^2.$$

We may use this relation to simplify the coefficient of π^3. This becomes

$$\begin{aligned} \xi^2c_2^2+c_2+\xi c_2+\xi &\equiv \xi^2(c_2+\xi^2)+c_2+\xi c_2+\xi \\ &\equiv (\xi^2+\xi+1)c_2+2\xi \\ &\equiv 0, \end{aligned}$$

so that our choice of $c_3=\xi$ is valid. We see now that the coefficient c_4 must satisfy

$$c_2+\xi c_2+c_4+c_4^2 \equiv 0,$$

which allows us to simplify the coefficient of π^5 to

$$\begin{aligned}
&\xi^2 c_4^2 + \xi^2 c_2^2 + c_2 + c_4 + \xi c_4 + \xi \\
&\qquad \equiv \xi^2(c_2 + \xi c_2 + c_4) + \xi^2(c_2 + \xi^2) + c_2 + c_4 + \xi c_4 + \xi \\
&\qquad \equiv (\xi^2 + \xi + 1)c_4 + 2\xi^2 c_2 + 2c_2 + 2\xi \\
&\qquad \equiv 0\,,
\end{aligned}$$

so that our choice of c_5 is valid. □

We may make a similar choice for the element t_2.

Lemma 3.2.7 *The element t_2 in equation (3.2.25) may be chosen to satisfy*

$$t_2 = \prod_{m=3}^{19} (1 + d_m \pi^m)\,(1 + u\pi^{20})\,,$$

with $u \in \mathcal{O}_{L_0}$ and where each d_m is a root of unity lying in $\mathbf{Q}_{2,nr}$. Moreover, in this expression we may take $d_3 = d_4^2 = d_5 = d_7 = \xi$ and $d_6 = \omega$, where ω satisfies the congruence noted in the preamble to Lemma 3.2.6.

Proof: The proof follows in a manner similar to that of the previous lemma. First note that since $t_2 \in U_{L_0}^3$, we may write t_2 in the above product form with the coefficients d_m as stated. However, as in Lemma 3.2.6, in the factor $(1 + u\pi^{20})$ we must allow $u \in \mathcal{O}_{L_0}$ in order to have equality.

We need to verify that the elements d_m, $m = 3, 4, 5, 6, 7$, may be chosen to have the stated values. To do so, this time we need to compute modulo $\pi^8 \mathcal{O}_{L_0}$. Following the argument of Lemma 3.2.6, we set

$$t = (1 + \xi\pi^3)\,(1 + \xi^2\pi^4)\,(1 + \xi\pi^5)\,(1 + \omega\pi^6)\,(1 + \xi\pi^7) + z$$

where $z \in \pi^8 \mathcal{O}_{L_0}$, and show that t satisfies the required equation mod $\pi^8 \mathcal{O}_{L_0}$. Rewriting equation (3.2.25) in the form

$$F_0(t) = t\,\frac{x(\pi)}{\pi}\,,$$

we compute both sides mod $\pi^8 \mathcal{O}_{L_0}$. We first see that

$$\begin{aligned} F_0(t) &\equiv F_0((1+\xi\pi^3)(1+\xi^2\pi^4)(1+\xi\pi^5)(1+\omega\pi^6)(1+\xi\pi^7)) \\ &\equiv (1+\xi^2\pi^3)(1+\xi\pi^4)(1+\xi^2\pi^5)(1+\omega^2\pi^6)(1+\xi^2\pi^7) \\ &\equiv 1+\xi^2\pi^3+\xi\pi^4+\xi^2\pi^5+\omega^2\pi^6+\xi\pi^7. \end{aligned}$$

Similarly,

$$\begin{aligned} t &\equiv (1+\xi\pi^3)(1+\xi^2\pi^4)(1+\xi\pi^5)(1+\omega\pi^6)(1+\xi\pi^7) \\ &\equiv 1+\xi\pi^3+\xi^2\pi^4+\xi\pi^5+\omega\pi^6+\xi^2\pi^7, \end{aligned}$$

so that

$$\begin{aligned} t\,y(\pi)/\pi &\equiv t\,(1+\pi^3+\pi^4+\pi^5+\pi^6+\pi^7) \\ &\equiv 1+(1+\xi)\pi^3+(1+\xi^2)\pi^4+(1+\xi)\pi^5 \\ &\quad +(\omega+\xi+1)\pi^6+(1+\xi+2\xi^2)\pi^7. \end{aligned}$$

Here we have again made use of the fact that $2 \in \pi^8\mathcal{O}_L$. Comparing coefficients as before shows that we may choose the d_m as stated. □

The reason for making the above choices for the elements t_1 and t_2 will become apparent in the next section. We will be computing norms of these elements, and the computations become simpler if we compute the norms of each term in the product separately and multiply the answers.

We close this section by computing the images under k of the generators c_1 and c_2 of $Ker(d)$, using the above choices of t_1 and t_2. These values will be used in Section 4.3.

Lemma 3.2.8 *Let k be the homomorphism defined via the diagram (3.2.23) and let c_1 and c_2 be the generators for $Ker(d)$. Then there exist $u, v \in \mathcal{O}_L$ such that*

$$(i) \quad k(c_1) = \frac{1}{\pi^2}(1+\pi+\pi^2+u\pi^4);$$

$$(ii) \quad k(c_2) = 1+\pi^3+\pi^4+v\pi^6.$$

Proof: From diagram (3.2.23) we see immediately that

$$k(c_1) = \frac{t_2 x(t_2)}{\pi t_1 y(\pi t_1)}$$

and

$$k(c_2) = \frac{t_2 x y(t_2) x(\pi t_1)}{\pi t_1}.$$

By the above lemma, we may write

$$t_1 = 1 + \xi\pi + z\pi^2 \qquad \textit{and} \qquad t_2 = 1 + \xi\pi^3 + w\pi^4,$$

with $z, w \in \mathcal{O}_{L_0}$. Also, by Lemma 3.2.3 we may write, modulo $\pi^6\mathcal{O}_{L_0}$,

$$x(\pi) = 1 + \pi^3 + \pi^4 + \pi^5 \qquad \textit{and} \qquad y(\pi) = 1 + \pi + \pi^2 + \pi^3 + \pi^4.$$

We begin by computing $k(c_1)$. This is accomplished by computing each piece. For the numerator of $k(c_1)$ we compute, modulo $\pi^4\mathcal{O}_{L_0}$,

$$\begin{aligned} t_2 x(t_2) &\equiv (1 + \xi\pi^3 + w\pi^4)(1 + \xi x(\pi^3) + x(w\pi^4)) \\ &\equiv 1 + \xi(\pi^3 + x(\pi^3)) \equiv 1, \end{aligned}$$

since $x(\pi^3) \equiv \pi^3$. Similarly, using the fact that for $a \in \mathcal{O}_{L_0}$ we have $a + y(a) \in \pi^2\mathcal{O}_{L_0}$, we compute

$$\begin{aligned} t_1 y(t_1) &\equiv (1 + \xi\pi + z\pi^2)(1 + \xi y(\pi) + y(z\pi^2)) \\ &\equiv 1 + \xi(\pi + y(\pi)) + \xi^2\pi y(\pi) \\ &\equiv 1 + \pi^2 + \pi^3. \end{aligned}$$

Moreover, modulo $\pi^6\mathcal{O}_{L_0}$, we have

$$\pi y(\pi) \equiv \pi^2 + \pi^3 + \pi^4 + \pi^5 \equiv \pi^2(1 + \pi + \pi^2 + \pi^3),$$

Combining these results yields the relation (i).

The proof of (ii) is similar. Working modulo $\pi^6\mathcal{O}_{L_0}$, Lemma 3.2.3 implies that

$$\frac{x(\pi)}{\pi} \equiv 1 + \pi^3 + \pi^4 + \pi^5.$$

Computations of the sort done above reveal that

$$\frac{x(t_1)}{t_1} \equiv 1 + \xi\pi^4 + \pi^5$$

and

$$t_2\, xy(t_2) \equiv 1 + \xi\pi^4 .$$

Multiplying these elements yields the stated result.

Finally, note that the images $k(c_1)$ and $k(c_2)$ lie in L^*, so that in the given relations we may indeed take $u, v \in \mathcal{O}_L$. □

3.3 Injectivity of k

The purpose of this section is to prove that the map

$$k : Ker(d) \longrightarrow L^*$$

of diagram (3.2.23) is injective.

The proof itself involves some computation and so, to simplify the proof we will extract these computations and present them as a lemma.

We write

$$\sigma = (1+y)(1+x+x^2+x^3) \tag{3.3.29}$$

$$\tau = (1-y)(1+x+x^2+x^3) \tag{3.3.30}$$

$$\lambda = (1-x)(1+y+y^2+y^3) \tag{3.3.31}$$

$$\rho = (1-x)(1+(xy)+(xy)^2+(xy)^3) \tag{3.3.32}$$

for the four rational idempotents of Q_8^{ab} which decompose $\mathbf{Q}[Q_8]^{<x^2>}$.

Lemma 3.3.1 *Let t_1 and t_2 be the liftings of $y(\pi)/\pi$ and $x(\pi)/\pi$ chosen in Lemmas 3.2.6 and 3.2.7. With the notation above we have*

$$(i)\ \sigma(t_2) = 13 + 32u_1\,;$$

$$(ii)\ \tau(t_2) = 25 + 20\sqrt{3} + 32u_2\,;$$

$$(iii)\ \lambda(\pi t_1) = 29 + 6\sqrt{2} + 32u_3\,;$$

$$(iv)\ \rho(t_2/(\pi t_1)) = 11 + 18\sqrt{6} + 32u_4\,;$$

$$(v)\ k((1-x^2)(c_1 - c_2)) = 1 + \pi^8 + \pi^{13} + \pi^{16} + \pi^{19} + \pi^{21} + \pi^{22}u_5\,;$$

where $u_1 \in \mathbf{Z}_2$, $u_2 \in \mathbf{Z}_2[\sqrt{3}]$, $u_3 \in \mathbf{Z}_2[\sqrt{2}]$, $u_4 \in \mathbf{Z}_2[\sqrt{6}]$, and $u_5 \in \mathcal{O}_L$.

Proof: Recall that by Lemmas 3.2.6 and 3.2.7, we may choose, mod $\pi^{20}\mathcal{O}_{L_0}$,

$$t_2 \equiv (1+\xi\pi^3)(1+\xi^2\pi^4)(1+\xi\pi^5)(1+\omega\pi^6)(1+\xi\pi^7)\prod_{m=8}^{19}(1+d_m\pi^m)$$

and

$$t_1 \equiv (1+\xi\pi)\prod_{m=2}^{19}(1+c_m\pi^m)\,.$$

where the elements ξ, ω, d_m, c_m $(m = 2, \ldots 19)$ lie in $\mathcal{O}_{\mathbf{Q}_{2,nr}}$, and $\xi^3 = 1$. The rationale behind choosing these liftings to have this form is so that we may compute the elements $\sigma(t_2)$, etc. by successively applying σ to each term in the product.

We also make use of the following simple observation. Let F_1/F_2 be a quadratic Galois extension of local fields having Galois group $\{1, s\}$, and let $\mathcal{P}$ denote the maximal ideal of $\mathcal{O}_{F_1}$. Then for $x \in \mathcal{P}^n$, we have that

$$\begin{aligned} N_{F_1/F_2}(1+x) &= (1+s)(1+x) \\ &= 1 + (x + s(x)) + xs(x) = 1 + Tr_{F_1/F_2}(x) + N_{F_1/F_2}(x)\,. \end{aligned}$$

This observation is actually a special case of a more general one found in [29, p.83], where a similar relation is shown to hold modulo $Tr(\mathcal{P}^{2n})$ in the case

when the extension is totally ramified and cyclic of prime order. We will make use of this observation when taking norms of elements in quadratic steps.

Throughout this proof, we will omit many of the details regarding the computations. Most of these computations were done both by hand and using the software package Maple.

(i) We begin the computation of $\sigma(t_2)$ by examining first the $(1+\xi\pi^3)$ term. We first compute that

$$\begin{aligned}(1+x+x^2+x^3)(1+\xi\pi^3) &= N_{L/K_3}(1+\xi\pi^3)\\ &\equiv 1+\pi_3^3+\xi\pi_3^4+\xi^2\pi_3^5+\xi^2\pi_3^6+\xi\pi_3^7 \quad mod\ \pi_3^8\mathcal{O}_{K_3}\,.\end{aligned}$$

Since $\pi_3 = 1+\sqrt{3}$ and $(1+y)(\pi_3^m) = N_{K_3/\mathbb{Q}_2}(\pi_3^m) = (-2)^m$, we may make use of the above observation to conclude that, modulo $32\mathcal{O}_{\mathbb{Q}_{2,nr}}$,

$$\begin{aligned}\sigma(1+\xi\pi^3) &\equiv (1+y)(1+\pi_3^3+\xi\pi_3^4+\xi^2\pi_3^5+\xi^2\pi_3^6+\xi\pi_3^7)\\ &\equiv 1+Tr(\pi_3^3)+\xi Tr(\pi_3^4)+\xi^2 Tr(\pi_3^5)+\xi^2 Tr(\pi_3^6)+\xi Tr(\pi_3^7)\\ &\qquad +N(\pi_3^3+\xi\pi_3^4+\xi^2\pi_3^5+\xi^2\pi_3^6+\xi\pi_3^7)\\ &\equiv 1+20+\xi(24)+\xi^2(24)+\xi(16)\\ &\qquad +(-8)N(1+\xi\pi_3+\xi^2\pi_3^2+\xi^2\pi_3^3+\xi\pi_3^4)\\ &\equiv 5+16\xi\,.\end{aligned}$$

Similar computations show that

$$\sigma(1+\xi^2\pi^4) \equiv 1+16\xi\,;$$

$$\sigma(1+\xi\pi^5) \equiv 1+16\xi^2+8\xi^2\,;$$

$$\sigma(1+\omega\pi^6) \equiv 1+8(\omega^2+\omega)+16\omega = 1+8\xi^2+16u\,;$$

$$\sigma(1+\xi\pi^7) \equiv 9+16\xi\,.$$

Here we have used the fact that $\omega^2+\omega = \xi^2+2u$. Multiplying these out, we compute the product to be

$$(5+16\xi)\,(1+16\xi)\,(1+16\xi^2+8\xi^2)\,(1+8\xi^2+16u)\,(9+16\xi) = 13+16z$$

for some z. Also, for $m = 8, \ldots, 19$

$$\sigma(1 + d_m \pi^m) \equiv 1 + 16 z_m \,,$$

where in fact, $z_m \equiv 0$ for $m = 9, 16, 17, 18, 19$, so that

$$\sigma(t_2) \equiv (13 + 16z) \prod_{m=8}^{19} (1 + 16 d_m) \equiv 13 + 16z' \,.$$

Since $(F_0/1)(\sigma(t_2)) = \sigma((F_0/1)(t_2)) = \sigma(x(\pi)/\pi) = 1$, we see that $\sigma(t_2)$ lies in $Ker(F_0/1) \cap \mathbf{Q}_{2,nr} = L^* \cap \mathbf{Q}_{2,nr} = \mathbf{Q}_2^*$. In particular, the coefficient z' in the above expression is either 0 or 1. If $z' = 1$, we adjust t_2 by multiplying by the factor $(1 + \pi^8)$, so that since $\sigma(1 + \pi^8) \equiv 1 + 16$, we obtain

$$\sigma(t_2) = 13 + 32 u_1 \,,$$

where $u_1 \in \mathbf{Z}_2$, as required.

(ii) Keeping the above notation, along with the possible adjustment of t_2 just described, we now compute $\tau(t_2)$. By a process similar to that used above, we may compute that, mod $32\mathbf{Z}_2[\sqrt{3}]$,

$$\begin{aligned} \tau(1 + \xi\pi^3) &\equiv (1 - y)(1 + \pi_3^3 + \xi\pi_3^4 + \xi^2\pi_3^5 + \xi^2\pi_3^6 + \xi\pi_3^7) \\ &\equiv 9 + 4\sqrt{3} + 8\xi^2\sqrt{3} + 16\xi^2\sqrt{3} \,, \end{aligned}$$

and similarly that

$$\tau(1 + \xi^2\pi^4) \equiv 17 + 24\sqrt{3} \,;$$

$$\tau(1 + \xi\pi^5) \equiv 1 \,;$$

$$\tau(1 + \omega\pi^6) \equiv 1 + 8\xi^2\sqrt{3} + 16z\sqrt{3} \,;$$

$$\tau(1 + \xi\pi^7) \equiv 1 + 8\sqrt{3} \,.$$

Multiplying out, we obtain

$$\begin{aligned} &(9 + 4\sqrt{3} + 8\xi^2\sqrt{3} + 16\xi^2\sqrt{3})\,(17 + 24\sqrt{3})\,(1 + 8\xi^2\sqrt{3} + 16z\sqrt{3})\,(1 + 8\sqrt{3}) \\ &\qquad \equiv 25 + 4\sqrt{3} + 16z'\sqrt{3} \,. \end{aligned}$$

Again for the higher terms (i.e. for $m \geq 8$) in the product for t_2, we have that

$$\tau(1 + d_m \pi^m) \equiv 1 + 16 z_m \sqrt{3},$$

so that, taking the entire product we find that

$$\tau(t_2) \equiv 25 + 4\sqrt{3} + 16 z'' \sqrt{3}.$$

As in the previous case, the coefficient z'' in this expression is either 0 or 1. If $z'' = 1$ we adjust t_2 by a factor $(1 + \pi^{10})$, which allows us to ensure the existence of a $16\sqrt{3}$ term.

(iii) In this case we are dealing with the element t_1, and must compute we now compute $\lambda(\pi t_1)$. By a process similar to that used above, we may compute that, mod $32\mathbb{Z}_2[\sqrt{2}]$,

$$\begin{aligned} \lambda(1 + \xi\pi) &\equiv (1 - x)(1 + \pi_2 + \xi^2 \pi_2^3 + \xi^2 \pi_2^7) \\ &\equiv 13 + 2\sqrt{2} + 4\xi^2\sqrt{2} + 8\xi^2\sqrt{2} + 16\xi\sqrt{2}, \end{aligned}$$

and similarly that

$$\lambda(1 + c_2\pi^2) \equiv 1 + 16\xi + 4\xi^2\sqrt{2} + 8z_1\sqrt{2} + 16z_2\sqrt{2};$$

$$\lambda(1 + \xi\pi^3) \equiv 1 + 16\xi + 4\xi\sqrt{2} + 16\sqrt{2};$$

$$\lambda(1 + c_4\pi^4) \equiv 1 + 8c_4\sqrt{2} + 16z'\sqrt{2};$$

$$\lambda(1 + \xi\pi^5) \equiv 1 + 16\xi + 4\xi^2\sqrt{2} + 8\xi^2\sqrt{2}.$$

Multiplying these terms out, we obtain

$$1 + 2\sqrt{2} + 4 + 4\sqrt{2} + 8 + 16 + 8z_1'\sqrt{2} + 16z_2'\sqrt{2} \equiv 29 + 6\sqrt{2} + 8z_1'\sqrt{2} + 16z_2'\sqrt{2}.$$

The higher terms (i.e., for $m \geq 6$) in the product for t_1 contribute

$$\lambda(1 + c_m\pi^m) \equiv 1 + 8z_m\sqrt{2} + 16z_m'\sqrt{2},$$

and so, taking the entire product we find that

$$\lambda(t_1) \equiv 29 + 6\sqrt{2} + 8z_1''\sqrt{2} + 16z_2''\sqrt{2}\,.$$

Similarly, we compute that $\lambda(\pi) \equiv 1 + 16\sqrt{2}$. Therefore

$$\lambda(\pi t_1) \equiv 29 + 6\sqrt{2} + 8w_1\sqrt{2} + 16w_2\sqrt{2}\,.$$

As before the unknown coefficients w_1 and w_2 are either 0 or 1. Since $\lambda(1 + \pi^{11}) \equiv 1 + 8\sqrt{2}$ and $\lambda(1 + \pi^{12}) \equiv 1 + 16\sqrt{2}$, we may adjust t_1 by either or both of these factors as necessary, to determine that

$$\lambda(\pi t_1) \equiv 29 + 6\sqrt{2} \quad mod\ 32\mathbf{Z}_2[\sqrt{2}]\,,$$

which is what we wished to show.

(iv) Again we retain the above notation, along with the possible adjustments of t_1 and t_2 described in the previous parts of the proof. We now wish to evaluate $\rho(t_2/(\pi t_1))$ mod $32\mathbf{Z}_2[\sqrt{6}]$ using methods similar to those above. Note first that in the fraction t_2/t_1, the terms $(1 + \xi\pi^3)$ and $(1 + \xi\pi^5)$ cancel. So we may ignore these. To be precise, we define s_1 and s_2 by setting, for $i = 1, 2$,

$$s_i = t_i\,(1 + \xi\pi^3)^{-1}\,(1 + \xi\pi^5)^{-1}\,,$$

so that $\rho(t_2/t_1) = \rho(s_2/s_1)$.

We begin by computing $\rho(s_2)$. As above we compute that

$$\rho(1 + \xi^2\pi^4) \equiv 1 + \xi^2\pi_6^7 + \pi_6^9\,;$$

$$\rho(1 + \omega\pi^6) \equiv 1 + \omega^2\pi_6^7 + z_6\pi_6^9\,;$$

$$\rho(1 + \xi\pi^7) \equiv 1 + \xi^2\pi_6^7 + \xi^2\pi_6^9\,.$$

Multiplying these terms out, we obtain

$$\rho((1 + \xi^2\pi^4)\,(1 + \omega^2\pi_6^7 + z_6\pi_6^9)\,(1 + \xi^2\pi_6^7 + \xi^2\pi_6^9)) \equiv 1 + w_1\pi_6^7 + w_2\pi_6^9\,.$$

Again for the higher terms (i.e., for $m \geq 8$) in the product for s_2, we have that

$$\rho(1 + d_m\pi^m) \equiv 1 + z_m\pi_6^7 + z'_m\pi_6^9,$$

so that, taking the entire product we compute that

$$\rho(s_2) \equiv 1 + z\pi_6^7 + z'\pi_6^9.$$

For the other terms, we let $\rho' = (x-1)(1+(xy)+(xy)^2+(xy)^3)$ and compute $\rho'(\pi s_1) = \rho(\pi s_1)^{-1}$. Similar computations to those above show that

$$\rho'(\pi) \equiv 1 + \pi_6^3 + \pi_6^4 + \pi_6^5 + \pi_6^9,$$

and

$$\rho'(s_1) \equiv 1 + \pi_6^3 + w\pi_6^7 + w'\pi_6^9.$$

Multiplying these values together, we find that, adjusting t_1 by either or both of $(1+\pi^9)$ and $(1+\pi^{14})$ as needed,

$$\rho(t_2/t_1) \equiv \rho(s_2)\,\rho'(s_1) \equiv 1 + \pi_6^3.$$

Finally, multiplying by $\rho'(\pi)$ gives

$$\rho(t_2/(\pi t_1)) \equiv 1 + \pi_6^4 + \pi_6^6 + \pi_6^7 + \pi_6^8 \equiv 11 + 18\sqrt{6}.$$

(v) We note that

$$k((1-x^2)(c_1-c_2)) = (x^2-1)(x+y)(\pi t_1)\ (1-x^2)(x-xy)(t_2).$$

Computing piece by piece we find that, modulo $\pi^{22}\mathcal{O}_L$,

$$\begin{aligned}(x^2-1)(x+y)(\pi) \ &\equiv 1 + \pi^8 + \pi^{10} + \pi^{11} + \pi^{12} + \pi^{13} + \pi^{14} + \pi^{15} \\ &\quad + \pi^{16} + \pi^{18} + \pi^{20} + \pi^{21};\end{aligned}$$

$$(x^2-1)(x+y)(t_1) \equiv 1 + \pi^{10} + \pi^{11} + \pi^{12} + \xi\pi^{14} + \xi\pi^{15} + \xi\pi^{16} + \pi^{18} + \pi^{21};$$

and

$$(1-x^2)(x-xy)(t_2) \equiv 1+\xi^2\pi^{14}+\xi^2\pi^{15}+\xi\pi^{16}+\pi^{18}+\pi^{21}.$$

Since in L we have $2 \sim \pi^8+\pi^{12}+\pi^{16}+\pi^{18}$, we find that upon multiplying these together,

$$k((1-x^2)(c_1-c_2)) = 1+\pi^8+\pi^{13}+\pi^{16}+\pi^{19}+\pi^{21},$$

as claimed. □

With the previous computations in hand, we may now prove the main result of this section.

Theorem 3.3.2 *Let L denote either of our local extensions $L_\pm$. The homomorphism*

$$k : Ker(d) \longrightarrow L^*$$

defined in (3.2.23) is injective.

Proof: Consider

$$k(c_1) = \frac{t_2 x(t_2)}{\pi t_1 y(\pi) y(t_1)}.$$

Since $t_1, t_2 \in U^1_{L_0}$, we see that the L-adic valuation of $k(c_1) \in L^*$ is equal to $v_L(k(c_1)) = -2$ which means that the composite homomorphism

$$v_L \cdot k : Ker(d) \longrightarrow L^* \longrightarrow 2\mathbb{Z}$$

is onto. Hence, it will suffice to prove that

$$k : Ker(d) \cap k^{-1}(\mathcal{O}_L^*) \longrightarrow \mathcal{O}_L^*$$

is injective.

For simplicity, we set

$$Y = Ker(d) \cap k^{-1}(\mathcal{O}_L^*)$$

and as in Section 2.1 we write

$$Y_{\pm} = \{ z \in Y \mid x^2(z) = \pm z \}.$$

We begin by showing that the map

$$k : Y_+ \longrightarrow (\mathcal{O}_L^*)_+ = \mathcal{O}_E^* \tag{3.3.33}$$

is injective. Since Y_+ is a free abelian group, this is equivalent to showing that

$$k : Y_+ \otimes \mathbf{Q} \longrightarrow \mathcal{O}_L^* \otimes \mathbf{Q}$$

is an injective map. But $Y_+ \otimes \mathbf{Q}$ decomposes as

$$Y_+ \otimes \mathbf{Q} = (\sigma Y \otimes \mathbf{Q}) \oplus (\tau Y \otimes \mathbf{Q}) \oplus (\lambda Y \otimes \mathbf{Q}) \oplus (\rho Y \otimes \mathbf{Q}),$$

so that we may obtain injectivity in (3.3.33) by showing injectivity on each summand.

First note that, if we denote by IQ_8 the augmentation ideal of $\mathbf{Z}[Q_8]$, we have

$$Y = IQ_8\langle c_1 \rangle + \mathbf{Z}[Q_8]\langle c_2 \rangle \subset \mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8].$$

Now let σ be as given in (3.3.29). Applying σ to Y, we notice that σIQ_8 is trivial, while $\sigma c_2 = 2\sigma b$. The infinite cyclic group $\mathbf{Z}\langle \sigma c_2 \rangle$ has finite index in Y^{Q_8}, so that because of the quaternion action it will suffice to show that $k(\sigma c_2)$ has infinite order in $\mathcal{O}_L^*$. But

$$k(\sigma c_2) = \sigma k(b)^2 = \sigma(t_2^2),$$

so that, by Lemma 3.3.1 (i),

$$k(\sigma c_2) = (13 + 32z)^2 = 9 + 32z'$$

for some $z, z' \in \mathbf{Z}_2$. Hence $k(\sigma c_2)$ is an element of infinite order in $1+8\mathbf{Z}_2 \subset \mathbf{Z}_2^*$.

We now let τ be as in (3.3.30). Applying τ to Y, we see that

$$\tau c_2 = (1-y)(1+x+x^2+x^3)c_2 = 0\,.$$

Hence τY contains the infinite cyclic group $\mathbf{Z}\langle \tau c_1 \rangle$ as a subgroup of finite index. Since $\tau c_1 = 2\tau b$, we see that

$$k(\tau c_1) = \tau(t_2^2)\,.$$

Using Lemma 3.3.1 (ii), we may compute that

$$k(\tau c_1) = (25 + 20\sqrt{3} + 32z)^2 = 1 + 8\sqrt{3} + 32z'$$

for some $z, z' \in \mathbf{Z}_2[\sqrt{3}]$, which implies that $k(\tau c_1)$ is an element of infinite order in $\mathbf{Z}_2[\sqrt{3}]^*$.

If we now let λ be as in (3.3.31), we find that

$$\lambda c_1 = \lambda c_2 = -2\lambda b'.$$

Hence λY contains the infinite cyclic group $\mathbf{Z}\langle 2\lambda b' \rangle$ as a subgroup of finite index. We notice that

$$k(\lambda b') = \lambda(\pi t_1)\,,$$

so that by Lemma 3.3.1 (iii), we may observe that

$$k(\lambda b') = 29 + 6\sqrt{2} + 32z$$

for some $z \in \mathbf{Z}_2[\sqrt{2}]$, which implies that $k(\lambda b')$ is an element of infinite order in $\mathbf{Z}_2[\sqrt{2}]^*$.

To complete the first part of the proof, we let ρ be as in (3.3.32). Then ρc_1 is trivial, while

$$\rho c_2 = 2\rho(b - b')\,.$$

In particular, ρY contains the infinite cyclic group $\mathbf{Z}\langle 2\rho(b-b')\rangle$ as a subgroup of finite index. Since

$$k(\rho(b-b')) = \rho(t_2/(\pi t_1)),$$

we may use part (iv) of Lemma 3.3.1 to deduce that

$$k(\rho(b-b')) = 11 + 18\sqrt{6} + 32z$$

for some $z \in \mathbf{Z}_2[\sqrt{6}]$. Therefore $k(\rho(b-b'))$ is an element of infinite order in $\mathbf{Z}_2[\sqrt{6}]^*$.

Thus we have shown that (3.3.33) is injective.

We now consider the map

$$k : Y_- \otimes \mathbf{Q} \longrightarrow (\mathcal{O}_L^*)_- \otimes \mathbf{Q}.$$

Since $Y_- \otimes \mathbf{Q}$ is a module over the rational quaternions $\mathbf{H_Q} = \mathbf{Q}[Q_8]/(x^2+1)$, in order to complete the proof of the theorem it suffices to find one element which maps nontrivially.

However, by Lemma 3.3.1 (v), we see that we may write

$$k((1-x^2)(c_1-c_2)) \equiv 1 + \pi^8 + \pi^{13} + \pi^{16}z.$$

Since the only roots of unity in $\mathcal{O}_L^*$ are $\{\pm 1\}$, we see that the image has infinite order in $\mathcal{O}_L^*$. This completes the proof of the theorem. □

Chapter 4

Proof of The Main Theorem

4.1 Beginning of the Proof

In this section, we begin the proof of Theorem 2.5.10. We keep the notation introduced in the previous chapter. In particular, throughout this section $N/\mathbf{Q}$ is a quaternion field whose 2-adic completion is one of the two local fields, $L_{\pm}/\mathbf{Q}_2$, of Section 3.1.

Before beginning the proof, we first recall some ideas regarding relations between cohomology and completions. Let G denote an arbitrary finite group, and let A be a finitely generated $\mathbf{Z}[G]$-module which is $\mathbf{Z}$-torsion free. For such a module we may apply the universal coefficient theorem for homology ([16, p.176]) to obtain, for $n \geq 0$,

$$H_n(G;A) \otimes_{\mathbf{Z}} \mathbf{Z}_2 \cong H_n(G; A \otimes_{\mathbf{Z}} \mathbf{Z}_2).$$

Similarly, we may apply the universal coefficient theorem for cohomology ([16, p.179]) to obtain, for $n \geq 0$,

$$H^n(G;A) \otimes_{\mathbf{Z}} \mathbf{Z}_2 \cong H^n(G; A \otimes_{\mathbf{Z}} \mathbf{Z}_2),$$

so that we obtain isomorphisms in Tate cohomology (even in the cases $n = 0, 1$) of the form

$$\hat{H}^n(G; A) \otimes_{\mathbf{Z}} \mathbf{Z}_2 \cong \hat{H}^n(G; A \otimes_{\mathbf{Z}} \mathbf{Z}_2).$$

As a consequence, we see that in the case where G is a 2-group, each cohomology group $\hat{H}^n(G; A)$ is a finite 2-group. Hence we may identify $\hat{H}^n(G; A)$ and $\hat{H}^n(G; A) \otimes_{\mathbf{Z}} \mathbf{Z}_2$ to obtain isomorphisms, for all $n \in \mathbf{Z}$,

$$\hat{H}^n(G; A) \cong \hat{H}^n(G; A \otimes_{\mathbf{Z}} \mathbf{Z}_2). \tag{4.1.34}$$

In order to simplify our notation in what follows, we write $\overline{A}$ for $A \otimes_{\mathbf{Z}} \mathbf{Z}_2$.

We now apply the above ideas to our case. We write L for either of the extensions $L_{\pm}$ of Section 3.1, and let

$$k : Ker(d) \longrightarrow L^*$$

be the injection of Theorem 3.3.2. Also, we set

$$Y_L = Ker(d) \cap k^{-1}(\mathcal{O}_L).$$

In the commutative diagram (3.2.23) of Section 3.2.1, the middle two terms in each row are cohomologically trivial. For the upper row, this follows from the fact that the middle modules are induced ([29, VIII, §1]), while for the lower row this follows from [29, p.202]. Therefore we have isomorphisms in Tate cohomology of the form

$$k_* : \hat{H}^n(G; Ker(d)) \xrightarrow{\cong} \hat{H}^n(G; L^*),$$

for every subgroup G of Q_8. Moreover, we may take intersections with $k^{-1}(\mathcal{O}_L)$ and $\mathcal{O}_L$, respectively to obtain similar isomorphisms:

$$k_* : \hat{H}^n(G; Y_L) \xrightarrow{\cong} \hat{H}^n(G; \mathcal{O}_L^*).$$

Applying the isomorphism (4.1.34) we obtain

$$k_* : \hat{H}^n(G;\overline{Y}_L) \xrightarrow{\cong} \hat{H}^n(G;\mathcal{O}_L^*). \tag{4.1.35}$$

These are isomorphisms for all subgroups G of Q_8.

By Theorem 3.3.2 we have an injection of $\mathbf{Z}[Q_8]$-modules of the form

$$k : \overline{Y}_L \longrightarrow \mathcal{O}_L^*.$$

Since $\mathcal{O}_L^*$ contains a copy of $\mathbf{Z}_2[Q_8]$ of finite index, the cokernel, M, of this map is finite. More precisely, this cokernel is a finite 2-group, and since we have isomorphisms of the form (4.1.35), the long exact cohomology sequence applied to the short exact sequence

$$0 \longrightarrow \overline{Y}_L \longrightarrow \mathcal{O}_L^* \longrightarrow M \longrightarrow 1,$$

implies that M must be a cohomologically trivial $\mathbf{Z}[Q_8]$-module.

Since we have an isomorphism of abelian groups of the form $L^* \cong \mathcal{O}_L^* \oplus \mathbf{Z}$, we have a corresponding isomorphism of the form

$$Ker(d) \cong Y_L \oplus \mathbf{Z}.$$

We may thus rewrite the commutative diagram (3.2.23) in the form

$$\begin{tikzcd}
Y_L \oplus \mathbf{Z} \arrow[r] \arrow[d, "k"] & \mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8] \arrow[r, "d"] \arrow[d, "j"] & \mathbf{Z}[Q_8] \arrow[r, "\varepsilon"] \arrow[d, "i"] & \mathbf{Z} \arrow[d, "1"] \\
L^* \arrow[r] & L_0^* \arrow[r, "F_0/1"] & L_0^* \arrow[r, "\varepsilon"] & \mathbf{Z}
\end{tikzcd} \tag{4.1.36}$$

We push out the top row of this diagram along k to obtain a second diagram of the form

$$\begin{tikzcd}
Y_L \oplus \mathbf{Z} \arrow[r] \arrow[d, "k"] & \mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8] \arrow[r, "d"] \arrow[d, "j'"] & \mathbf{Z}[Q_8] \arrow[r, "\varepsilon"] \arrow[d, "1"] & \mathbf{Z} \arrow[d, "1"] \\
L^* \arrow[r] & A \arrow[r, "F_0/1"] & \mathbf{Z}[Q_8] \arrow[r, "\varepsilon"] & \mathbf{Z}
\end{tikzcd} \tag{4.1.37}$$

Here the maps k and j' are injective. Also, by definition of pushout (cf. [26, Ex. 2.29]) the module A may be obtained by constructing $L^* \oplus (\mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8])$ and factoring out by the subgroup W defined by

$$W = \{ (k(z), -z) \mid z \in Y_L \oplus \mathbf{Z} \}.$$

The map j' is defined explicitly by

$$j'(z_1, z_2) = (0, z_1, z_2) + W.$$

We now assume that X and X_2 are chosen as in Section 2.4.3. (In Section 4.2.2 we will make an explicit choice for X_2.) Then the local Chinburg invariant of Section 2.4.2 is given by

$$\Omega(L/\mathbf{Q}_2, 1 + X_2) = [A/(1 + X_2)] \in \mathcal{CL}(\mathbf{Z}[Q_8]),$$

since the class $[\mathbf{Z}[Q_8]]$ is trivial. By Kim's formula (cf. Theorem 2.4.9), since 2 is the only wild prime in N, this allows us to compute the global Chinburg invariant as

$$\Omega(N/\mathbf{Q}, 2) = [X] + [A/(1 + X_2)] \in \mathcal{CL}(\mathbf{Z}[Q_8]).$$

Our goal now is to compute the class $[A/(1+X_2)] \in \mathcal{CL}(\mathbf{Z}[Q_8])$. By considering kernels and cokernels in diagram (4.1.37), we obtain a commutative diagram of the form

$$\begin{tikzcd}
Ker(k') \arrow[r] \arrow[d, "\cong"] & Y_L \oplus \mathbf{Z} \arrow[r, "k'"] \arrow[d] & L^*/(1+X_2) \arrow[r, "\varepsilon"] \arrow[d] & Coker(k') \arrow[d, "\cong"] \\
Ker(j'') \arrow[r] & \mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8] \arrow[r, "j''"] & A/(1+X_2) \arrow[r, "\varepsilon"] & Coker(j'')
\end{tikzcd} \tag{4.1.38}$$

where the two middle vertical maps are injections. The bottom row of this diagram gives us an equation in $\mathcal{CL}(\mathbf{Z}[Q_8])$,

$$\begin{aligned}
[A/(1+X_2)] &= [Coker(j'')] + [\mathbf{Z}[Q_8] \oplus \mathbf{Z}[Q_8]] - [Ker(j'')] \\
&= [Coker(j'')] - [Ker(j'')] = [Coker(k')] - [Ker(k')],
\end{aligned}$$

since the maps on the ends are isomorphisms.

Furthermore, if we choose X_2 to satisfy $X_2 \subset 2^4 O_L$, then by the computations of Section 4.3, the composite homomorphism

$$1 + X_2 \longrightarrow L^* \longrightarrow L^*/(k(Y_L \otimes_{\mathbf{Z}} \mathbf{Z}_2) \oplus \mathbf{Z}) \cong M$$

is trivial. Therefore we have that

$$\begin{aligned}
Coker(k') &\cong (L^*/(1+X_2))/(k'(Y_L \oplus \mathbf{Z})) \\
&\cong (L^*/(1+X_2))/(k((Y_L \otimes \mathbf{Z}_2) \oplus \mathbf{Z})) \\
&\cong L^*/(k((Y_L \otimes \mathbf{Z}_2) \oplus \mathbf{Z})) \cong M.
\end{aligned}$$

The above results combine to yield the following relation.

$$\Omega(N/\mathbf{Q}, 2) = [X] + [M] - [Ker(k')] \in \mathcal{CL}(\mathbf{Z}[Q_8]). \tag{4.1.39}$$

The proof therefore follows from the equation (4.1.39) and the following three propositions. These propositions will be proven in Sections 4.2–4.4.

Proposition 4.1.1 *Let $N/\mathbf{Q}$ be a quaternion field such that the completion at the prime 2 is either L_+ or L_-. Let $W_{N/\mathbf{Q}}$ be the Artin root number class of Section 2.3.3. Then in $C\mathcal{L}(\mathbf{Z}[Q_8])$,*

$$[X] = -W_{N/\mathbf{Q}} \qquad if\ \alpha = \alpha_+ ,$$

and

$$[X] = W_{N/\mathbf{Q}} \qquad if\ \alpha = \alpha_- . \qquad \square$$

Proposition 4.1.2 *Let $N/\mathbf{Q}$ be a quaternion field such that the completion at the prime 2 is either L_+ or L_- and let M be the cokernel of the map k as defined above. Then in $C\mathcal{L}(\mathbf{Z}[Q_8])$,*

$$[M] = 1 . \qquad \square$$

Proposition 4.1.3 *Let $N/\mathbf{Q}$ be a quaternion field such that the completion at the prime 2 is either L_+ or L_-. Then in $C\mathcal{L}(\mathbf{Z}[Q_8])$,*

$$[Ker(k')] = -1 \qquad if\ \alpha = \alpha_+ ,$$

and

$$[Ker(k')] = 1 \qquad if\ \alpha = \alpha_- . \qquad \square$$

4.2 Proof of Proposition 4.1.1

The purpose of this section is to determine the class in $C\mathcal{L}(\mathbf{Z}[Q_8])$ represented by $[X]$. In particular, if $W_{N/\mathbf{Q}}$ is the Artin root number class of Section 2.3.3,

then we will prove that in $\mathcal{CL}(\mathbf{Z}[Q_8])$,

$$[X] = -W_{N/\mathbf{Q}} \qquad if\ \alpha = \alpha_+ ,$$

and

$$[X] = W_{N/\mathbf{Q}} \qquad if\ \alpha = \alpha_- .$$

The proof will be given in Section 4.2.3. We first compute some values that we will need.

4.2.1 The Local Root Number

In this section we compute the value of the local root number at 2 for the 2-dimensional irreducible representation ν of Q_8. More precisely, we prove:

Lemma 4.2.1 *If ν denotes the 2-dimensional, irreducible complex representation of $G(N/\mathbf{Q}) \cong Q_8$, then the local Artin root number of ν, $W_{\mathbf{Q}_2}(\nu)$, satisfies*

$$W_{\mathbf{Q}_2}(\nu) = 1 .$$

To simplify notation a bit, throughout this section we denote the quadratic subfield $K_2 = \mathbf{Q}_2(\sqrt{2})$ by K.

Following the calculation in [7, §3] we set $Q = \sqrt{2}\mathcal{O}_K$ and $\epsilon = 1 + \sqrt{2}$, so that we have an isomorphism

$$\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \longrightarrow \left(\mathcal{O}_K/Q^5\right)^*$$

$$(b_1, b_2, b_3) \longrightarrow \epsilon^{b_1}(-1)^{b_2}5^{b_3}.$$

By local class field theory we know that

$$\mathbf{Q}_2(\sqrt{2})^*/N(L^*) \cong \mathbf{Z}/4\mathbf{Z}$$

where we denote a generator of the left hand side by z. A straightforward computation shows that

Lemma 4.2.2 *Let $L = L_{\pm}$. Then*

$$U_K^5 \subseteq N(U_L^1). \qquad \square$$

We thus have a map

$$U_K^1 \longrightarrow \frac{U_K^1}{N(U_L^1)}$$

and this map sends $U_K^5 \mapsto 0$ by Lemma 4.2.2. Hence we have a surjection

$$\eta : \frac{U_K^1}{U_K^5} \longrightarrow \frac{U_K^1}{N(U_L^1)}.$$

Let $K' = Ker(\eta)$. Then we have isomorphisms

$$\frac{\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}}{K'} \cong \frac{(U_K^1/U_K^5)}{K'} \cong \frac{U_K^1}{N(U_L^1)} \cong \frac{K^*}{N(L^*)} \cong \mathbf{Z}/4\mathbf{Z}.$$

We set $B = (U_K^1/U_K^5)/K'$ and let $\varepsilon = 1 + \sqrt{2} \in B$. Recalling that $B \cong U_K^1/N(U_L^1)$, since elements of $N(U_L^1)$ are trivial in B we have that (in B)

$$\varepsilon^2 = 3 + 2\sqrt{2} = 3 + 6\sqrt{2} = 3(1 + 2\sqrt{2}) = 3N(1 + \pi_L) = 3,$$

while

$$-1 = 15 = N(1 + \pi_L + \pi_L^2) = 1.$$

In particular this implies that $\varepsilon^2 = 3 = 3(-1) = 5$. Therefore the 16 elements of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ reduce in B to the four elements

$$\varepsilon, \quad \varepsilon^2 = 5, \quad \varepsilon^3 = 5\varepsilon, \quad \varepsilon^4 = 1$$

and so we may take $\varepsilon = 1 + \sqrt{2}$ as a generator of $B \cong \mathbf{Z}/4\mathbf{Z}$.

We let χ be the following character of $Gal(L/K)$ of order 4. We write μ_4 for the complex 4th roots of unity and let

$$\chi : \frac{U_K^1}{N(U_L^1)} \longrightarrow \mu_4$$

be the character which sends $\varepsilon \mapsto i$. Hence

$$\begin{aligned} \chi(\varepsilon) &= i \\ \chi(\varepsilon^2) &= \chi(5) = -1 \\ \chi(-1) &= 1 \ (= \chi(1)) \end{aligned}$$

It will be shown in Lemma 4.2.3 that $W_K(\chi) = 1$.

In order to compute the local root number, we note that $Gal(L/K) \cong \mathbf{Z}/4$, and that $\nu = Ind_{\mathbf{Z}/4}^{\mathbf{Q}_2}(\chi)$. Also, we have $Ind_{\mathbf{Z}/4}^{\mathbf{Q}_2}(\chi - 1) = \nu - Ind_{\mathbf{Z}/4}^{\mathbf{Q}_2}(1)$, so that in particular, by properties similar to those of Proposition 2.3.2,

$$W_{\mathbf{Q}_2}(\nu) = W_{\mathbf{Q}_2}(Ind_{\mathbf{Z}/4}^{\mathbf{Q}_2}(\chi - 1))\, W_{\mathbf{Q}_2}(Ind_{\mathbf{Z}/4}^{\mathbf{Q}_2}(1)).$$

But

$$W_{\mathbf{Q}_2}(Ind_{\mathbf{Z}/4}^{\mathbf{Q}_2}(\chi - 1)) = W_K(\chi) = 1,$$

so that in fact

$$W_{\mathbf{Q}_2}(\nu) = W_{\mathbf{Q}_2}(Ind_{\mathbf{Z}/4}^{\mathbf{Q}_2}(1)).$$

If we now let φ be the nontrivial character of $Gal(K/\mathbf{Q}_2)$, we see that

$$Ind_{\mathbf{Z}/4}^{\mathbf{Q}_2}(1) = 1 + Inf_{\mathbf{Z}/2}^{\mathbf{Q}_2}(\varphi).$$

In particular this implies that

$$W_{\mathbf{Q}_2}(\nu) = W_{\mathbf{Q}_2}(Inf_{\mathbf{Z}/2}^{\mathbf{Q}_2}(\varphi)) = W_{\mathbf{Q}_2}(\varphi),$$

again appealing to the local version of Proposition 2.3.2.

This last value may be computed quite easily, using the methods developed in [30, pp.263-6] for quadratic characters. Following the notation introduced there, we define a map (cf. also [30, p.61])

$$\ell(2) : \Omega_{\mathbf{Q}_2} \longrightarrow \{\pm 1\}$$

by setting $\ell(2)(\omega) = \omega(\sqrt{2})/\sqrt{2}$. Now we are finished, since (cf. [30, pp.266])

$$W_{\mathbf{Q}_2}(\varphi) = W_{\mathbf{Q}_2}(\ell(2)) = 1 . \qquad \square$$

It remains only to derive the value of $W_K(\chi)$ used above.

Lemma 4.2.3 *With the above notation we have*

$$W_K(\chi) = 1 .$$

Proof: Our argument here is essentially that of [7, Th.3.1].

By definition,

$$W_K(\chi) = \frac{\tau(\overline{\chi})}{\sqrt{Nf(\chi)}} ,$$

where τ denotes the Gauss sum, $f(\chi)$ is the local Artin conductor ideal and N denotes the absolute norm. We write $\psi = \psi_K$ for the additive character of K of Section 2.3.2 and denote by f_χ the conductor of χ (cf. [38, p.19]). The local Artin conductor ideal is then defined to be $f(\chi) = \mathcal{M}_K^{f_\chi} = (\sqrt{2})^{f_\chi}\mathcal{O}_K$. We write $\mathcal{D}$ and $\mathcal{D}^{-1}$ for the different and inverse different of K.

Recall from Section 2.3.2 that the Gauss sum $\tau(\overline{\chi})$ is defined as

$$\tau(\overline{\chi}) = \sum_{u \in U_K^1/U_K^{f_\chi}} \overline{\chi}(\frac{u}{c})\psi(\frac{u}{c})$$

where c is such that the ideal $c\mathcal{O}_K = (\sqrt{2})^{f_\chi}\mathcal{D}$.

To compute f_χ then, we simply note that $\mathbf{Z}/4\mathbf{Z} \cong (\mathbf{Z}/5\mathbf{Z})^*$ and since 5 is prime we have that $f_\chi = 5$. Hence the conductor ideal is $f(\chi) = (\sqrt{2})^5\mathcal{O}_K$ and we note in passing that

$$\sqrt{Nf(\chi)} = (\sqrt{2})^5 .$$

We now compute $\mathcal{D}^{-1}$. First note that for $a+b\sqrt{2} \in K$, $Tr_{K/\mathbf{Q}_2}(a+b\sqrt{2}) = 2a$. If m is even, then

$$Tr_{K/\mathbf{Q}_2} : (\sqrt{2})^{-m} \longmapsto 2(\sqrt{2})^{-m} = \frac{2}{(\sqrt{2})^m}$$

while for m odd, $Tr_{K/\mathbf{Q}_2}((\sqrt{2})^{-m}) = 0$. Let $x = a+b\sqrt{2} \in \mathcal{O}_K$ with $a, b \in \mathbf{Z}_2$. Taking $m = 3$ in the above discussion, we compute that

$$Tr(\frac{x}{(\sqrt{2})^3}) = Tr(\frac{a\sqrt{2}}{4} + \frac{b}{2}) = b \in \mathbf{Z}_2 \ .$$

This implies that $\psi\left((\sqrt{2})^{-3}\mathcal{O}_K\right) = 1$. On the other hand,

$$Tr(\frac{x}{(\sqrt{2})^4}) = Tr(\frac{a}{4} + \frac{b\sqrt{2}}{4}) = \frac{a}{2} \notin \mathbf{Z}_2$$

whenever $a \notin 2\mathbf{Z}_2$. Hence $\psi((\sqrt{2})^{-4}\mathcal{O}_K) \neq 1$. Thus $\mathcal{D}^{-1} = (\sqrt{2})^{-3}\mathcal{O}_K$, so that

$$\mathcal{D} = (\sqrt{2})^3\mathcal{O}_K \ .$$

Setting $c = 16$, we see therefore that $c\mathcal{O}_K = (\sqrt{2})^{f_\chi}\mathcal{D}$.

We come finally to the computation of the Gauss sum,

$$\tau(\overline{\chi}) = \sum_{u \in U_K^1/U_K^5} \overline{\chi}(\frac{u}{c})\psi(\frac{u}{c}) \ .$$

As before a set of representative elements of U_K^1/U_K^5 is given by

$$\left\{\varepsilon^j(-1)^k 5^\ell, \text{ where } j = 0,1,2,3;\ k,\ell = 0,1\right\} \ .$$

We have already computed the images of such u's under χ, namely that

$$\chi(\varepsilon) = i; \qquad \chi(-1) = 1; \qquad \text{and } \chi(5) = -1 \ ;$$

and so we consider the images under ψ. Since ψ is exponential in form, we have that

$$\psi\left(\frac{\varepsilon^j(-1)^k 5^\ell}{2^4}\right) = \psi\left(\frac{\varepsilon^j}{2^4}\right)^{(-1)^k 5^\ell}$$

and so in fact we need only compute four images. Let $\xi_8 = (1+i)/\sqrt{2}$, a primitive complex 8th root of unity. We compute first

$$\begin{aligned}\psi(1/2^4) &= \exp\left(2\pi i\ Tr_{K/\mathbf{Q}_2}(1/2^4)\right)\\ &= \exp(2\pi i\,(1/8))\\ &= \exp(\pi i/4) = \xi_8\ .\end{aligned}$$

Recall that $\varepsilon = 1+\sqrt{2}$, so that $Tr_{K/\mathbf{Q}_2}(\varepsilon/2^4) = 1/8$. Also, since $\varepsilon^2 = 3+2\sqrt{2}$ and $\varepsilon^3 = 7+5\sqrt{2}$, we see that $Tr_{K/\mathbf{Q}_2}(\varepsilon^2/2^4) = 3/8$ and $Tr_{K/\mathbf{Q}_2}(\varepsilon^3/2^4) = 7/8$. This implies that we have

$$\psi\left(\frac{\varepsilon}{2^4}\right) = \xi_8; \qquad \psi\left(\frac{\varepsilon^2}{2^4}\right) = \xi_8^3; \qquad \text{and} \quad \psi\left(\frac{\varepsilon^3}{2^4}\right) = \xi_8^7.$$

Noticing that $\chi(2)$ is a 4th root of unity we see that $\chi(2^4) = \chi(2)^4 = 1$.

Therefore we can compute

$$\begin{aligned}\tau(\overline{\chi}) &= \textstyle\sum_{u\in U_K^1/U_K^3} \overline{\chi}(u)\psi(\frac{u}{c})\\ &= \overline{\chi}(1)\psi(1/16) + \overline{\chi}(\varepsilon)\psi(\varepsilon/16) + \overline{\chi}(\varepsilon^2)\psi(\varepsilon^2/16) + \overline{\chi}(\varepsilon^3)\psi(\varepsilon^3/16)\\ &\quad +\overline{\chi}(-1)\psi(1/16)^{-1} + \overline{\chi}(-\varepsilon)\psi(\varepsilon/16)^{-1} + \overline{\chi}(-\varepsilon^2)\psi(\varepsilon^2/16)^{-1}\\ &\quad +\overline{\chi}(-\varepsilon^3)\psi(\varepsilon^3/16)^{-1} + \overline{\chi}(5)\psi(1/16)^5 + \overline{\chi}(5\varepsilon)\psi(\varepsilon/16)^5\\ &\quad +\overline{\chi}(5\varepsilon^2)\psi(\varepsilon^2/16)^5 + \overline{\chi}(5\varepsilon^3)\psi(\varepsilon^3/16)^5 + \overline{\chi}(-5)\psi(1/16)^{-5}\\ &\quad +\overline{\chi}(-5\varepsilon)\psi(\varepsilon/16)^{-5} + \overline{\chi}(-5\varepsilon^2)\psi(\varepsilon^2/16)^{-5} + \overline{\chi}(-5\varepsilon^3)\psi(\varepsilon^3/16)^{-5}\\ &= \xi_8 + (-i)\xi_8 + (-1)\xi_8^3 + i\xi_8^7 + \xi_8^7 + (-i)\xi_8^7 + (-1)\xi_8^5 + i\xi_8\\ &\quad +(-1)\xi_8^5 + i\xi_8^5 + \xi_8^7 + (-i)\xi_8^3 + (-1)\xi_8^3 + i\xi_8^3 + \xi_8 + (-i)\xi_8^5\\ &= \xi_8 + \xi_8^7 + \xi_8^7 + \xi_8 + \xi_8^7 + \xi_8^5 + \xi_8 + \xi_8^3\\ &\quad +\xi_8 + \xi_8^7 + \xi_8^7 + \xi_8 + \xi_8^7 + \xi_8^5 + \xi_8 + \xi_8^3\\ &= 4\xi_8 + 4\xi_8^7 + 2(\xi_8 + \xi_8^3 + \xi_8^5 + \xi_8^7)\ ,\end{aligned}$$

since $i = \xi_8^2$, $(-1) = \xi_8^4$ and $(-i) = \xi_8^6$. Now $\xi_8 = (1+i)/\sqrt{2}$ and $\xi_8^7 = (1-i)/\sqrt{2}$, so that $\xi_8+\xi_8^7 = \sqrt{2}$. Similarly, $\xi_8^3 = (-1+i)/\sqrt{2}$ and $\xi_8^5 = (-1-i)/\sqrt{2}$, so that $\xi_8^3 + \xi_8^5 = -\sqrt{2}$.

Therefore

$$\tau(\overline{\chi}) = 4\sqrt{2} + 2\left(\sqrt{2} + (-\sqrt{2})\right) = 4\sqrt{2} = (\sqrt{2})^5 ,$$

so that

$$W_K(\chi) = \frac{1}{(\sqrt{2})^5}\left[\sqrt{2}\right]^5 = 1 ,$$

as required. □

4.2.2 Resolvents

In order to facilitate our computations in the next section, we need to recall some facts about manipulating resolvents. For more details, see [12, pp.28-32].

If Λ is any ring which admits a $G(N/\mathbf{Q})$-action, and $u \in \Lambda$, then for any $\chi \in R(Q_8)$, we define the resolvent of χ by the formula

$$(u\,|\,\chi) := det\left(\sum_{g\in G(N/\mathbf{Q})} g(u)\chi(g^{-1})\right) .$$

The $\Omega_{\mathbf{Q}}$-action on the resolvent homomorphism is given as follows. If $\omega \in \Omega_{\mathbf{Q}}$ then

$$\omega(u\,|\,\chi) = det\left(\sum_g \omega(g(u))\omega(\chi(g^{-1}))\right)$$

$$= det\left(\sum_{\omega g} \omega g(u)\,\chi((\omega g)^{-1})\,\chi(\omega g)\,\omega(\chi(g^{-1}))\right) .$$

Now, for χ irreducible and 1-dimensional,

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

and

$$\chi(\omega g) = \chi(\omega)\,\chi(g) ,$$

so that

$$\begin{aligned}\omega(u\,|\,\chi) &= det\left(\textstyle\sum_g g(u)\,\chi(g^{-1})\,\chi(\omega)\right)\\ &= det\,(\chi(\omega))\;det\left(\textstyle\sum_g g(u)\,\chi(g^{-1})\right)\\ &= (\,u\,|\,\chi\,)\,det\,(\chi(\omega))\;.\end{aligned}$$

(In [12, p.30] this formula is shown to be true in general.)

Recall from Section 4.1 that the local module X_2 must be a free $\mathbf{Z}_2[Q_8]$-module on one generator such that $X_2 \subset 2^4\mathcal{O}_L$. We choose X_2 to be the free module generated by the element

$$a_2 = 2^t(1+\sqrt{2}+\sqrt{3}+\sqrt{6}+\alpha) \in 2^4\mathcal{O}_L\,,$$

with $t \geq 0$. We need to verify that this module is in fact free.

To fix notation, recall first that the irreducible Q_8-representations are 1, χ_1, χ_2, $\chi_1\chi_2$, and ν, where χ_1 and χ_2 are defined by

$$\chi_1 : \begin{cases} x & \longmapsto -1 \\ y & \longmapsto 1 \end{cases}$$

and

$$\chi_2 : \begin{cases} x & \longmapsto 1 \\ y & \longmapsto -1 \end{cases}\;.$$

The irreducible 2-dimensional complex representation, ν, is given by the action of Q_8 on the quaternions. By complexifying, we have that $\nu : Q_8 \to GL_2(\mathbf{C})$ is defined by

$$\nu(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \nu(x) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$\nu(y) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \nu(xy) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

and $\nu(x^2g) = -\nu(g)$.

Lemma 4.2.4 *Keeping the notation introduced above, the module* $\mathbf{Z}_2[Q_8]\langle a_2\rangle$ *(with* $t=0$*) is a free* $\mathbf{Z}_2[Q_8]$*-submodule of* $\mathcal{O}_L$.

Proof: We follow the approach of [20, p.138]. To each irreducible representation χ of Q_8 we associate the idempotent

$$e_\chi = \frac{dim(\chi)}{8}\sum_{g\in Q_8}\chi(g^{-1})\,g\,.$$

Arguing as in [20] we see that $e_\chi\mathcal{O}_L$ contains a free $e_\chi\mathbf{Z}_2[Q_8]$-module with generator γ_χ. We set γ to be the sum $\gamma=\gamma_1+\gamma_{\chi_1}+\gamma_{\chi_2}+\gamma_{\chi_1\chi_2}+\gamma_\nu$. Then, multiplying by a power of 2 if necessary, γ generates a free $\mathbf{Z}_2[Q_8]$-module of $\mathcal{O}_L$.

The proof now follows by computing the generators γ_χ.

For $\chi=1$ we compute that

$$e_1\mathcal{O}_L=(\frac{1}{8}\sum_{g\in Q_8}g)\mathcal{O}_L=\frac{1}{8}Tr_{L/\mathbf{Q}_2}(\mathcal{O}_L)=\mathbf{Z}_2\,,$$

so that we may take $\gamma_1=1$. Similarly, for $\chi=\chi_1$, we compute that

$$e_{\chi_1}\mathcal{O}_L=(\frac{1}{8}\sum_{g\in Q_8}\chi_1(g^{-1})g))\mathcal{O}_L=\frac{1}{8}\lambda(\mathcal{O}_L)=\mathbf{Z}_2\cdot\sqrt{2}\,,$$

and we may choose $\gamma_{\chi_1}=\sqrt{2}$. Similar computations reveal that we may select $\gamma_{\chi_2}=\sqrt{3}$, $\gamma_{\chi_1\chi_2}=\sqrt{6}$ and $\gamma_\nu=\alpha$, proving the lemma. □

In the next section we will need the values of the resolvent homomorphism $(a_2\,|\,\cdot)$ on irreducible representations of Q_8. We compute these now.

Proposition 4.2.5 *With the notation outlined above, the resolvent homomorphism* $(a_2\,|\,\cdot)$ *is given on irreducible representations as follows:*

$$(a_2\,|\,1)=2^{t+3};$$

$$(a_2\,|\,x)=2^{t+3}\sqrt{2};$$

$$(a_2\,|\,y) = 2^{t+3}\sqrt{3};$$

$$(a_2\,|\,xy) = 2^{t+3}\sqrt{6};$$

$$(a_2\,|\,\nu) = \begin{cases} 2^{t+4} & if\ \alpha = \alpha_+; \\ (-1)\,2^{t+4} & if\ \alpha = \alpha_-. \end{cases}$$

Proof: To simplify the computations, since Q_8 acts trivially on the leading term 2^t, we may assume that $t = 0$. The Q_8-action on the element a_2 is given by the following equations:

$$1(a_2) = 1 + \sqrt{2} + \sqrt{3} + \sqrt{6} + \alpha;$$

$$x(a_2) = 1 - \sqrt{2} + \sqrt{3} - \sqrt{6} + (\sqrt{2} - 1)(\sqrt{3} - \sqrt{2})\alpha;$$

$$x^2(a_2) = 1 + \sqrt{2} + \sqrt{3} + \sqrt{6} - \alpha;$$

$$x^3(a_2) = 1 - \sqrt{2} + \sqrt{3} - \sqrt{6} - (\sqrt{2} - 1)(\sqrt{3} - \sqrt{2})\alpha;$$

$$y(a_2) = 1 + \sqrt{2} - \sqrt{3} - \sqrt{6} + (\sqrt{3} - \sqrt{2})\alpha;$$

$$xy(a_2) = 1 - \sqrt{2} - \sqrt{3} + \sqrt{6} + (\sqrt{2} - 1)\alpha;$$

$$x^2y(a_2) = 1 + \sqrt{2} - \sqrt{3} - \sqrt{6} - (\sqrt{3} - \sqrt{2})\alpha;$$

$$x^3y(a_2) = 1 - \sqrt{2} - \sqrt{3} + \sqrt{6} - (\sqrt{2} - 1)\alpha.$$

Then

$$(a_2\,|\,1) = \sum_{g \in Q_8} g(a_2) = 8,$$

and

$$\begin{aligned} (a_2\,|\,\chi_1) &= \textstyle\sum_{\chi_1(g)=1} g(a_2) - \sum_{\chi_1(g)=-1} g(a_2) \\ &= \{a_2 + x^2(a_2) + y(a_2) + x^2y(a_2)\} \\ &\qquad -\{x(a_2) + x^3(a_2) + xy(a_2) + x^3y(a_2)\} \\ &= \{4 + 4\sqrt{2}\} - \{4 - 4\sqrt{2}\} = 8\sqrt{2}. \end{aligned}$$

Similar computations show that

$$(a_2 \,|\, \chi_2) = 8\sqrt{3} \qquad \textit{and} \qquad (a_2 \,|\, \chi_1\chi_2) = 8\sqrt{6}.$$

Finally, we have that $(a_2 \,|\, \nu) = det(A)$, where the matrix A is given by

$$\begin{pmatrix} (1-x^2)(a_2) + i(x^3-x)(a_2) & (x^2y-y)(a_2) - i(x^3y-xy)(a_2) \\ (y-x^2y)(a_2) - i(x^3y-xy)(a_2) & (1-x^2)(a_2) - i(x^3-x)(a_2) \end{pmatrix}$$

$$= \begin{pmatrix} 2\alpha - 2i(\sqrt{2}-1)(\sqrt{3}-\sqrt{2})\alpha & -2(\sqrt{3}-\sqrt{2})\alpha + 2i(\sqrt{2}-1)\alpha \\ 2(\sqrt{3}-\sqrt{2})\alpha + 2i(\sqrt{2}-1)\alpha & 2\alpha + 2i(\sqrt{2}-1)(\sqrt{3}-\sqrt{2})\alpha \end{pmatrix},$$

so that

$$\begin{aligned} det(A) &= 4\alpha^2 \begin{pmatrix} 1 - i(\sqrt{2}-1)(\sqrt{3}-\sqrt{2}) & -(\sqrt{3}-\sqrt{2}) + i(\sqrt{2}-1) \\ (\sqrt{3}-\sqrt{2}) + i(\sqrt{2}-1) & 1 + i(\sqrt{2}-1)(\sqrt{3}-\sqrt{2}) \end{pmatrix} \\ &= 4\alpha^2[(1 + (\sqrt{2}-1)^2(\sqrt{3}-\sqrt{2})^2) + ((\sqrt{3}-\sqrt{2})^2 - (\sqrt{2}-1)^2)] \\ &= 4\alpha^2[1 + (\sqrt{2}-1)^2][1 + (\sqrt{3}-\sqrt{2})^2]. \end{aligned}$$

However, since

$$\alpha^2 = \pm\frac{\sqrt{6}}{6}(\sqrt{2}+1)(\sqrt{3}+\sqrt{2}),$$

we see immediately that

$$\begin{aligned} &4\alpha^2[1 + (\sqrt{2}-1)^2][1 + (\sqrt{3}-\sqrt{2})^2] \\ &= \pm\frac{4\sqrt{6}}{6}[(\sqrt{2}+1) + (\sqrt{2}-1)]\,[(\sqrt{3}+\sqrt{2}) + (\sqrt{3}-\sqrt{2})^2] \\ &= \pm\frac{4\sqrt{6}}{6}(2\sqrt{2})(2\sqrt{3}) = \pm 16, \end{aligned}$$

as claimed. □

4.2.3 Proof of Proposition 4.1.1

Our approach will make use of the Hom-description of Section 2.2.2, as well as results of A. Fröhlich, J. Martinet, and M.J. Taylor.

We start with some remarks concerning properties of Hom-descriptions which are relevant to our case. We let F be any finite Galois extension of $\mathbf{Q}$ large enough so that $N(\sqrt{-1}) \subset F$. Then Theorem 2.2.1 implies that

$$\mathcal{CL}(\mathbf{Z}[Q_8]) \cong \frac{Hom_{\Omega_\mathbf{Q}}(R(Q_8), J(F))}{Hom_{\Omega_\mathbf{Q}}(R(Q_8), F^*)\ Det(U(\mathbf{Z}[Q_8]))}.$$

Since all characters of Q_8 are integer-valued, clearly $\Omega_\mathbf{Q}$ acts trivially on $R(Q_8)$, so that we have isomorphisms

$$Hom_{\Omega_\mathbf{Q}}(R(Q_8), F^*) \cong Hom(R(Q_8), \mathbf{Q}^*).$$

and

$$Hom_{\Omega_\mathbf{Q}}(R(Q_8), J(F)) \cong Hom\left(R(Q_8), J(F)^{\Omega_\mathbf{Q}}\right)$$

Elements of this last group land in the $\Omega_\mathbf{Q}$-fixed points of the adèle group, so we pause for a moment to describe these points. The p-part of the adèles is

$$F \otimes_\mathbf{Q} \mathbf{Q}_p \cong \prod_{P|p} F_P$$

the product here being over all primes P of F which divide the integral prime p. Now, $\Omega_\mathbf{Q}$ acts on the factors F_P transitively with stabilizer $\Omega_{\mathbf{Q}_p}$, and $\Omega_{\mathbf{Q}_p}$ acts on each F_P componentwise. Hence, in particular,

$$(F \otimes_\mathbf{Q} \mathbf{Q}_p)^{\Omega_\mathbf{Q}} \cong F_P^{\Omega_{\mathbf{Q}_p}} = \mathbf{Q}_p$$

for any choice of P dividing p. This implies that

$$Hom_{\Omega_\mathbf{Q}}(R(Q_8), J(F)) \cong \prod_p' Hom\left(R(Q_8), \mathbf{Q}_p^*\right)$$

where this weak product includes one factor corresponding to the infinite place $p = \infty$.

We now compute the Hom-description for $[X] - W_{N/\mathbf{Q}}$. The locally free module X is defined componentwise by demanding that

$$X \otimes \mathbf{Q} \cong N \cong \mathbf{Q}[Q_8] < a >$$

for an appropriate $a \in \mathcal{O}_N \setminus \{0\}$, and

$$X_2 = X \otimes_{\mathbf{Z}} \mathbf{Z}_2 \cong \mathbf{Z}_2[Q_8] < a_2 >$$

with (cf. Lemma 4.2.4)

$$a_2 = 2^t(1 + \sqrt{2} + \sqrt{3} + \sqrt{6} + \alpha) \in 4\mathcal{O}_L$$

Note that since we cannot assume $a_2 \in N$, we certainly are unable to assume that $a_2 = a$.

The component of X at the odd prime p is

$$X_p = X \otimes_{\mathbf{Z}} \mathbf{Z}_p \cong \mathbf{Z}_p[Q_8] < a_p > \cong \prod_{P|p} \mathcal{O}_{N_P},$$

where $a_p \in \mathcal{O}_{N_P}$ for some P dividing p, and

$$\mathcal{O}_{N_P} = \mathbf{Z}_p\,[G(N_P/\mathbf{Q}_p)] < a_p > .$$

The above implies that we have homomorphisms

$$R(Q_8) \longrightarrow \prod_{P|p} N_P^*$$

$$\chi \longmapsto \frac{(a_p\,|\,\chi)}{(a\,|\,\chi)}$$

and

$$R(Q_8) \longrightarrow N_2^*$$

$$\chi \longmapsto \frac{(a_2 \,|\, \chi)}{(a \,|\, \chi)}.$$

Considering now the characters on Q_8, we see first of all that, since $det(\nu) = 1$, when $\chi = \nu$ each resolvent is a $\Omega_{\mathbf{Q}}$-map, i.e.

$$\omega(u \,|\, \nu) = (u \,|\, \nu).$$

But for the one dimensional characters χ, some care must be taken to preserve quotients, e.g.

$$\frac{(a_p \,|\, \chi)}{(a \,|\, \chi)}$$

so that the factors $det(\chi(\omega))$ cancel. In other words, while such quotients are $\Omega_{\mathbf{Q}}$-equivariant, the individual factors are not.

The Hom-description of X is now given as in Section 2.2 by

$$\chi \longmapsto \begin{cases} \frac{(a_p|\chi)}{(a|\chi)} & p \ finite\,; \\ 1 & p = \infty. \end{cases}$$

Consider now

$$\tau_{N/\mathbf{Q}}(\chi) = \prod_{p \ finite} \tau_p(\chi_p).$$

According to [12, p.119], the $\Omega_{\mathbf{Q}}$-action is given by

$$\omega(\tau_{N/\mathbf{Q}}(\chi)) = \tau_{N/\mathbf{Q}}(\chi)\, det(\chi)(\omega).$$

In addition, in [11] it is shown that for odd p, $(a_p \,|\, \chi)/(\tau_p(\chi_p))$ is unit-valued in $\prod_{P|p} \mathcal{O}^*_{N_P}$, and hence $N_P/\mathbf{Q}_p$ is tame. But then $|\tau_p(\chi_p)|$ is a power of p, and this is unit-valued so that

$$\frac{(a_p \,|\, \chi)}{\tau_{N/\mathbf{Q}}(\chi)} \in Hom_{\Omega_{\mathbf{Q}}}\left(R(Q_8), \prod_{P|p} \mathcal{O}^*_{F_P}\right).$$

But, by [12, Prop. 2.2], we have that

$$Hom_{\Omega_{\mathbf{Q}}}\left(R(Q_8), \prod_{P|p} \mathcal{O}^*_{F_P}\right) = Det\,(\mathbf{Z}_p[Q_8]^*)$$

provided that $p \neq 2$.

Thus at each odd prime p we may divide by

$$\chi \longmapsto \frac{(a_p \,|\, \chi)}{\tau_{N/\mathbb{Q}}(\chi)}$$

to obtain a Hom-representative for $[X]$ of the form

$$\chi \longmapsto \begin{cases} \frac{(a_2|\chi)}{(a|\chi)} & p = 2\,; \\ \frac{\tau(\chi)}{(a|\chi)} & p \neq 2,\ \textit{finite}\,; \\ 1 & p = \infty\,. \end{cases}$$

Now, by our computations in Proposition 4.2.5, the resolvent homomorphism

$$\chi \longmapsto (a_2 \,|\, \chi)$$

is defined on irreducible characters by

$$1 \longmapsto 2^{t+3}$$

$$\chi_1 \longmapsto 2^{t+3}\sqrt{2}$$

$$\chi_2 \longmapsto 2^{t+3}\sqrt{3}$$

$$\chi_1\chi_2 \longmapsto 2^{t+3}\sqrt{6}$$

$$\nu \longmapsto \begin{cases} 2^{t+4} & \textit{for } \alpha = \alpha_+ \\ 2^{t+4}(-1) & \textit{for } \alpha = \alpha_- \end{cases}.$$

In addition, the global function

$$\chi \longmapsto \frac{\tau(\chi)}{(a|\chi)}$$

lies in $Hom_{\Omega_{\mathbb{Q}}}(R(Q_8), F^*)$, and so we may divide by this to obtain an alternate Hom-representative for $[X]$, namely

$$\chi \longmapsto \begin{cases} \frac{(a_2|\chi)}{\tau(\chi)} & p = 2\,; \\ 1 & p \neq 2,\ \textit{finite}\,; \\ \frac{(a|\chi)}{\tau(\chi)} & p = \infty\,. \end{cases}$$

By a result of Fröhlich [10, p.200], the sign of $(a\,|\,\nu)$ at any infinite place of N is equal to the sign of $W_\infty(\nu)$. Moreover, Serre [27] proves that the absolute norm of the conductor of an orthogonal representation is a square, and in [10, p.198], Fröhlich shows that the same is true for a symplectic representation.

Recalling that each local Gauss sum is equal to

$$\tau_p(\nu) = W_p(\nu)\sqrt{N(f(\nu))}\,.$$

The above remarks imply that

$$sign(\tau_p(\nu)) = sign(W_p(\nu))\ for\ all\ p\,.$$

In particular then, $sign(\tau(\nu)) = sign(W_f(\nu))$, and so

$$sign(\tau(\nu)\,W_\infty(\nu)) = sign(W_f(\nu)\,W_\infty(\nu)) = sign(W_{\mathbf{Q}}(\nu))\,.$$

Consider now the function

$$\chi \longmapsto \begin{cases} 1 & p \neq \infty\,; \\ (a\,|\,\chi)\,(\tau(\chi))^{-1}\,W_{\mathbf{Q}}(\chi) & p = \infty\,. \end{cases}$$

By [36, p.9],[5, p.19] and [31, p.336], its sign at ∞ on $\chi = \nu$ is

$$sign\left(\frac{(a\,|\,\nu)}{\tau(\nu)}\,W_{\mathbf{Q}}(\nu)\right) = sign\left(\frac{W_{\mathbf{Q}}(\nu)}{W_\infty(\nu)\tau(\nu)}\right) = 1\,,$$

and since $W_{\mathbf{Q}}(\chi) = 1$ when $dim(\chi) = 1$, we have that the above function lies in

$$Hom_{\Omega_{\mathbf{Q}}}(R(Q_8), F^*)\,.$$

Therefore a Hom-representative for the difference $[X] - W_{N/\mathbf{Q}}$ is

$$\chi \longmapsto \begin{cases} \frac{(a_2|\chi)}{\tau(\chi)} & p = 2\,; \\ 1 & p \neq 2\,. \end{cases}$$

We next define a function $h : R(Q_8) \longrightarrow \mathbf{Z}_2^*$ by the formula

$$h(\chi)\,2^{\beta(\chi)} = \frac{(a_2\,|\,\chi)}{\tau(\chi)}.$$

Also, define $\chi_+ : (\mathbf{Z}/8)^* \longrightarrow \{\pm 1\}$, by

$$\chi_+(\pm 1) = 1 \quad \textit{and} \quad \chi_+(\pm 3) = -1.$$

Then in $\mathcal{CL}(\mathbf{Z}[Q_8]) \cong (\mathbf{Z}/4)^*$, the map h defines a class $H = [h]$ by

$$H = h(\nu)\,\chi_+(h(1 + \chi_1 + \chi_2 + \chi_1\chi_2))$$

Ignoring powers of 2, this is

$$H \equiv \frac{(a_2\,|\,\nu)}{\tau(\nu)}\,\chi_+\left(\frac{(a_2\,|\,1 + \chi_1 + \chi_2 + \chi_1\chi_2)}{\tau(1 + \chi_1 + \chi_2 + \chi_1\chi_2)}\right) \qquad \textit{mod}\ 4.$$

By construction we therefore have

$$H = [X] - W_{N/\mathbf{Q}} \in \mathcal{CL}(\mathbf{Z}[Q_8]) \cong (\mathbf{Z}/4)^*.$$

The remainder of the proof involves computing the value of H mod 4. We accomplish this by computing the various pieces and combining the information obtained. Recall from Proposition 4.2.5 that

$$(a_2\,|\,\nu) = \begin{cases} 1 & \textit{if}\ \alpha = \alpha_+; \\ -1 & \textit{if}\ \alpha = \alpha_-. \end{cases}$$

In either case,

$$W_2(\nu) = 1,$$

and

$$(a_2\,|\,1 + \chi_1 + \chi_2 + \chi_1\chi_2) = 2^{4t+4} \cdot 3.$$

This implies, in particular, that

$$\chi_+(a_2\,|\,1 + \chi_1 + \chi_2 + \chi_1\chi_2)) = -1.$$

Writing $f(\chi)$ for the Artin conductor associated to the character χ, we have

$$W_f(\chi) = \prod_{p \text{ finite}} W_p(\chi_p) = f(\chi)\,\tau(\chi)\,.$$

Also, we have

$$f(1+\chi_1+\chi_2+\chi_1\chi_2) = f\left(Ind_{G(N/E)}^{G(N/\mathbf{Q})}(1)\right) = D_{E/\mathbf{Q}}\,;$$

$$f(2\nu+1+\chi_1+\chi_2+\chi_1\chi_2) = f\left(Ind_{1}^{G(N/\mathbf{Q})}(1)\right) = D_{N/\mathbf{Q}}\,,$$

so that

$$f(\nu)^2 = D_{N/\mathbf{Q}}/D_{E/\mathbf{Q}}\,.$$

By [23, p.531],

$$f(\nu)^2 = \left(\prod_{\substack{p \text{ ramified} \\ \text{in } N/\mathbf{Q}}} p^4\right)\left(\prod_{\substack{p \text{ ramified} \\ \text{in } E/\mathbf{Q}}} p^2\right) D_{E/\mathbf{Q}}^{-1}\,,$$

so that, taking the odd part, we get

$$f(\nu) = \prod_{\substack{2\neq p \text{ ramified} \\ \text{in } N/\mathbf{Q}}} p^2 \equiv 1 \quad mod\ 4\,.$$

Combining the above facts, we see that we may compute H as

$$H \equiv \frac{(a_2\,|\,\chi)\sqrt{f(\nu)}}{\prod_p W_{\mathbf{Q}_p}(\nu_p)}\chi_+\left(\frac{(a_2\,|\,1+\chi_1+\chi_2+\chi_1\chi_2)}{W_f(Ind_{<x^2>}^{Q_8}(1))}\sqrt{D_{E/\mathbf{Q}}}\right) \qquad mod\ 4\,.$$

We complete the proof by computing the values in this expression.

By Lemma 4.2.3, we have that $W_2 = W_{\mathbf{Q}_2}(\nu_2) = 1$. Thus we have

$$W_f(\nu) = \prod_{\substack{2\neq p \text{ ramified} \\ \text{in } N/\mathbf{Q}}} W_{\mathbf{Q}_p}(\nu_p)\,.$$

Now $Ind_{<x^2>}^{Q_8}(1)$ is orthogonal, so that

$$W_{\mathbf{Q}}(Ind_{<x^2>}^{Q_8}(1)) = 1\,.$$

Also,

$$W_\infty(Ind_{<x^2>}^{Q_8}(1)) \in \{\pm 1\},$$

and hence,

$$\chi_+\left(W_{\mathbf{Q}}(Ind_{<x^2>}^{Q_8}(1))\right) = \chi_+(\pm 1) = 1.$$

We write D_0 for the odd part of $\sqrt{D_{E/\mathbf{Q}}}$. Then by [23, p.531] or [20, Lemma 3.1], we see that mod 4,

$$\prod_{\substack{2\neq p \text{ ramified} \\ \text{in } N/\mathbf{Q}}} W_{\mathbf{Q}_p}(\nu_p) \equiv \left(\frac{2}{D_0}\right) \prod_{\substack{2\neq p \text{ ramified} \\ \text{in } N/\mathbf{Q}}} p.$$

Finally, from the definition of the Jacobi symbol, it follows that

$$\left(\frac{2}{D_0}\right) = \chi_+(D_0),$$

and combining all the above information reveals that in $\mathcal{CL}(\mathbf{Z}[Q_8])$,

$$[H] = \begin{cases} -1 & if\ \alpha = \alpha_+; \\ 1 & if\ \alpha = \alpha_-, \end{cases}$$

which proves the Proposition. □

4.3 Proof of Proposition 4.1.2

In this section we focus on the computation of the class $[M]$ of the cokernel of the map k. To be precise, we show that in $\mathcal{CL}(\mathbf{Z}[Q_8])$,

$$[M] = 1.$$

As in Section 2.1 we write

$$M_\pm = \{m \in M \mid x^2(m) = \pm m\}.$$

In order to prove the desired result, we shall build up the modules $M_{\pm}$. We begin by considering M_{-}.

Recall from Section 2.1 that M_{-} is a module over the ring

$$\mathbf{H}_{\mathbf{Z}} = \mathbf{Z}[i,j,k]/(i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j)$$

of integral quaternions. As in [32, pp.149-53] we see that M_{-} is a left $\mathbf{H}_{\mathbf{Z}}$-module on one generator, and moreover, $|M_{-}|$ is at least 4. As in [32, Prop.6.2.1], we have a short exact sequence of the form

$$0 \longrightarrow (1-x^2)\overline{k(Ker(d))} \longrightarrow (1-x^2)L^{*} \longrightarrow M_{-} \longrightarrow 0\,.$$

Moreover, multiplication by $(1-x^2)$ induces an isomorphism of the form

$$L^{*}/E^{*} \xrightarrow{1-x^2} L^{*}_{-}\,,$$

since x^2 acts trivially on E, and it follows that we have an isomorphism of the form

$$M_{-} \cong \frac{L^{*}/E^{*}}{\langle k(c_1), k(c_2)\rangle}\,. \tag{4.3.40}$$

Recall that by Proposition 3.2.8, the images of c_1 and c_2 satisfy

$$k(c_1) = \frac{1}{\pi^2}(1+\pi+\pi^2+u\pi^4)$$

and

$$k(c_2) = 1+\pi^3+\pi^4+v\pi^6\,.$$

Lemma 4.3.1 *Keeping the above notation, there is an isomorphism of abelian groups of the form*

$$M_{-} \cong \mathbf{Z}/2 \oplus \mathbf{Z}/2\,.$$

Proof: Our approach is to use the isomorphism (4.3.40), and consider the image in M_{-} of the filtration U_L^n/U_L^{n+1} for L in terms of unit groups. Each

of these factors has order 2, and we use the images of c_1 and c_2 to determine which levels are trivial in M_-. Throughout the proof we use the notation $\sim$ to indicate equivalence in M_-.

We first note that $\pi_E \sim 1$, so that since $\pi_E = \pi^2 u_E$ for some $u_E \in U_L^7 \setminus U_L^8$, in M_- we have that, by Proposition 3.2.8,

$$k(c_1) \sim 1 + \pi + \pi^2 + u\pi^4 .$$

Similarly,

$$k(c_2) \sim 1 + \pi^3 + \pi^4 + v\pi^6 ,$$

and so, since the left sides are trivial, the filtration levels U_L^1/U_L^2 and U_L^3/U_L^4 are trivial in M_-. Working with $k(c_1)$, we compute that

$$1 \sim k(c_1)^2 \sim (1 + \pi + \pi^2 + u\pi^4)^2 \sim 1 + \pi^2 + \pi^4 + \pi^8 z ,$$

while

$$1 \sim k(c_1)^4 \sim (1 + \pi + \pi^2 + u\pi^4)^4 \sim 1 + \pi^4 + \pi^8 + \pi^{10} z' ,$$

so that the levels U_L^2/U_L^3 and U_L^4/U_L^5 are also trivial. Using the above calculations, we may observe that $k(c_1)^4 k(c_2) \sim 1 + \pi^3 + \pi^6 z$, so that squaring this gives

$$1 \sim (1 + \pi^3 + \pi^6 z)^2 \sim 1 + \pi^6 + \pi^7 z' ,$$

which shows that the level U_L^6/U_L^7 is trivial. Similarly, since $x(\pi^3) = \pi^3(1 + \pi^3 + \pi^4 + \pi^5 + \pi^6 w)$ for some $w \in U_L^1$, and since $a + x(a) \in \pi^4 \mathcal{O}_L$ for $a \in \mathcal{O}_L$, we see that

$$1 \sim (1 + x)(1 + \pi^3 + \pi^6 z) \sim 1 + \pi^7 + w'\pi^8 ,$$

showing that the level U_L^7/U_L^8 is trivial. Continuing in this manner, we may use the Q_8-action to show that the levels U_L^m/U_L^{m+1} are trivial, for $8 \leq m \leq 16$. Recalling that the squaring map defines an isomorphism (cf. [29, V,§3])

$U_L^n/U_L^{n+1} \cong U_L^{n+8}/U_L^{n+9}$ for $n \geq 9$, this shows that all higher levels are trivial. We are left with only the levels $(L^*/E^*)/U_L^1$ and U_L^5/U_L^6.

We now see therefore that the module M_- is generated by the elements π and $1+\pi^5$. Squaring these, we find that $\pi^2 = \pi_E/u_E \sim 1$ and $(1+\pi^5)^2 = 1+\pi^{10}+z\pi^{11}$. Since U_L^{10}/U_L^{11} is trivial in M_-, this implies that both the generators have order at most 2. But $|M_-| \geq 4$, so that these have order exactly 2. Hence we may write M_- in terms of generators and relations as

$$M_- = \langle \pi, 1+\pi^5 \mid \pi^2 = (1+\pi^5)^2 = 1 \rangle,$$

and, therefore, as an abelian group $M_- \cong \mathbf{Z}/2 \oplus \mathbf{Z}/2$, as claimed. □

We now try to obtain a lower bound on the order of M. Before doing so, we need to examine the Q_8-fixed points of M.

Lemma 4.3.2 *With the notation introduced above,*

$$M^{Q_8} \cong \mathbf{Z}/2.$$

Proof: Recall that M was defined via the short exact sequence

$$0 \longrightarrow \overline{k(Ker(d))} \longrightarrow L^* \longrightarrow M \longrightarrow 1,$$

so that taking Q_8-cohomology we obtain the long exact sequence

$$0 \longrightarrow \overline{k(Ker(d))}^{Q_8} \longrightarrow (L^*)^{Q_8} \longrightarrow M^{Q_8} \longrightarrow H^1(Q_8; \overline{k(Ker(d))}) \longrightarrow \cdots.$$

However,

$$H^1(Q_8; \overline{k(Ker(d))}) \cong H^1(Q_8; L^*) = 0,$$

by Hilbert's Theorem 90. Therefore

$$M^{Q_8} \cong \frac{(L^*)^{Q_8}}{\overline{k(Ker(d))}^{Q_8}} = \frac{\mathbf{Q}_2^*}{\langle k(\sigma b), k(\sigma b') \rangle}.$$

By Lemma 3.3.1 (i), we may compute that

$$k(\sigma b) = \sigma(t_2) = 5 + 8u$$

for some $u \in U^2_{\mathbb{Q}_2}$. Now $k(\sigma b') = \sigma(\pi t_1)$, and computing as in the proof of Lemma 3.3.1 (i) and (iii) we deduce that

$$\sigma(\pi t_1) = \sigma(\pi)\,(1+x)(1+\pi_2+\pi_2^2+u\pi_2^3) = (-2)(3+4c) = 2(1+4c'),$$

for some $c, c' \in \mathbb{Z}_2$. The first computation shows that $k(\sigma b)$ generates the image of $U^2_{\mathbb{Q}_2}$ in M^{Q_8}, and the in the second we see that the element $(1+4c')$ lies in this image. In particular, by dividing we see that the image of 2 in M^{Q_8} is trivial. Hence $M^{Q_8} \cong \mathbb{Z}/2$, as required. □

Lemma 4.3.3 *The module M satisfies $|M| \geq 2^8$.*

Proof: This result essentially follows from the methods of [32, p.157]. To fix notation, for $g \in Q_8$ of order 4, we define

$$M^g = M^{\langle g \rangle} = \{\, m \in M \mid g(m) = m \,\}.$$

By [32, Prop.6.2.7] there are two possibilities regarding the three submodules M^x, M^y and M^{xy}. If we denote by V the Klein 4-group, then the two possibilities may be listed by stating that as abelian groups, either

(A) $M^g \cong V$ for $g = x, y, xy$;

or

(B) Two of the M^g are cyclic with $|M^g| \geq 8$ and the third is the sum of the first two.

Suppose first that case (A) holds. Then the intersection of any two of the M^g is M^{Q_8} which has order 2 by Lemma 4.3.2. So each of the M^g contains

two 2-torsion elements which are not in any of the others. In particular we see that in this case, $|Tor(\mathbf{Z}/2, M_+)| \geq 8$. However, Lemma 4.3.1 implies that

$$|Tor(\mathbf{Z}/2, M_+)| = |Tor(\mathbf{Z}/2, M_-)| = |M_-| = 4\,,$$

a contradiction.

Therefore we must be in the situation of case (B). Assume without loss of generality that the modules M^x and M^y are cyclic of orders 2^{r+1} and 2^{s+1} respectively. (In fact it may be shown that these are the cyclic ones, but the argument below doesn't rely on this exact knowledge.)

As in [32, p.154-5], if IV denotes the augmentation ideal of $\mathbf{Z}[V]$, we may prove that

$$IV \cdot M_+ = M^x + M^y$$

and moreover that $|M_+/(IV \cdot M_+)| = 2$. In particular this implies that $|M_+| = 2 \cdot |M^x + M^y|$.

Furthermore, since $M^x \cap M^y \cong \mathbf{Z}/2$ as noted above, we see that there is an isomorphism

$$M^x + M^y \cong \frac{\mathbf{Z}/2^{r+1} \oplus \mathbf{Z}/2^{s+1}}{\langle (2^r, 2^s) \rangle}\,.$$

Taking orders on both sides, we see that

$$|M| = |M_-| \cdot |M_+| = 4 \cdot (2 \cdot (2^{r+1})\,(2^{s+1})/2 \geq 4 \cdot 2^6 = 2^8\,,$$

which is what we wanted to prove. □

Having obtained the above facts, we may now compute the exact order of M and in fact its structure as an abelian group.

Proposition 4.3.4 *With the notation introduced above,*

$$M \cong (\mathbf{Z}/16) \oplus (\mathbf{Z}/16)\ .$$

as an abelian group.

Proof: The proof is mostly computational.

Recall that we have an isomorphism of the form

$$M \cong \frac{L^*}{< k(c_1), k(c_2) >},$$

where c_1 and c_2 are the $\mathbf{Z}[Q_8]$-generators of $Ker(d)$. As in Lemma 4.3.1, our approach for the proof will be to consider the filtration on L^* by unit groups and determine which filtration levels may be generated by $k(c_1)$ and $k(c_2)$, using both the $\mathbf{Z}[Q_8]$-action along with the squaring isomorphism. In particular, we will prove that we can generate an element in U_L^n/U_L^{n+1} for all positive n, with the exception of the values $n = 1, 2, 5, 9, 11, 19$, and 27. Combining this with the group L^*/U_L^1 proves that $|M| \leq 2^8$, and hence by Lemma 4.3.3 that $|M| = 2^8$.

We will then show that M has the structure claimed by examining the elements in the remaining filtration levels.

In order to generate the levels claimed, we first recall that for $m \geq 9$, the squaring map $u \to u^2$ on U_L^m induces an isomorphism

$$U_L^m/U_L^{m+1} \xrightarrow{\cong} U_L^{m+8}/U_L^{m+9}. \tag{4.3.41}$$

To ease notation in what follows, we write u and v for arbitrary elements of $\mathcal{O}_L$, which need not be the same from line to line. We note that for any such $u \in \mathcal{O}_L$, we have that $u + y(u) \in \pi^2\mathcal{O}_L$ and $u + x(u) \in \pi^4\mathcal{O}_L$ To begin we recall from Lemma 3.2.8 that U_L^3/U_L^4 is generated by

$$k(c_2) = 1 + \pi^3 + \pi^4 + \pi^6 u.$$

Also,

$$\begin{aligned}(1+y)(k(c_2)) &= [1 + \pi^3 + \pi^4 + \pi^6 u][1 + \pi^3 + \pi^7 + \pi^6 y(u) + \pi^8 v] \\ &= 1 + 2\pi^3 + \pi^4 + \pi^7 + \pi^8 v \\ &= 1 + \pi^4 + \pi^7 + \pi^8 v\end{aligned}$$

generates U_L^4/U_L^5. For U_L^6/U_L^7, we square $k(c_2)$, to obtain

$$(1+\pi^3+\pi^4+\pi^6u)^2 = 1+\pi^6+\pi^8+\pi^{11}+\pi^{12}u\,.$$

Applying $1+x$ to $k(c_2)$ we see that

$$\begin{aligned}(1+x)(k(c_2)) &= [1+\pi^3+\pi^4+\pi^6u] \\ &\qquad \times[1+\pi^3+\pi^4+\pi^6+\pi^7+\pi^8+\pi^6y(u)+\pi^{10}v] \\ &= 1+2\pi^3+2\pi^4+\pi^6+\pi^7+\pi^8+\pi^{10}v \\ &= 1+\pi^6+\pi^7+\pi^8+\pi^9+\pi^{10}v\,.\end{aligned}$$

Multiplying, we generate an element of the form $1+\pi^7+\pi^9+\pi^{10}v$, which generates the level U_L^7/U_L^8. Squaring our generator for U_L^4/U_L^5 gives

$$(1+\pi^4+\pi^7+\pi^8v)^2 = 1+\pi^8+\pi^{14}v\,, \tag{4.3.42}$$

which generates U_L^7/U_L^8. A similar application of the squaring map to the elements above yields generators of U_L^{12}/U_L^{13}, U_L^{14}/U_L^{15} and U_L^{18}/U_L^{19}.

To obtain a generator for U_L^{10}/U_L^{11}, we notice that

$$(1+x)(1+\pi^7+\pi^9+\pi^{10}v) = 1+\pi^{10}+\pi^{11}+\pi^{12}u\,.$$

Also, Lemma 3.3.1 (v) implies that

$$k((1-x^2)(c_1-c_2)) = 1+\pi^8+\pi^{13}+\pi^{16}u\,,$$

so that by (4.3.42) we may generate an element $1+\pi^{13}+\pi^{16}u$ in U_L^{13}/U_L^{14}. Applying $(1+x)$ to this element yields a generator $1+\pi^{16}+\pi^{17}+\pi^{18}v$ for U_L^{16}/U_L^{17}.

Finding a generator for U_L^{15}/U_L^{16} is a little more complicated. Note first that we may generate an element of the form $1+\pi^6+\pi^7+\pi^9v$ whose square is $1+\pi^{12}+\pi^{15}+\pi^{16}u$. Also, we have an equation in L of the form $\pi_3 = \pi^4+\pi^8+\pi^{12}+\pi^{13}u$. As in the proof of Lemma 3.3.1 we may compute that

$$(1+x)\,(1+x^2)(t_2) = 1+\pi_3^3+\pi_3^4+\pi_3^5+\pi_3^7+\pi_3^8u\,.$$

This is an element of $\langle k(c_1), k(c_2)\rangle$, and by the remark above this equals $1 + \pi^{12} + \pi^{16}v$. Putting this together we generate the required element $1+\pi^{15}+\pi^{16}v$ in U_L^{15}/U_L^{16}.

Hence we may generate an element of the form $1 + \pi^{13} + \pi^{16}u$. Applying $(1+y)$ to this reveals an element of the form $1+\pi^{16}+\pi^{18}u$. Together with the previously generated element in U_L^{16}/U_L^{17} this gives a generator of U_L^{17}/U_L^{18}.

Finally, by an argument similar to that given for U_L^{15}/U_L^{16}, we may generate an element in U_L^{35}/U_L^{36}. Using the squaring map, we may therefore generate all levels U_L^n/U_L^{n+1} except for those corresponding to $n = 1, 2, 5, 9, 11, 19$, and 27.

In particular, as mentioned at the outset, this shows that $|M| = 2^8$.

We now examine the relations among the remaining elements of M. We start by determining the order of π. Recall that in M,

$$1 \sim k(c_1) \sim \frac{1}{\pi^2}(1 + \pi + \pi^2 + u\pi^4),$$

so that $\pi^2 \sim 1 + \pi + \pi^2 + u\pi^4$. Therefore π^2 generates U_L^1/U_L^2. This relation may actually be improved to give that $\pi^2 \sim 1+\pi+\pi^2+u\pi^5$. Squaring, we see that π^4 generates U_L^2/U_L^3 and $\pi^8 \sim 1 + \pi^4 + \pi^8 + \pi^{10}u$. Multiplying by trivial elements generated above shows that, in M, π^8 generates U_L^9/U_L^{10}.

Similarly we may show that $(1+\pi^5)^2$ generates U_L^{11}/U_L^{12}, so that $(1+\pi^5)^4$ generates U_L^{19}/U_L^{20} and $(1+\pi^5)^8$ generates U_L^{27}/U_L^{28}. In particular, in M this implies that both π^{16} and $(1+\pi^5)^{16}$ are trivial.

Therefore we have shown that M is generated by the images of π and $1+\pi^5$. There are no further relations between π and $1+\pi^5$, so that

$$M \cong \langle \pi, 1+\pi^5 \mid \pi^{16} = 1 = (1+\pi^5)^{16} \rangle.$$

Therefore

$$M \cong (\mathbf{Z}/16) \oplus (\mathbf{Z}/16)$$

as an abelian group. □

With this result in hand we may now determine the class $[M]$ in $\mathcal{CL}(\mathbf{Z}[Q_8])$. We first consider the action of Q_8 on $M \cong (\mathbf{Z}/16) \oplus (\mathbf{Z}/16)$. Note that

$$x(\pi) = \pi(1 + \pi^3 + \pi^4 + \pi^5 + \pi^6 v)\,.$$

Since $k(c_2) = 1 + \pi^3 + \pi^4 + \pi^6 u$, we see that in M, $x(\pi) = \pi(1 + \pi^5)$.

Now $\langle y \rangle \cong \mathbf{Z}/4$ and therefore $\mathcal{CL}(\mathbf{Z}[\langle y \rangle])$ is trivial. The above action of x shows in particular that $M = Ind_{\langle y \rangle}^{Q_8}(\mathbf{Z}/16)$. Therefore in $\mathcal{CL}(\mathbf{Z}[Q_8])$,

$$[M] = Ind_{\langle y \rangle}^{Q_8}([\mathbf{Z}/16]) = 0\,,$$

as required. □

4.4 Proof of Proposition 4.1.3

The purpose of this section is to determine the class corresponding to $Ker(k')$. To be precise, we shall show that, in $\mathcal{CL}[Q_8]$,

$$[Ker(k')] = -1 \qquad if\ \alpha = \alpha_+\,,$$

and

$$[Ker(k')] = 1 \qquad if\ \alpha = \alpha_-\,.$$

Following the discussion of [32, p.169-73], we see that for $[Ker(k')]$ there is a Hom-representative of the form

$$g \in Hom_{\Omega_{Q_2}}(R(Q_8), \mathbf{Z}_2^*)$$

which satisfies

$$2^e\, g(T) = \frac{(\,a_2\,|\,T\,)}{(\,log_2(k(x_0))\,|\,T\,)}\,. \tag{4.4.43}$$

Here ε is a positive integer, T denotes an element of $R(Q_8)$, and

$$a_2 = 2^t(1+\sqrt{2}+\sqrt{3}+\sqrt{6}+\alpha)$$

is as in Section 4.2.2. In addition, the element x_0 is defined to be

$$x_0 = 2^s(\,\sigma(c_2)+\tau(c_1)+\lambda(c_1)+\rho(c_2)+(1-x^2)(c_1-c_2)\,)\,.$$

From a result of Taylor ([36, Prop.2.21], it follows that the class

$$[g] \in \mathcal{CL}(\mathbf{Z}[Q_8]) \cong D(\mathbf{Z}[Q_8]) \cong (\mathbf{Z}/4)^*$$

can be determined using the formula

$$[g] \equiv g(\nu)\,(-1)^{(1/4)log_2(g(1+\chi_1+\chi_2+\chi_1\chi_2))} \quad (mod\ 4)\,. \tag{4.4.44}$$

Moreover, since for $w \in \mathbf{Z}_2$,

$$(-1)^{(1/4)log_2(1+4w)} = (-1)^{w-w^2} = (-1)^w\,,$$

it is clear that we need only compute the values $g(1)$, $g(\chi_1)$, $g(\chi_2)$ and $g(\chi_1\chi_2)$ modulo 8.

We compute the values of the map g in the following sequence of lemmas.

Lemma 4.4.1 *Let $g : R(Q_8) \longrightarrow \mathbf{Z}_2^*$ be the function defined by equation (4.4.43). Then*

$$g(1) \in 1+8\mathbf{Z}_2\,.$$

Proof: As noted in [32, p.174], the denominator in equation (4.4.43) is

$$(\,log_2(k(x_0))\,|\,1\,) = 2^{s+3}log_2(k(\sigma c_2))\,,$$

and from Proposition 3.3.1 (i) we have that

$$k(\sigma c_2) = \sigma(t_2^2) = (13+32z)^2\,,$$

where z is some element in $\mathbf{Z}_2$. Therefore we may compute

$$\begin{aligned} 2^{s+3}log_2(k(\sigma c_2)) &= 2^{s+4}log_2(1+4(3+8z)) \\ &= 2^{s+4}[4(3+8z)-8(3+8z)^2+32z'] \\ &= 2^{s+6}[(3+8z)-2(9+4z')] \\ &= 2^{s+6}[1+8z'] \end{aligned}$$

so that, using Proposition 4.2.5, we compute

$$\frac{(a_2\,|\,1)}{(\,log_2(k(x_0))\,|\,1\,)} = \frac{2^{t+3}}{2^{s+6}\,[\,1+8z'\,]}\,,$$

which implies, since $(1+8\mathbf{Z}_2)^{-1} = (1+8\mathbf{Z}_2)$, that

$$g(1) \in 1+8\mathbf{Z}_2\,,$$

as claimed. □

Lemma 4.4.2 *Let $g : R(Q_8) \longrightarrow \mathbf{Z}_2^*$ be the function defined by equation (4.4.43). Then*

$$g(\chi_1) \in 1+8\mathbf{Z}_2\,.$$

Proof: In this case, it is shown in [32, p.175] that the denominator in equation (4.4.43) is

$$(\,log_2(k(x_0))\,|\,\chi_1\,) = -2^{s+4}log_2(k(\lambda b'))\,,$$

and from Lemma 3.3.1 (iii) we have that

$$k(\lambda b') = \lambda(\pi t_1) = 13+6\sqrt{2}+16z\,,$$

where z is some element in $\mathbf{Z}_2[\sqrt{2}]$. Setting $d = 6+3\sqrt{2}+8z$, we compute that

$$\begin{aligned} -2^{s+4}log_2(k(\lambda b')) &= -2^{s+4}log_2(1+2d) \\ &= -2^{s+4}[2d-2d^2+8d^3/3-4d^4+16z'] \\ &= -2^{s+5}[(6+3\sqrt{2})-(6+4\sqrt{2})+8z'] \\ &= -2^{s+5}[7+8z']\,. \end{aligned}$$

Using Proposition 4.2.5, we compute

$$\frac{(a_2 \,|\, \chi_1)}{(log_2(k(x_0)) \,|\, \chi_1)} = \frac{2^{t+3}\sqrt{2}}{-2^{s+5}\sqrt{2}[7+8z']},$$

which implies, since $(7+8\mathbf{Z}_2)^{-1} = (7+8\mathbf{Z}_2)$, that

$$g(\chi_1) \in 1 + 8\mathbf{Z}_2,$$

as claimed. □

Lemma 4.4.3 *Let $g : R(Q_8) \longrightarrow \mathbf{Z}_2^*$ be the function defined by equation (4.4.43). Then*

$$g(\chi_2) \in 5 + 8\mathbf{Z}_2.$$

Proof: Again it is shown in [32, p.176] that the denominator in equation (4.4.43) is

$$(log_2(k(x_0)) \,|\, \chi_2) = 2^{s+3} log_2(k(\tau c_1)).$$

From Lemma 3.3.1 (ii) we have that

$$k(\tau c_1) = \tau(t_2^2) = (25 + 20\sqrt{3} + 32z)^2,$$

where z is some element in $\mathbf{Z}_2[\sqrt{3}]$. Therefore we may compute

$$\begin{aligned} 2^{s+3} log_2(k(\tau c_1)) &= 2^{s+4} log_2(1+4d) \\ &= 2^{s+4}[4d - 8d^2 + 32z'] \\ &= 2^{s+6}[(6+5\sqrt{3}) - 2(3+4z') + 8z] \\ &= 2^{s+6}\sqrt{3}[5+8z'], \end{aligned}$$

where we have let $d = 6 + 5\sqrt{3} + 8z$. Hence using Proposition 4.2.5, we may compute that

$$\frac{(a_2 \,|\, \chi_2)}{(log_2(k(x_0)) \,|\, \chi_2)} = \frac{2^{t+3}\sqrt{3}}{2^{s+6}\sqrt{3}[5+8z']},$$

which implies, since $(5+8\mathbf{Z}_2)^{-1} = (5+8\mathbf{Z}_2)$, that

$$g(\chi_2) \in 5+8\mathbf{Z}_2\,,$$

as claimed. □

Lemma 4.4.4 *Let $g : R(Q_8) \longrightarrow \mathbf{Z}_2^*$ be the function defined by equation (4.4.43). Then*

$$g(\chi_1\chi_2) \in 3+8\mathbf{Z}_2\,.$$

Proof: It is shown in [32, p.177] that in this case the denominator in equation (4.4.43) is

$$(\,log_2(k(x_0))\,|\,\chi_1\chi_2\,) = 2^{s+4}log_2(k(\rho(b-b')))\,,$$

and from Lemma 3.3.1 (iv) we have that

$$k(\rho(b-b')) = \rho(t_2/(\pi t_1)) = 11+2\sqrt{6}+16z\,,$$

where z is some element in $\mathbf{Z}_2[\sqrt{6}]$. Therefore we may compute

$$\begin{aligned} 2^{s+4}log_2(k(\rho(b-b'))) &= 2^{s+4}log_2(1+2d) \\ &= 2^{s+4}[\,2d-2d^2+8d^3/3-4d^4+16z'] \\ &= 2^{s+5}[\,(5+\sqrt{6})-(7+2\sqrt{6})+(4+4\sqrt{6})-2] \\ &= 2^{s+6}\sqrt{6}[\,3+8z'\,] \end{aligned}$$

where, to simplify the equation, we have let $d = 5+\sqrt{6}+16z$. Therefore, using Proposition 4.2.5, we compute

$$\frac{(\,a_2\,|\,\chi_1\chi_2\,)}{(\,log_2(k(x_0))\,|\,\chi_1\chi_2\,)} = \frac{2^{t+3}\sqrt{6}}{2^{s+6}\sqrt{6}\,[\,3+8z'\,]}\,,$$

which implies, since $(3+8\mathbf{Z}_2)^{-1} = (3+8\mathbf{Z}_2)$, that

$$g(\chi_1\chi_2) \in 3+8\mathbf{Z}_2\,,$$

as claimed. □

Before computing $g(\nu)$ we need to calculate a value we will need. To compute the value of the denominator in equation (4.4.43), we must compute with $D = log_2(k((1-x^2)(c_1-c_2)))$.

Lemma 4.4.5 *With the notation just introduced, we have that*

$$(1+x+y+xy)(D^2) \in 32(3+4\mathbf{Z}_2)\,.$$

Proof:

By Lemma 3.3.1 (v), we may write

$$k((1-x^2)(c_1-c_2)) = 1+\pi^8+\pi^{13}+\pi^{16}+\pi^{19}+\pi^{21}+\pi^{22}z\,,$$

for some $z \in \mathcal{O}_L$.

We set $B = 1+\pi^8+\pi^{13}+\pi^{16}+\pi^{19}+\pi^{21}$. Then working modulo $\pi^{22}\mathcal{O}_L$, we compute that

$$\begin{aligned} D &\equiv B - B^2/2 + B^3/3 - B^4/4 + B^5/5 - \cdots \\ &\equiv (\pi^8+\pi^{13}+\pi^{16}+\pi^{19}+\pi^{21}) - (\pi^8+\pi^{12}+\pi^{21}) - \pi^{16} \\ &\equiv \pi^{12}+\pi^{13}+\pi^{19}+\pi^{20} \end{aligned}$$

Squaring, we compute that, modulo $\pi^{42}\mathcal{O}_L$

$$D^2 \equiv \pi^{24}+\pi^{26}+\pi^{33}+\pi^{37}+\pi^{38}+\pi^{39}+\pi^{40}\,.$$

We let the elements 1, x, y, and xy act on these powers and sum up to obtain, writing $z = 1+x+y+xy$,

$$\begin{aligned} z\,(D^2) &\equiv z\,(\pi^{24}+\pi^{26}+\pi^{33}+\pi^{37}+\pi^{38}+\pi^{39}+\pi^{40}) \\ &\equiv z(\pi^{24})+z(\pi^{26})+z(\pi^{33})+z(\pi^{37})+z(\pi^{38})+z(\pi^{39})+z(\pi^{40})\,, \end{aligned}$$

where the congruence is modulo $\pi^{49}\mathcal{O}_L$. In order to compute this expression, we have to consider the cases $\alpha = \alpha_+$ and $\alpha = \alpha_-$ separately, since the actions are slightly different. All computations are modulo $\pi^{49}\mathcal{O}_L$. In both cases we have that $z(\pi^{24}) \equiv z(\pi^{40}) \equiv 0$, while $z(\pi^{36}) \equiv \pi^{48}$. If $\alpha = \alpha_+$, we may compute that

$$z(\pi^{26}) \equiv \pi^{38} + \pi^{39} + \pi^{41} + \pi^{42} + \pi^{43} + \pi^{46} + \pi^{47} + \pi^{48};$$

$$z(\pi^{33}) \equiv \pi^{38} + \pi^{39} + \pi^{40} + \pi^{41} + \pi^{44} + \pi^{47};$$

and

$$z(\pi^{37}) \equiv \pi^{42} + \pi^{43} + \pi^{47}.$$

Similarly, for $\alpha = \alpha_-$ we have that

$$z(\pi^{26}) \equiv \pi^{38} + \pi^{39} + \pi^{41} + \pi^{42} + \pi^{43} + \pi^{45} + \pi^{46} + \pi^{48};$$

$$z(\pi^{33}) \equiv \pi^{38} + \pi^{39} + \pi^{40} + \pi^{41} + \pi^{44} + \pi^{45} + \pi^{46} + \pi^{48};$$

$$z(\pi^{37}) \equiv \pi^{42} + \pi^{43} + \pi^{46} + \pi^{47} + \pi^{48}.$$

Substituting these values into the previous equation we find that in both cases,

$$(1 + x + y + xy)(D^2) \equiv \pi^{40} + \pi^{44}.$$

To complete the proof, we simply notice that we may write π^{40} as

$$\pi^{40} = 32(1 + \pi^4 + \pi^9 u)$$

for some $u \in \mathcal{O}_L$, which implies that

$$(1 + x + y + xy)(D^2) \equiv 32(1 + \pi^8),$$

and this verifies the claim. □

Lemma 4.4.6 *Let $g : R(Q_8) \longrightarrow \mathbf{Z}_2^*$ be the function defined by equation (4.4.43). Then*

$$g(\nu) \in \begin{cases} 3 + 4\mathbf{Z}_2 & if\ \alpha = \alpha_+ ; \\ 1 + 4\mathbf{Z}_2 & if\ \alpha = \alpha_- . \end{cases}$$

Proof: We use an approach similar to that taken in the previous lemmas. First note that as shown in [32, p.178], we calculate that

$$(\, log_2(k(x_0)) \,|\, \nu \,) = 2^s (\, log_2(k((1-x^2)(c_1 - c_2))) \,|\, \nu \,) .$$

As in Lemma 4.4.5 we set $D = log_2(k((1-x^2)(c_1 - c_2)))$, and since $x^2(D) = -D$, we may compute as in [32, p.179] that

$$(\, D \,|\, \nu \,) = det \begin{pmatrix} (1 - x^2 - ix + ix^3)(D) & (x^2y - y - ixy + ix^3y)(D) \\ (y - x^2y - ixy + ix^3y)(D) & (1 - x^2 + ix - ix^3)(D) \end{pmatrix},$$

$$= 4[\,(1 + x + y + xy)(D^2)\,] .$$

By Lemma 4.4.5 above, we have that

$$(1 + x + y + xy)(D^2) = 96 + 128z = 32(3 + 4z)$$

for some $z \in \mathbf{Z}_2$. Hence applying Proposition 4.2.5, we compute

$$\frac{(\, a_2 \,|\, \nu \,)}{(\, log_2(k(x_0)) \,|\, \nu \,)} = \frac{2^{2t+4}(\pm 1)}{2^{s+7}\,[\,3 + 4z\,]},$$

which implies that for $\alpha = \alpha_+$,

$$g(\nu) \in 3 + 4\mathbf{Z}_2 ,$$

while for $\alpha = \alpha_-$,

$$g(\nu) \in 1 + 4\mathbf{Z}_2 ,$$

as claimed. □

We may now combine the above lemmas with Taylor's formula (4.4.44) to obtain our result.

Proof of Proposition 4.1.3: Considering first the 1-dimensional representations, we see that

$$\begin{aligned} B &= g(1+\chi_1+\chi_2+\chi_1\chi_2) \\ &= g(1)\,g(\chi_1)\;g(\chi_2)\,g(\chi_1\chi_2) \in 7+8\mathbf{Z}_2\,. \end{aligned}$$

Hence, if we denote by u some undetermined element of $\mathbf{Z}_2$, we obtain

$$\begin{aligned} log_2(B) &\equiv log_2(1+6+8u) \\ &\equiv 6-18-4+8u' \equiv 0 \;\; (mod\ 8)\,. \end{aligned}$$

It follows that

$$(-1)^{(1/4)log_2(B)} = (-1)^2 = 1\,,$$

so that by Proposition 4.4.6 and equation (4.4.44) we compute that

$$[Ker(k')] = [g] = \begin{cases} -1 & if\ \alpha = \alpha_+ \\ 1 & if\ \alpha = \alpha_- \end{cases}. \qquad \square$$

Bibliography

[1] Ph. Cassou-Noguès: Quelques théorèmes de base normal d'entiers; Ann. Inst. Fourier 28 (1978) 1–33.

[2] Ph. Cassou-Noguès, T. Chinburg, A. Fröhlich and M.J. Taylor: L-functions and Galois modules; London Math. Soc. 1989 Durham Symposium, *L-functions and Arithmetic* Cambridge University Press (1991) 75–139.

[3] T. Chinburg: On the Galois structure of algebraic integers and S-units; Inventiones Math. 74 (1983) 321–349.

[4] T. Chinburg: Exact sequences and Galois module structure; Annals Math. 121 (1985) 351–376.

[5] T. Chinburg: *The Analytic Theory of Multiplicative Galois Structure*; Mem. A.M. Soc. 395 (1989).

[6] T. Chinburg, M. Kolster, G. Pappas and V. Snaith: *Galois structure of K-groups of rings of integers*; C. R. Acad. Sci. Paris, t. 320, Série I (1995) 1435–1440.

[7] T. Chinburg, M. Kolster, G. Pappas and V. Snaith: *Quaternionic Exercises in K-Theory Galois Module Structure*; McMaster University preprint No. 5 (1995).

[8] C.W. Curtis and I. Reiner:*Methods of Representation Theory* vols.I & II; Wiley (1981,1987).

[9] A. Fröhlich: Artin root numbers and normal integral bases for quaternion fields; Inventiones Mathematicae 17 (1972) 143–166.

[10] A. Fröhlich: Resolvents and trace form; Math. Proc. Cambridge Phil. Soc. 78 (1975) 185–210.

[11] A. Fröhlich: Arithmetic and Galois module structure for tame extensions; J. Reine. Angew. Math. 286/7 (1976) 380–440.

[12] A. Fröhlich: *Galois Module Structure of Algebraic Integers* ; Ergebnisse der Mathematik und ihrer Grenzgebiete 3 Folge-Band 1 Springer-Verlag (1983).

[13] A. Fröhlich and J. Queyrut: On the functional equation for Artin L-functions for characters of real representations; Inv. Math. 20 (1973) 125–138.

[14] C. Greither: On Chinburg's second conjecture for abelian fields; Preprint (1995) .

[15] C. Greither and D. Holland: Chinburg's third invariant in the defect class group for abelian extensions of $\mathbf{Q}$; Preprint (1993) .

[16] P.J. Hilton and U. Stammbach: *A Course in Homological Algebra*; Grad. Texts in Math. # 4 (1971) Springer-Verlag.

[17] D. Holland: Additive Galois module structure and Chinburg's invariant; J. reine angew. Math 425 (1992) 193–218.

[18] C.U. Jensen and N. Yui: Quaternion extensions; Conf. Alg. Geom. and Comm. Alg. in honour of M. Nagata (1987) 155–182.

[19] S. Kim: A generalization of Fröhlich's theorem to wildly ramified quaternion extensions of $\mathbf{Q}$; Ill. J. Math. 35 (1991) 158–189.

[20] S. Kim: The root number class and Chinburg's second invariant; J. Alg. 153 (1992) 133–202.

[21] J. Martinet: Sur l'arithmetique d'une extension galoisiennes à groupe de Galois diédral d'ordre $2p$; Ann. Inst. Fourier 19 (1969) 1–80.

[22] J. Martinet: Character theory and Artin L-functions; London Math. Soc. 1975 Durham Symposium, *Algebraic Number Fields* Academic Press (1977) 1–87.

[23] J. Martinet: H_8; London Math. Soc. 1975 Durham Symposium, *Algebraic Number Fields* Academic Press (1977) 525–538.

[24] J. Neukirch: Class Field Theory; Grundlehren der mathematischen Wissenschaften 280 (1986) Springer-Verlag.

[25] D.S. Passman: *A Course in Ring Theory*; (1991) Wadsworth & Brooks/Cole.

[26] J.J. Rotman: *An Introduction to Homological Algebra* ; (1979) Academic Press.

[27] J-P. Serre: Conducteurs d'Artin des caractères réels; Inv. Math. 14 (1971) 173–183.

[28] J-P. Serre: *A Course in Arithmetic*; Graduate Texts in Mathematics # 7 (1973) Springer-Verlag.

[29] J-P. Serre: *Local Fields* ; Graduate Texts in Mathematics # 67 (1979) Springer-Verlag.

[30] V.P. Snaith: *Topological Methods in Galois Representation Theory*; C.M.Soc. Monographs (1989) Wiley.

[31] V.P. Snaith: *Explicit Brauer Induction (with applications to algebra and number theory)*; Cambridge Studies in Advanced Math. 40 (1994) Cambridge University Press.

[32] V.P. Snaith: *Galois Module Structure*; Fields Institute Monographs (1994) American Mathematical Society.

[33] J.T. Tate: Local Constants; London Math. Soc. 1975 Durham Symposium, *Algebraic Number Fields* (ed. A. Fröhlich) 89–131 (1977) Academic Press.

[34] M.J. Taylor: Adams operations, local root numbers and the Galois module structure of rings of integers; Proc. London Math. Soc. (3) 39 (1979) 147–175.

[35] M.J. Taylor: On Fröhlich's conjecture for rings of integers of tame extensions; Inventiones Math. 63 (1981) 41–79.

[36] M.J. Taylor: *Class Groups of Group Rings*; L.M.Soc. Lecture Notes Series # 91 (1984) Cambridge University Press.

[37] M.V. Tran: The Second Chinburg Conjecture for Quaternion Fields; Ph.D. Thesis, McMaster University, 1996.

[38] L. Washington: *Introduction to Cyclotomic Fields*; Graduate Texts in Mathematics # 83 (1982) Springer-Verlag.