UNIVERSITY OF CALIFORNIA, SAN DIEGO

On the Values of Equivariant and Artin L-functions of Cyclic Extensions of Number Fields

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Barry Ried Smith

Committee in charge:

Professor Cristian Popescu, Chair
Professor Wee Teck Gan
Professor Ronald Graham
Professor Russell Impagliazzo
Professor Harold Stark

2007

The dissertation of Barry Ried Smith is approved, and it is acceptable in quality and form for publication on microfilm:

_____

_____

_____

_____

_____

Chair

University of California, San Diego

2007

To my wife, my parents, and my brother.

Last time, I asked:

"What does mathematics mean to you?"

And some people answered:

"The manipulation of numbers, the manipulation of structures."

And if I had asked what music means to you, would you have answered:

"The manipulation of notes?"

—Serge Lang, *The Beauty of Doing Mathematics*

TABLE OF CONTENTS

Signature Page . . . iii

Dedication . . . iv

Epigraph . . . v

Table of Contents . . . vi

List of Tables . . . viii

Acknowledgements . . . ix

Vita and Publications . . . x

Abstract of the Dissertation . . . xi

Chapter 1 Introduction . . . 1
1.1 History . . . 1
1.2 The L-function evaluator . . . 8

Chapter 2 Algebraic Background . . . 11
2.1 Torsion modules over Dedekind domains . . . 11
2.2 Representation theory . . . 12
2.3 Group Algebras . . . 14
2.4 Fitting Ideals . . . 19
2.5 Kummer Theory . . . 26
2.6 Class field theory . . . 27
2.6.1 The Artin map . . . 28
2.6.2 Class fields . . . 30
2.7 Group extensions . . . 31

Chapter 3 The Objects and Conjectures of Study . . . 38
3.1 Properties of Artin L-functions . . . 38
3.2 Partial Zeta Functions . . . 43
3.3 Components of the equivariant L-function . . . 47
3.4 The Brumer and Brumer-Stark Conjectures . . . 53
3.4.1 Statement of the conjectures . . . 53
3.4.2 The state of knowledge . . . 56
3.5 Hayes's Conjecture . . . 58

Chapter 4 L-values of Cyclic Extensions 61
4.1 Overview 61
4.2 L-values for quadratic extensions 63
4.3 Norms of L-values for degree 2^m extensions 64
4.4 L-values for degree 2^m extensions 70
4.5 Norms of L-values for degree $2^m p$ extensions 75
4.6 Norms of L-values for degree $2^m p^n$ extensions 86
4.7 L-values for degree $2^m p^n$ extensions 99
4.8 A generalization of a theorem of Kummer 104
4.9 L-values in cyclotomic towers 111

Chapter 5 The Brumer-Stark Conjecture 114
5.1 The Brumer-Stark conjecture for extensions of degree 2^m 114
5.2 The component Brumer-Stark conjecture for extensions of degree $2^m p^n$ 124
5.2.1 Local results at primes other than 2 and p 125
5.2.2 The 2-primary part 130
5.2.3 The p-primary part 132
5.3 The Brumer-Stark conjecture for extensions of degree $2^m p^n$ 141

Chapter 6 Hayes's Conjecture 152
6.1 Hayes's conjecture for degree 2^m extensions 152
6.2 Change of the set S in Hayes's conjecture 156
6.3 Top change for Hayes's conjecture 157
6.4 Hayes's conjecture for Abelian extensions of prime conductor 161
6.4.1 The key congruence 161
6.4.2 The p-primary part of Hayes's conjecture 164
6.4.3 Examples 170
6.4.4 The 2-primary part of Hayes' Conjecture 171
6.5 A numerical counterexample 175

References 177

LIST OF TABLES

Table 6.1: Irregular prime numbers p with small $d_{p,n}$ 171

ACKNOWLEDGEMENTS

How fortuitous for me that my advisor, Cristian Popescu, arrived at the University of California, San Diego, during my graduate studies! My academic life was transformed on the first day of our seminar on Drinfeld modules, and I cannot express how much of an influence and an inspiration you have been since. Thank you for introducing me to Stark's conjectures, arithmetic geometry, class field theory, Iwasawa theory, and my dissertation work in particular. I have loved the time I have spent working in this area. You have been both a mentor and a friend, and your generosity with your time – weekly meetings, reading through complicated calculations, and the brilliant courses – has been tremendous.

I must also thank professors Evans, Gan, Stark, and Terras. Each of you has presented me with a new perspective on number theory, which has deepened my appreciation for the mystery and beauty of the subject. Thank you for your patience and advice. Also, I must include Fred Koch, my first great teacher and the man who inspired me to be both a mathematician and a scholar.

I would especially like to thank all of my relatives and friends for your encouragement and sacrifices during my inordinately long education. Mom and Dad, you provided me with the environment and freedom to explore my dreams, and I hope to be as good with my own children. Your careful proofreading of this dissertation has also been invaluable. Owen, my oldest friend and role model, I have always strived to emulate you. You get special acknowledgement on p. 170. And Kelly, my dear wife, you have worked hard to provide for our family during my graduate education. Your unwavering support and encouragement have been my foundation throughout this endeavor, and I love you for it. Finally, I would like to thank Bailey, the dog, who provided an excuse to spend hours walking and pondering, and a companion during the long and trying process of writing a dissertation.

VITA

2000	B. A., Mathematics, *magna cum laude*, University of California, San Diego
2000	B. S., Chemical Physics, *magna cum laude*, University of California, San Diego
2001-2006	Teaching assistant, Department of Mathematics, University of California, San Diego
2003	M. A., Mathematics, University of California, San Diego
2005	C. Phil., Mathematics, University of California, San Diego
2005-2006	Adjunct Instructor, Department of Mathematics, San Diego Mesa College
2006-2007	Adjunct Instructor, Department of Rhetoric and Writing Studies, San Diego State University
2007	Ph. D., University of California, San Diego

ABSTRACT OF THE DISSERTATION

On the Values of Equivariant and Artin L-functions of Cyclic Extensions of Number Fields

by

Barry Ried Smith
Doctor of Philosophy in Mathematics
University of California, San Diego, 2007
Professor Cristian Popescu, Chair

We study the values produced by equivariant Artin L-functions at zero. We begin with three preliminary chapters providing the requisite background. In the fourth chapter, we derive expressions for the norms of the values of Artin L-functions attached to cyclic extensions of degree $2^m p^n$, where p is an odd prime number, $m \geq 1$, and $n \geq 0$. We propose hypothetical expressions for the values themselves in terms of the Fitting ideals of two arithmetic modules over the ring of integers in a cyclotomic field, and validate the expressions and their local variants in several cases.

In chapter five, the formulas from chapter four are used to study the Brumer-Stark conjecture and its local variants in several new cases. Our methods are similar to those used in the study of degree $2p$ extensions by Greither, Roblot, and Tangedal, excepting the use of the formulas from chapter four that enable proofs in our more general setting. Some results deal only with the annihilation statement of the p-primary part of the conjecture for degree $2^m p^n$ extensions. They hint that something deeper is happening with the p-primary part of the conjecture in the cases where general proofs cannot yet be given.

In chapter six, the expressions from chapter four are used to study a new conjecture of Hayes concerning the precise denominators of the values of the equivariant L-functions at zero. A variant of this conjecture is proved for extensions of degree

2^m using the formulas from chapter four. Following that, it is shown that the truth of the conjecture is preserved under lowering of the top field. We then prove the conjecture for extensions where both fields are absolutely Abelian of prime conductor. Lastly, a counterexample is provided to a stronger conjecture posed by Hayes in an unpublished manuscript.

Chapter 1

Introduction

1.1 History

Zeta and L-functions are ubiquitous in mathematics. A description of the state of knowledge of all such functions would fill many volumes, so we must aim for something more modest within this chapter. We will attempt to give a brief overview only of the various zeta and L-functions relevant to the results in this work. Even this would be too large an undertaking for our purposes; for instance, we would need to discuss the relationship between these functions and both the analytic and algebraic aspects of the theory, including such topics as the Riemann Hypothesis and the Prime Number Theorem. We will therefore strive to give a history only of the creation of these functions, and the relationship between their special values and the algebraic side of the theory.

The study of special values of zeta and L-functions was initiated in 1650, when Pietro Mengoli asked for the value of the infinite series

$$\sum_{n=1}^{\infty} \frac{1}{n^2}.$$

This problem resisted the efforts of such masters as Gottfried von Leibnitz, Jacob Bernoulli, and Johann Bernoulli, before it succumbed to Leonard Euler in 1735. Using a brilliant, albeit unrigorous, argument, he found that

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

His paper included several similar evaluations, and demonstrated that he was already studying what is now known as the Riemann zeta function,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

as a function of the variable s for integer valued $s > 1$. In 1737, he discovered the Eulerian product,

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}},$$

from which followed a new proof of the infinitude of prime numbers. This important formula was the first indication of the algebraic nature of zeta and L-functions. Euler spent the next several years extending his results and striving to place them on a firm foundation. Finally, in 1750, he published the following remarkable formula for the values of the Riemann zeta function at positive even integers:

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = (-1)^{k-1} \frac{(2\pi)^{2k}}{2\,(2k)!} B_{2k}.$$

The rational numbers B_{2k} are the Bernoulli numbers.

In 1674, the young Leibniz was the first to discover a special value of what is now termed an L-function, when he evaluated

$$L(1) = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} = \frac{\pi}{4}.$$

In his paper of 1735, Euler evaluated

$$L(s) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s}$$

for various positive integral values of s. His paper of 1737 then included, besides the Eulerian product expansion for $\zeta(s)$, the related product expansion for $L(1)$. He later recognized that this result gives an analytic proof of the infinitude of prime numbers of the forms $4n+1$ and $4n+3$. It should be noted that Euler also obtained a result equivalent to the functional equations for $\zeta(s)$ and $L(s)$, which was unfortunately ignored for the next 100 years.

In 1837, Johann Lejeune Dirichlet extended the idea of Euler's proof of the infinitude of prime numbers of the form $4n+1$ and $4n+3$ to prove his famous

theorem on prime numbers in arithmetic progressions. To accomplish this, he introduced a variant of the Riemann zeta function, the Dirichlet L-function. It is defined by

$$L(s,\chi) = \sum_{i=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \frac{1}{1-\chi(p)p^{-s}},$$

where χ is a periodic and multiplicative function on the integers called a Dirichlet character. As indicated, these can be written either as a series or as an Eulerian product; both expressions converge to an analytic function of the complex variable s in the half-plane $\Re(s) > 1$. An example is the L-function considered by Euler in his paper of 1735, which is associated with the Dirichlet character defined by

$$\chi(n) = \begin{cases} 1, & \text{if } n \equiv 1 \pmod 4; \\ -1, & \text{if } n \equiv 3 \pmod 4; \\ 0, & \text{if } n \equiv 0 \text{ or } 2 \pmod 4. \end{cases}$$

Dirichlet's work also provided the next conceptual advance in the theory of zeta and L-functions – the idea that the special values of these functions, besides having simple closed-form expressions, also contain arithmetic information. He derived an explicit expression, partly anticipated by Carl Jacobi, for the class number of an imaginary quadratic field in terms of the value of a Dirichlet L-function at $s = 1$. He also derived a class number formula for real quadratic fields, expressing a relationship between the value of a Dirichlet L-function at $s = 1$ and the class number and fundamental unit of the corresponding real quadratic field.

Both the Riemann zeta-function and the Dirichlet L-functions can be analytically continued, the zeta function to the whole complex plane excluding a simple pole at $s = 1$, and the L-functions to entire functions. Thus, one may also consider their values at negative integers. Analytic continuation is required to show that these values exist. One might therefore suspect that the values produced thereby are transcendental, and perhaps do not have simple closed-form expressions. It is a mystifying result, then, that the values of these functions at negative integers are algebraic. This follows from the equally astounding result that these functions, satisfy "functional equations", which relate the value of a function at a complex number s to the value at $1 - s$. The values of the Riemann zeta-function

and Dirichlet L-functions at negative integers are given in terms of generalized Bernoulli numbers, although this was not fully understood until the twentieth century. These numbers lie in the field of values of the associated Dirichlet character.

The next major advances in the theory of zeta and L-functions required the development of the theory of more general number fields, finite extension fields of the rational numbers. The first important advance in this direction was Ernst Kummer's theory of ideal numbers. In 1850, Kummer published a paper which used this theory to prove some of the cornerstones of the theory of cyclotomic fields. Two are of interest to the history of values of zeta functions. First, he introduced a function associated with each cyclotomic field of prime conductor, later known as a Dedekind zeta function. He showed that the residues of these functions at $s = 1$ contain arithmetic information about the associated fields. Second, he discovered that the class number of the cyclotomic field of conductor p is divisible by p exactly when p divides the numerator of $\zeta(-n)$ for some $n = 1, 3, \ldots, p-4$. Thus, the values of the Riemann zeta function encode information about extension fields of the rational numbers.

In the 1870's, Richard Dedekind created ideals as an alternative to ideal numbers for overcoming the lack of unique factorization in general number fields. He demonstrated that an ideal in the ring of integers of such a field always has a unique factorization as a product of prime ideals. Later, he created generalizations of the Riemann zeta function called Dedekind zeta functions. Given an algebraic number field K, the associated Dedekind zeta function is defined as

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}},$$

where the sum runs over the integral ideals of the ring of integers of K, the product runs over the prime ideals of this ring, and $\mathfrak{N}(\mathfrak{a})$ denotes the absolute norm of the ideal $\mathfrak{a}$. Again, a Dedekind zeta function has expressions both as a series and as an Eulerian product, and both expressions converge to an analytic function on the half-plane $\Re(s) > 1$. In the case where $K = \mathbb{Q}$, the Dedekind zeta function is just the Riemann zeta function. In the eleventh supplement to Dirichlet's *Vorlesungen Über Zahlentheorie* published in 1894, Dedekind proved the seminal analytic class

number formula. This says that the residue at $s = 1$ of the Dedekind zeta function of a field K is

$$\frac{2^{r_1}(2\pi)^{r_2}}{W\,|d|^{1/2}}hR,$$

where r_1 is the number of real embeddings $K \hookrightarrow \mathbb{C}$, r_2 is the number of pairs of complex conjugate embeddings $K \hookrightarrow \mathbb{C}$, W is the number of roots of unity in K, d is the discriminant of K, h is the class number of K, and R is the regulator of a fundamental system of units of K. The Dedekind zeta function therefore encodes all of the important arithmetic information about K.

Number theorists next sought a common generalization of the Dedekind zeta functions and the Dirichlet L-functions, but the correct generalization of the Dirichlet characters is not the most obvious possibility. Since the Dedekind zeta function of a field K is defined as a sum over ideals, the definition of the new L-functions involves a multiplicative function on the ideal group of the ring of integers of K. It was desired that the new L-functions have meromorphic continuations to the complex plane and functional equations. To ensure that the L-functions have such properties, it is necessary to restrict the definition of the multiplicative function. Erich Hecke found the appropriate restriction, and called these multiplicative functions Größencharacters. Given a Größencharacter χ, the corresponding L-series is defined by

$$L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}\mathfrak{a}}.$$

Between 1917 and 1920, Hecke managed to prove that his new L-functions, including the Dedekind zeta function in the special case where $\chi(\mathfrak{a}) = 1$ for all $\mathfrak{a}$, have analytic continuations to the entire complex plane (excepting a simple pole at $s = 1$ for the Dedekind zeta function), and that they satisfy functional equations.

Using the functional equation and the analytic class number formula, one can show that the Maclaurin series of the Dedekind zeta function of a field K begins with the term

$$-\frac{hR}{W}s^{r_1+r_2-1}. \tag{1.1}$$

Thus, the value of a certain derivative of the zeta function at $s = 0$ gives information about the arithmetic of the field. However, the special values of other Hecke

L-functions are much less understood. For instance, special values of Abelian L-functions, particular types of Hecke L-series, were expressed through an appropriate generalization of the Bernoulli numbers only in 1979 by Takuro Shintani. A closed-form expression or arithmetic interpretation for the special values of general Hecke L-functions has not yet been found.

Until now, the zeta and L-functions that we have considered have each been associated with a number field. The next major historical step was Emil Artin's creation of L-functions attached to Galois *extensions* of number fields. This idea grew out of the Eulerian product for Abelian L-functions. Given a field k, the associated Abelian L-functions are the Hecke L-functions whose associated Größencharakters come from characters on ray class groups of k. The introduction of class field theory allows one to consider these as characters on Galois groups of Abelian extensions of k. In a paper of 1923, Artin extended this idea to define functions attached to characters of represenations of arbitrary Galois extensions of number fields. If K/k is such an extension, with Galois group G, and if ρ is a representation of G on a finite dimensional complex vector space V with character χ, then the Artin L-function associated with χ is defined as

$$L_{K/k}(s,\chi) = \prod_{\mathfrak{p}} \frac{1}{\det\left(1 - \sigma_{\mathfrak{P}} \mathfrak{N}(\mathfrak{p})^{-s}; V^{I_{\mathfrak{P}}}\right)}. \tag{1.2}$$

Here, $\mathfrak{p}$ runs through the prime ideals of k, $\mathfrak{P}$ is a prime ideal of K dividing $\mathfrak{p}$, $\sigma_{\mathfrak{P}}$ is an arbitrary Frobenius automorphism associated with $\mathfrak{P}$, and $V^{I_{\mathfrak{P}}}$ is the subspace of V fixed by the inertia group $I_{\mathfrak{P}}$ of $\mathfrak{P}$ over $\mathfrak{p}$. As indicated in the notation, representations with the same character yield the same Artin L-function, and the definition is independent of the choice of Frobenius element for the ramified primes $\mathfrak{P}$. With this definition, Artin introduced the monumental idea that one should define L-functions through Eulerian products whose local factors are given by the determinant of the action of a Frobenius element on a certain module. A series expansion analogous to that of the Riemann zeta function does not exist for general Artin L-functions, but they behave well under change of the extension K/k, they have meromorphic continuations to the complex plane, and they satisfy functional equations. The Artin conjecture states that if χ is the character of an irreducible

representation of G, then the Artin L-function associated with χ has a holomorphic continuation to the complex plane, excepting the known pole at $s = 1$ when χ is the trivial character.

The Galois-equivariant Artin L-function is created by assembling together the various Artin L-functions associated with an extension as follows. Let K/k be an Abelian extension of number fields with Galois group G. Given a complex-valued character $\chi \in \widehat{G}$, there is an associated idempotent in $\mathbb{C}[G]$:

$$e_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi\left(\sigma^{-1}\right) \sigma. \tag{1.3}$$

The equivariant Artin L-function associated with K/k is defined by

$$\theta_{K/k}(s) = \sum_{\chi \in \widehat{G}} L_{K/k}\left(s, \chi^{-1}\right) e_\chi, \tag{1.4}$$

where the functions $L_{K/k}(s, \chi)$ are the Artin L-functions of K/k. θ is a meromorphic function from the complex numbers to the complex group ring $\mathbb{C}[G]$. When G is the trivial group, the equivariant L-function is the Dedekind zeta function of k.

Much less is known about the special values of Artin and equivariant Artin L-functions than those of the subset of Abelian L-functions. The description of the values of Artin L-functions in terms of the arithmetic of the associated fields is the goal of the extremely far-reaching Stark conjectures. These conjectures and their refinements, the first being developed in the 1970's and early 1980's by Harold Stark ([53], [54], [55], [56]), describe the coefficients of the leading terms of the Maclaurin series of Artin and equivariant Artin L-functions. The Abelian refinements of Stark's main conjecture suggest that these coefficients contain arithmetic information about the fields K and k, including information about generators of Abelian extensions of k. As a special case, just as the rational part of the coefficient in (1.1) is the quotient of the ideal class number by the number of roots of unity in the associated field, it is suspected that the value of an equivariant Abelian L-function at $s = 0$, when nonzero, contains more refined algebraic information about these groups. In the next section, we will discuss three ideas in this direction — one known and two conjectural.

1.2 The L-function evaluator

To obtain clean results about the values of Artin and equivariant Artin L-functions, we must introduce their S-truncated variants. For an Abelian extension of number fields K/k with Galois group G and a set S of places of k containing the Archimedean places, the S-truncated Artin L-function associated with a character $\chi \in \widehat{G}$ is the Artin L-function associated with χ deprived of the Euler factors corresponding to the finite places in S. The S-truncated equivariant L-function is formed from the S-truncated Artin L-functions by using S-truncated L-functions in (1.4). In both cases, the S-truncated versions are denoted by adding an S to the subscript in the function's name.

The special value of the equivariant L-function $\theta_{K/k,S}(0)$ is called the L-function evaluator associated with K/k and S. It will usually be written as $\theta_{K/k,S}$, or simply as θ when the context is clear. It is the element of $\mathbb{C}[G]$ defined by

$$\theta = \sum_{\chi \in \widehat{G}} L_{K/k,S}\left(0, \chi^{-1}\right) e_\chi,$$

where the idempotents e_χ are defined by (1.3). It is so named because applying the $\mathbb{C}$-linear extension of a character χ to θ gives the Artin L-function value $L_{K/k,S}\left(0, \chi^{-1}\right)$.

The most important property of the $\theta_{K/k,S}$ is that its coefficients are rational numbers when S contains the prime ideals that ramify in K. This was first proved by Siegel [52], building upon earlier work of Klingen [30]. A little later, Shintani [51] reproved this by different methods. A stronger result, proved independently by Daniel Barsky [2], Pierrette Cassou-Noguès [5] and Deligne-Ribet [8] says that θ is almost integral; the denominators of its coefficients divide $W_K = |\mu_K|$, the number of roots of unity in K. They actually proved that multiplying θ by the $\mathbb{Z}[G]$-annihilator of μ_K gives an ideal in the integral group ring $\mathbb{Z}[G]$, known as the Stickelberger ideal. This result is the G-equivariant analogue of the rational part of the coefficient in (1.1) having denominator W_K.

Multiplying the rational part of the coefficient in (1.1) by W gives the class number of K. Continuing with our analogy, one might suspect that the Stickelberger ideal is related to the class group of K. There are two conjectures describing

such a relationship. Brumer's conjecture states that the Stickelberger ideal is contained in the $\mathbb{Z}[G]$-annihilator of the ideal class group of K. The Brumer-Stark conjecture asserts first that $W_K\theta$ is contained in the $\mathbb{Z}[G]$-annihilator of the ideal class group of K. This is just a special case of Brumer's conjecture. However, the Brumer-Stark conjecture further claims that the principal ideal produced by applying $W_K\theta$ to a given ideal of K has a generator with very special properties – all of its algebraic conjugates have absolute value 1, and its W_Kth root generates an Abelian extension of k. Thus, the Brumer-Stark conjecture suggests that the value of the equivariant L-function at $s = 0$ contains information about Abelian extensions of k larger than K. This has implications for Hilbert's 12th problem.

The final part of the analogy concerns the denominators of the coefficients of the value of the equivariant L-function at $s = 0$ when reduced to lowest terms. These denominators may be proper divisors of the number of roots of unity of K. In the case of the Dedekind zeta function, the actual denominator of the rational part of the coefficient in (1.1) is found by removing a factor from W equal to the greatest common denominator of the class number and number of roots of unity. David Hayes ([25]) recently stated a conjecture which proposes a relationship between the actual denominators of the coefficients of the value of the equivariant L-function at $s = 0$ and the structure of the class group of K. We will see that there can also be a relationship between the structures of the class group and roots of unity of K that is manifest in the values of the S-truncated Artin L-functions of the extension at $s = 0$. For the trivial extension $K = k$, this relationship (manifest in the value of the S-truncated Dedekind zeta function) is uninteresting.

The purpose of this work is to develop new information about the special values of Artin and equivariant Artin L-functions for certain *cyclic* extensions. We will discuss the result and conjectures mentioned in the previous paragraphs for these extensions, proving them in some cases. In Chapter 2, we will review the algebraic results that will be used in the later chapters. Chapter 3 gives an introduction to the main objects of study, including precise statements of the above conjectures and a summary of cases in which they are known to be true. In Chapter 4, we will provide expressions for values of L-functions in terms of the arithmetic of the

associated fields. In Chapter 5, we will use the results in Chapter 4 to prove new cases of the Brumer-Stark conjecture for certain cyclic extensions. In Chapter 6, we will use the results from Chapter 4 to analyze Hayes's conjecture for certain cyclic extensions. We will examine the effects of changing the set S or the top field appearing in the conjecture. We will then prove part of Hayes's conjecture in several instances. Finally, we will provide a counterexample to another part of Hayes's conjecture.

Chapter 2

Algebraic Background

In this chapter, we will collect the prerequisite algebraic knowledge that will be used in later chapters. We assume a knowledge of basic algebraic number theory and commutative algebra. This includes commutative ring theory and Galois theory. We also assume standard knowledge about algebraic integers, ideal groups, ideal class groups, and unit groups. Furthermore, we assume that the reader has a basic familiarity with p-adic integers. See, for instance, [11], [38], or [50].

2.1 Torsion modules over Dedekind domains

Finitely generated torsion modules over a fixed Dedekind domain are classified by the Primary Decomposition Theorem:

The Primary Decomposition Theorem. *Let M be a finitely generated torsion module over the Dedekind domain R. Then M is isomorphic to a module of the form*

$$\bigoplus_{\mathfrak{p}\in I_R} \left(R/\mathfrak{p}^{e(\mathfrak{p},1)} \oplus R/\mathfrak{p}^{e(\mathfrak{p},2)} \oplus \cdots \oplus R/\mathfrak{p}^{e(\mathfrak{p},l(\mathfrak{p}))} \right).$$

The sum is over the prime ideals of R, and for each prime ideal $\mathfrak{p}$, $l(\mathfrak{p})$ is an integer, the exponents $e(\mathfrak{p}, i)$ are positive integers, and $l(\mathfrak{p}) = 0$ for all but finitely many primes $\mathfrak{p}$. This decomposition is unique up to rearrangement of the summands.

For a proof, see [3, Theorem 6.3.20].

2.2 Representation theory

A reference for this material is [49]. Given a finite group G, a representation of G in a complex vector space V is a group homomorphism ρ from G into $\mathrm{GL}(V)$, the group of isomorphisms of V. V will also be called a representation of G. When V has finite dimension n, the representation is said to have degree n. If W is a subspace of V which is stable under the action of G, then the homomorphism from G to $\mathrm{GL}(W)$ given by composing ρ with restriction to W gives a representation of G in W; W is said to be a subrepresentation of V. A representation of G in a space V is said to be irreducible if V is nonzero and no subspace of V other than 0 and V is stable under the action of G. For instance, a representation of degree 1 is irreducible.

We may reformulate the above terminology in terms of modules over the group ring $\mathbb{C}[G]$ (see Section 2.3). A representation of G in a space V endows V with the structure of a $\mathbb{C}[G]$-module. In this context, a subrepresentation of V is just a $\mathbb{C}[G]$-submodule of V. An irreducible representation is one for which the corresponding module is simple. Two representations are said to be isomorphic if the corresponding $\mathbb{C}[G]$-modules are isomorphic.

If $V = \bigoplus_i W_i$ is a decomposition of V as a direct sum of subspaces and if each subspace W_i is a $\mathbb{C}[G]$-submodule of V, we say that V is the direct sum of the representations W_i. Every representation can be decomposed as a direct sum of irreducible representations. In such a decomposition, the number of irreducible representations isomorphic to a given one is independent of the chosen decomposition.

All irreducible representations of an Abelian group G have degree 1. In other words, an irreducible representation of an Abelian group G is just a character $\chi : G \to \mathbb{C}^\times$. In this work, we will only consider representations of finite Abelian groups.

If ρ is a representation of a finite group G in a space V, the character χ_ρ of ρ is the complex-valued function on G defined by

$$\chi_\rho(g) = \mathrm{Trace}(\rho(g)).$$

Surprisingly, a representation is determined up to isomorphism by its character. Let V be a representation space with a decomposition as a direct sum of subrepresentations

$$V = \bigoplus_{i=1}^{n} W_i,$$

Let χ be the character of V and let χ_i be the character of W_i for $1 \leq i \leq n$. These characters satisfy the relation

$$\chi = \sum_{i=1}^{n} \chi_i.$$

We can define a scalar product on the characters of representations of G by

$$\langle \chi, \psi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}.$$

If χ and ψ are the characters of two irreducible representations, then

$$\langle \chi, \psi \rangle_G = \begin{cases} 1, & \text{if } \chi \text{ and } \psi \text{ are isomorphic;} \\ 0, & \text{otherwise.} \end{cases} \tag{2.1}$$

If H is a subgroup of G, then a representation of H in a space W induces a representation V of G:

$$V = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W.$$

V is called the representation induced by W. If χ is the character of the representation W, then the character of the induced representation will be denoted by $\operatorname{Ind} \chi$. Similarly, if ρ is a representation of G, then the restriction of ρ to H is a representation of H. If χ is the character of the representation ρ of G, then the restriction of χ to H is the character of the restriction of ρ to H. This restricted character will be denoted $\operatorname{Res} \chi$.

If H is a subgroup of G, ψ is the character of a representation of G, and χ is the character of a representation of H, then the Frobenius Reciprocity Theorem says:

$$\langle \chi, \operatorname{Res} \psi \rangle_H = \langle \operatorname{Ind} \chi, \psi \rangle_G . \tag{2.2}$$

We will only need this theorem to prove the following proposition.

Proposition 2.2.1. *Let H be a subgroup of a finite Abelian group G. If χ is an irreducible character on H, then*

$$\operatorname{Ind}\chi = \sum_{\substack{\psi\in\widehat{G}\\ \operatorname{Res}\psi=\chi}} \psi.$$

Proof. Since G and H are Abelian, the characters of the irreducible representations of G and H are the usual characters in $\widehat{G}$ and $\widehat{H}$. If $\psi \in \widehat{G}$ is such that $\operatorname{Res}_H \psi = \chi$, then by Frobenius Reciprocity,

$$\langle \chi, \chi \rangle_H = \langle \operatorname{Ind}\chi, \psi \rangle_G .$$

It follows from (2.1) that

$$\langle \operatorname{Ind}\chi, \psi \rangle_G = 1.$$

Otherwise, if $\operatorname{Res}_H \psi \neq \chi$, then since unequal characters are not isomorphic, similar reasoning shows that

$$\langle \operatorname{Ind}\chi, \psi \rangle_G = 0.$$

The proposition now follows since, for any character $\psi \in \widehat{G}$, the number of characters in a decomposition of $\operatorname{Ind}\chi$ into irreducible characters that are isomorphic to ψ is $\langle \operatorname{Ind}\chi, \psi \rangle$ (see, for instance, [49, §2.3, Theorem 4]). □

2.3 Group Algebras

A reference for this material is [45, Chapter 15]. Let G be a finite Abelian group, written multiplicatively. We will have cause to consider the group algebras $R[G]$ for various subrings R of $\mathbb{C}$. The group algebra $R[G]$ is the free R-module with basis given by the elements of G. Multiplication of basis elements σ, τ is defined as $\sigma \cdot \tau = \sigma\tau$, where the product on the right is that of G. The product of arbitrary elements is then defined through the distributive law. If we write 1 for the identity element of G, then $R[G]$ has the structure of an R-algebra through the injection $r \mapsto r \cdot 1$.

If $G = G_1 \times G_2$ is the internal direct product of two Abelian subgroups, there is an isomorphism

$$R\,[G_1]\,[G_2] \cong R[G]$$

given by

$$\sum_{\sigma\in G_2}\left(\sum_{\tau\in G_1} a_{\sigma\tau}\tau\right)\sigma \mapsto \sum_{\sigma\in G_2}\sum_{\tau\in G_1} a_{\sigma\tau}\sigma\tau. \tag{2.3}$$

Every group homomorphism $G \to R^\times$ extends by R-linearity to a homomorphism of R-algebras $R[G] \to R$. This provides a bijection

$$\mathrm{Hom}_{\mathbb{Z}-\mathrm{mod}}\left(G, R^\times\right) \longleftrightarrow \mathrm{Hom}_{R-\mathrm{alg}}\left(R[G], R\right).$$

As a special case, every group homomorphism $G_1 \to G_2$ induces an R-algebra homomorphism $R\left[G_1\right] \to R\left[G_2\right]$.

We shall have need of three such induced R-algebra homomorphisms. First, the map induced by the group homomorphism $G \to R^\times$ sending $\sigma \mapsto 1$ for all elements σ in G is called the augmentation map and will be denoted by ε. The kernel of ε in $R[G]$ is called the augmentation ideal. Now let χ be a complex-valued character of G, and assume that $R^\times$ contains the values of the character χ. The second homomorphism we will consider is the R-algebra homomorphism $R[G] \to \mathbb{C}$ induced by χ. We will abuse notation and refer to this map as χ as well. The third homomorphism is called the twist by χ and will be denoted by t_χ. It is the R-algebra homomorphism $R[G] \to R[G]$ induced by the group homomorphism $G \to R[G]^\times$ such that $\sigma \mapsto \chi(\sigma)\sigma$.

Keeping our previous assumptions, we now assume further that $|G|$ is invertible in R. Then we may define an idempotent in $R[G]$ as in the definition of the equivariant L-functions:

$$e_\chi = \frac{1}{|G|}\sum_{\sigma\in G}\chi\left(\sigma^{-1}\right)\sigma.$$

These idempotents satisfy the following properties:

Properties of idempotents in group algebras.

1. *For all $\sigma \in G$, we have $\sigma e_\chi = \chi(\sigma)e_\chi$.*
2. *For all $\chi, \psi \in \widehat{G}$, we have $e_\chi e_\psi = \delta(\chi,\psi)e_\chi$.*
3. *$\sum_{\chi\in\widehat{G}} e_\chi = 1$.*
4. *For $\chi, \psi \in \widehat{G}$, we have $\chi\left(e_\psi\right) = \delta(\chi,\psi)$.*

5. *The set* $\{ e_\chi | \chi \in \widehat{G} \}$ *is a free* R *basis for* $R[G]$.

6. *If* $G = G_1 \times G_2$, *then a character* χ *on* G *restricts to characters* χ_1 *and* χ_2 *on* G_1 *and* G_2. *Within* $R[G]$, *we have*

$$e_\chi = e_{\chi_1} e_{\chi_2}.$$

Proofs of properties 1 through 5 can be found immediately following [45, Lemma 15.4]. Suppose that G, G_1, and G_2, χ, χ_1, and χ_2 satisfies the assumptions of property 6. Then

$$\begin{aligned} e_\chi &= \frac{1}{|G|} \sum_{\sigma \in G} \chi\left(\sigma^{-1}\right) \sigma \\ &= \frac{1}{|G_1|\,|G_2|} \sum_{\sigma \in G_1} \chi_1\left(\sigma^{-1}\right) \sum_{\tau \in G_2} \chi_2\left(\tau^{-1}\right) \\ &= e_{\chi_1} e_{\chi_2}. \end{aligned}$$

If V is an $R[G]$-module, we set $V^\chi = e_\chi V$. This $R[G]$-submodule is called the χ-th isotypic component of V. It is also characterized by

$$V^\chi = \{ v \in V | \sigma v = \chi(\sigma) v \text{ for all } \sigma \in G \}.$$

The following proposition is fundamental to the theory of Galois module structures in number theory (see [45, Proposition 15.5]):

Proposition 2.3.1. *Let* G *be a finite Abelian group. Let* R *be a subring of* $\mathbb{C}$ *such that* $R^\times$ *contains the roots of unity of order* $|G|$, *as well as the integer* $|G|$. *Let* V *be an* $R[G]$*-module. Then* V *is the direct sum of its isotypic components:*

$$V \cong \bigoplus_{\chi \in \widehat{G}} V^\chi$$

The following lemmas describe the behavior of these idempotents under certain maps between group algebras. We continue to assume that $R^\times$ contains $|G|$ and the values of the characters on G.

Lemma 2.3.2. *Let H be a subgroup of the finite Abelian group G. Let χ be in $\widehat{G}$. Then*

$$\pi\left(e_\chi\right) = \begin{cases} e_\chi, & \text{if } \chi(H) = 1; \\ 0, & \text{otherwise,} \end{cases}$$

where $\pi\colon R[G] \to R[G/H]$ is the map induced by projection. Observe that when $\chi(H) = 1$, χ is being considered as both a character on G and a character on G/H.

Proof. Orthogonality relations. □

Lemma 2.3.3. *Let G be a finite Abelian group, and let $\chi \in \widehat{G}$. For all $\psi \in \widehat{G}$,*

$$t_\chi\left(e_\psi\right) = e_{\chi^{-1}\psi},$$

where t_χ is the twist by χ.

Proof. From the definitions of t_χ and e_ψ, we have

$$\begin{aligned} t_\chi\left(e_\psi\right) &= \frac{1}{|G|}\sum_{\sigma\in G}\psi\left(\sigma^{-1}\right)\chi\left(\sigma\right)\sigma \\ &= \frac{1}{|G|}\sum_{\sigma\in G}\chi^{-1}\psi\left(\sigma^{-1}\right)\sigma \\ &= e_{\chi^{-1}\psi}. \end{aligned}$$

□

We will need a lemma concerning the structure of group algebras $R[G]$ when G is cyclic of order 2^m or $2^m p^n$. Let R be either of the rings $\mathbb{Z}$ or $\mathbb{Q}$.

Lemma 2.3.4. *Assume that G is a cyclic group of order 2^m. Let τ be an element of G of order 2^m. Set $\mathrm{N}_\tau = 1 + \tau^{2^{m-1}}$. Let χ be a complex-valued character on G of order 2^m. Then χ induces an isomorphism*

$$\chi\colon R\left[G\right] / \left(\mathrm{N}_\tau\right) \cong R\left[\zeta_{2^m}\right].$$

Now assume that p is an odd prime number and that G is a cyclic group of order $2^m p^n$. Let σ and τ be elements of G of orders p^n and 2^m respectively. Let N_τ be as above and set $\mathrm{N}_\sigma = \sum_{i=1}^{p-1}\sigma^{ip^{n-1}}$. Let χ be a complex-valued character on G of order $2^m p^n$. Then χ induces an isomorphism

$$\chi\colon R\left[G\right] / \left(\mathrm{N}_\tau, \mathrm{N}_\sigma\right) \cong R\left[\zeta_{2^m p^n}\right].$$

Proof. In either case above, the surjectivity is immediate. Assume first that G has order 2^m. Set $\zeta_{2^m} = \chi(\tau)$. To demonstrate the injectivity, let $\alpha = \sum_{i=0}^{2^m-1} a_i \tau^i$ be an element of $R[G]$ such that $\chi(\alpha) = 0$. Then

$$\begin{aligned}\chi(\alpha) &= \sum_{i=0}^{2^{m-1}-1} a_i \zeta_{2^m}^i + \sum_{i=2^{m-1}}^{2^m-1} a_i \zeta_{2^m}^i \\ &= \sum_{i=0}^{2^{m-1}-1} \left(a_i - a_{i+2^{m-1}}\right) \zeta_{2^m}^i = 0.\end{aligned}$$

Since the numbers $\zeta_{2^m}^i$ for $0 \leq i \leq 2^{m-1}-1$ form an R-module basis for $R[\zeta_{2^m}]$, it follows that $a_i = a_{i+2^{m-1}}$ for $0 \leq i \leq 2^{m-1}-1$. We thus have the factorization

$$\alpha = \mathrm{N}_\tau \sum_{i=0}^{2^{m-1}-1} a_i \tau^i,$$

so the class of α is trivial in $R[G]/(\mathrm{N}_\tau)$.

Now assume that G has order $2^m p^n$. Set $\zeta_{2^m} = \chi(\tau)$ and $\zeta_{p^n} = \chi(\sigma)$. To demonstrate the injectivity, let

$$\alpha = \sum_{i=0}^{p-1} \sum_{j=0}^{p^{n-1}-1} \sum_{k=0}^{2^m-1} a_{ijk} \tau^k \sigma^{ip^{n-1}+j}$$

be an element of $R[G]$ such that $\chi(\alpha) = 0$. Then

$$\sum_{i=0}^{p-1} \sum_{j=0}^{p^{n-1}-1} \sum_{k=0}^{2^m-1} a_{ijk} \zeta_{2^m}^k \zeta_{p^n}^{ip^{n-1}+j} = 0.$$

Subtracting

$$\chi\left(\left(\sum_{j=0}^{p^{n-1}-1} \sum_{k=0}^{2^m-1} a_{(p-1)jk} \tau^k \sigma^j\right) N_\sigma\right) \tag{2.4}$$

gives

$$\sum_{i=0}^{p-2} \sum_{j=0}^{p^{n-1}-1} \sum_{k=0}^{2^m-1} \left(a_{ijk} - a_{(p-1)jk}\right) \zeta_{2^m}^k \zeta_{p^n}^{ip^{n-1}+j} = 0.$$

Since $\zeta_{2^m}^{2^{m-1}} = -1$, we may rewrite this as

$$\sum_{i=0}^{p-2} \sum_{j=0}^{p^{n-1}-1} \sum_{k=0}^{2^{m-1}-1} \left(a_{ijk} - a_{(p-1)jk} - a_{ij(k+2^{m-1})} + a_{(p-1)j(k+2^{m-1})}\right) \zeta_{2^m}^k \zeta_{p^n}^{ip^{n-1}+j} = 0.$$

Now the numbers $\zeta_{2^m}^k \zeta_{p^n}^{ip^{n-1}+j}$ for $0 \leq i \leq p-2$, $0 \leq j \leq p^{n-1}-1$, and $0 \leq k \leq 2^{m-1}-1$ form an R-module basis for $R[\zeta_{2^m p}]$ over R ([38, Chapter 1, Proposition 10.3]). Therefore, each coefficient in the triple sum above is zero, so

$$a_{ijk} - a_{(p-1)jk} = a_{ij(k+2^{m-1})} - a_{(p-1)j(k+2^{m-1})}$$

for each triple of indices i, j, k.

The argument of χ in (2.4) is a multiple of N_σ, and subtracting that argument from α gives

$$\begin{aligned}
&\sum_{i=0}^{p-2} \sum_{j=0}^{p^{n-1}-1} \sum_{k=0}^{2^m-1} \left(a_{ijk} - a_{(p-1)jk}\right) \tau^k \sigma^{ip^{n-1}+j} \\
&= \sum_{i=0}^{p-2} \sum_{j=0}^{p^{n-1}-1} \sum_{k=0}^{2^{m-1}-1} \left(\left(a_{ijk} - a_{(p-1)jk}\right) + \tau^{2^{m-1}} \left(a_{ij(k+2^{m-1})} - a_{(p-1)j(k+2^{m-1})}\right) \right) \tau^k \sigma^{ip^{n-1}+j} \\
&= \left(\sum_{i=0}^{p-2} \sum_{j=0}^{p^{n-1}-1} \sum_{k=0}^{2^{m-1}-1} \left(a_{ijk} - a_{(p-1)jk}\right) \tau^k \sigma^{ip^{n-1}+j} \right) N_\tau.
\end{aligned}$$

Therefore, α is in the ideal $(1+\tau, N_H)$ of $R[G]$. The injectivity of χ follows. □

2.4 Fitting Ideals

Accounts of Fitting ideals can be found in [41, §1.4], [36, Appendix], and [39]. Throughout this section, all rings are commutative with unit element, and a morphism from R_1 to R_2 is understood to take the unit element of R_1 to the unit element of R_2. Furthermore, all modules are assumed to be finitely generated. We will only need to consider the zero-th Fitting ideal of an R-module M, although the concept of higher Fitting ideals does exist. Because of this, we will refer to the zero-th Fitting ideal simply as *the* Fitting ideal $\mathrm{Fit}_R(M)$.

Throughout this work, if R is the ring of integers in a number field, the absolute norm on ideals of R will be denoted by $\mathfrak{N}$. It is the function from the nonzero ideals of R to the positive integers defined by

$$\mathfrak{N}(\mathfrak{a}) = |R/\mathfrak{a}|.$$

It extends to the fractional ideals of R by multiplicativity.

Suppose M has generators $m_1, \ldots, m_n$. Then $\mathrm{Fit}_R(M)$ is the ideal in R generated by the determinants of all $n \times n$ matrices $A = (a_{ij})$ where $a_{ij} \in R$ and $\sum_{i=1}^{n} a_{ij} m_i = 0$ for all j. In other words, the columns of A consist of relations among the generators m_i. We will use the following properties of Fitting ideals:

Properties of Fitting ideals.

1. $\mathrm{Fit}_R(M)$ *is independent of the choice of generators* $m_1, \ldots, m_n$.
2. $\mathrm{Fit}_R(M) \subset \mathrm{Ann}_R(M)$.
3. *For an ideal* I *of* R, $\mathrm{Fit}_R(R/I) = I$.
4. *If* $M_1, \ldots, M_k$ *are* R*-modules, then* $\mathrm{Fit}_R\left(\bigoplus_{i=1}^{k} M_i\right) = \prod_{i=1}^{k} \mathrm{Fit}_R(M_i)$.
5. *If* $f\colon R_1 \to R_2$ *is a surjective homomorphism of rings, and if* M *is a finitely generated module over* R_2*, then* $f(\mathrm{Fit}_{R_1}(M)) = \mathrm{Fit}_{R_2}(M)$.
6. *If* R *is the ring of integers in a number field and* M *is a finite module over* R*, then* $\mathfrak{N}(\mathrm{Fit}_R(M)) = |M|$. *Here, if* $\mathfrak{a}$ *is an ideal of* R, $\mathfrak{N}(\mathfrak{a})$ *denotes the absolute norm* $|R/\mathfrak{a}|$ *of* $\mathfrak{a}$.
7. *If* $M_1 \to M_2$ *is an* R*-module epimorphism, then* $\mathrm{Fit}_R(M_1) \subseteq \mathrm{Fit}_R(M_2)$.

Proof.

(1): It suffices to show that the Fitting ideal computed using generators $m_1, \ldots, m_n$ of M is the same as that computed using generators $m_1, \ldots, m_n, m_{n+1}$ for any m_{n+1} in M. For now, we denote the first of these ideals as $\mathrm{Fit}_n(M)$ and the second as $\mathrm{Fit}_{n+1}(M)$.

Suppose we are given a determinant

$$\begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{vmatrix},$$

whose entries are in R and whose columns satisfy

$$\sum_{j=1}^{n} a_{jr} m_j = 0$$

for all $r = 1, \ldots n$. Since $m_{n+1} \in M$ and $m_1, \ldots m_n$ generate M, we can find $b_1, \ldots, b_n$ in R satisfying

$$m_{n+1} = \sum_{j=1}^{n} b_j m_j. \tag{2.5}$$

Then the columns of the determinant

$$\begin{vmatrix} a_{11} & \ldots & a_{1n} & -b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \ldots & a_{nn} & -b_n \\ 0 & \ldots & 0 & 1 \end{vmatrix}$$

are relations among $m_1, \ldots, m_n, m_{n+1}$. Since the above determinants are equal, it follows that $\mathrm{Fit}_n(M) \subset \mathrm{Fit}_{n+1}(M)$.

For the reverse inclusion, suppose we are given a determinant

$$\begin{vmatrix} a_{11} & \ldots & a_{1(n+1)} \\ \vdots & \ddots & \vdots \\ a_{(n+1)1} & \ldots & a_{(n+1)(n+1)} \end{vmatrix}$$

having entries in R and whose columns satisfy

$$\sum_{j=1}^{n+1} a_{jr} m_j = 0 \tag{2.6}$$

for $r = 1, \ldots n+1$. Let the elements $b_1, \ldots b_n$ be defined by (2.5). Since adding a multiple of the last row to another row leaves the value of the determinant unchanged, the value of the above determinant is equal to that of

$$\begin{vmatrix} a_{11} + b_1 a_{(n+1)1} & \ldots & a_{1(n+1)} + b_1 a_{(n+1)(n+1)} \\ \vdots & \ddots & \vdots \\ a_{n1} + b_n a_{(n+1)1} & \ldots & a_{n(n+1)} + b_n a_{(n+1)(n+1)} \\ a_{(n+1)1} & \ldots & a_{(n+1)(n+1)} \end{vmatrix}.$$

Expanding this determinant along the last row gives

$$\pm \sum_{r=1}^{n+1} (-1)^r \, a_{(n+1)r} A_r, \tag{2.7}$$

where A_r is the determinant of a matrix whose columns have the form

$$\begin{bmatrix} a_{1s} + b_1 a_{(n+1)s} \\ \vdots \\ a_{ns} + b_n a_{(n+1)s} \end{bmatrix}.$$

Taking a linear combination of $m_1, \ldots, m_n$ with coefficients given by the entries in this vector gives

$$\sum_{j=1}^{n} a_{js} m_j + a_{(n+1)s} \sum_{j=1}^{n} b_j m_j = \sum_{j=1}^{n} a_{js} m_j + a_{(n+1)s} m_{n+1} = 0,$$

where the last equality follows from (2.6). Thus, each determinant A_r in (2.7) is an element of $\mathrm{Fit}_n(M)$, and hence the original determinant is as well. This shows the reverse containment, so $\mathrm{Fit}_n(M) = \mathrm{Fit}_{n+1}(M)$.

(2): Let $m_1, \ldots, m_n$ be generators for the R-module M. Suppose we are given an $n \times n$ matrix $A = (a_{ij})$ whose entries are in R and whose columns satisfy

$$\sum_{j=1}^{n} a_{jr} m_j = 0$$

for $r = 1, \ldots n$. Multiplying the equation

$$A^T \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = 0$$

by the adjoint of A^{T} shows that $\det(A) m_r = 0$ for $r = 1, \ldots n$. Hence, $\det(A)$ is in $\mathrm{Ann}(M)$, and so $\mathrm{Fit}(M) \subset \mathrm{Ann}(M)$.

(3): The relations on the generator $\overline{1}$ of R/I are $r \cdot \overline{1} = 0$ for $r \in I$.

(4): It suffices to prove that if M and N are finitely generated R-modules, then $\mathrm{Fit}_R(M \oplus N) = \mathrm{Fit}_R(M)\,\mathrm{Fit}_R(N)$. Let $m_1, \ldots, m_s$ be generators for M, and let $n_1, \ldots, n_t$ be generators for N. Then $m_1, \ldots m_s, n_1, \ldots n_t$ are generators for $M \oplus N$.

Let $A = (a_{ij})$ be an $s \times s$ matrix with entries in R whose columns satisfy

$$\sum_{i=1}^{s} a_{ir} m_i = 0$$

for all $r = 1, \ldots, s$, and let $B = (b_{ij})$ be a $t \times t$ matrix with entries in R whose columns satisfy

$$\sum_{i=1}^{t} b_{ir} n_i = 0$$

for all $r = 1, \ldots, t$. Then the columns of the $(s+t) \times (s+t)$ matrix

$$C = (c_{ij}) = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

satisfy

$$\sum_{i=1}^{s} c_{ir} m_i + \sum_{i=s+1}^{s+t} c_{ir} n_i = 0$$

for $r = 1, \ldots, s+t$. Thus, $\det(C) = \det(A)\det(B)$ is contained in $\mathrm{Fit}_R(M \oplus N)$, and hence, $\mathrm{Fit}_R(M)\,\mathrm{Fit}_R(N) \subset \mathrm{Fit}_R(M \oplus N)$.

For the reverse inclusion, we relabel the above generators of $M \oplus N$ as

$$m_1, \ldots m_s, n_{s+1}, \ldots n_{s+t}.$$

Let $C = (c_{ij})$ be an $(s+t) \times (s+t)$ matrix with entries in R whose columns are relations on $m_1, \ldots, m_s, n_{s+1}, \ldots, n_{s+t}$. Explicitly, the entries satisfy

$$\sum_{i=1}^{s} c_{ir} m_i + \sum_{i=s+1}^{s+t} c_{ir} n_i = 0 \tag{2.8}$$

for $r = 1, \ldots, s+t$.

We will calculate $\det(C)$ using Laplace's expansion of the determinant using the rows indexed by $1, 2, \ldots, s$ (see, for example, [40, p. 92, equation 5.3.7]). Fix a sequence $K = (k_1, \ldots, k_s)$ of p integers satisfying

$$1 \leq k_1 < k_2 < \ldots < k_s \leq s+t.$$

Let $\tilde{K} = \left(\tilde{k}_1, \ldots, \tilde{k}_t\right)$ be the sequence obtained from $(1, 2, \ldots, s+t)$ by deleting the terms that belong to K. For such sequences, we define

$$D_K = \begin{vmatrix} c_{1k_1} & c_{1k_2} & \ldots & c_{1k_s} \\ c_{2k_1} & c_{2k_2} & \ldots & c_{2k_s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{sk_1} & c_{sk_2} & \ldots & c_{sk_s} \end{vmatrix}$$

and

$$D_{\tilde{K}} = \begin{vmatrix} c_{(s+1)\tilde{k}_1} & \cdots & c_{(s+1)\tilde{k}_t} \\ \vdots & \ddots & \vdots \\ c_{(s+t)\tilde{k}_1} & \cdots & c_{(s+t)\tilde{k}_t} \end{vmatrix}.$$

Laplace's expansion using the rows indexed by $1, 2, \ldots, s$ is

$$\det(C) = \sum_K \varepsilon_K D_K D_{\tilde{K}}, \tag{2.9}$$

where the sum is over all possible sequences K as defined above and the coefficients ε_K are all equal to either 1 or -1.

Since the sets $\{ m_1, \ldots, m_s \}$ and $\{ n_1, \ldots, n_t \}$ are respectively sets of generators of M and N, the relation (2.8) splits into the relations

$$\sum_{i=1}^{s} c_{ir} m_i = 0$$

and

$$\sum_{i=s+1}^{s+t} c_{ir} n_i = 0.$$

The columns in each determinant D_K are the coefficients in the first relation above as r runs through the indices in K. The columns in each determinant $D_{\tilde{K}}$ are the coefficients in the second relation as r runs through the indices in $\tilde{K}$. Thus, each determinant D_K is in $\mathrm{Fit}_R(M)$, and each determinant $D_{\tilde{K}}$ is in $\mathrm{Fit}_R(N)$. It follows that the right side of the equation (2.9) is in $\mathrm{Fit}_R(M)\,\mathrm{Fit}_R(N)$. Since C was an arbitrary matrix with columns giving relations on generators of $M \oplus N$, we find that $\mathrm{Fit}_R(M \oplus N) \subset \mathrm{Fit}_R(M)\,\mathrm{Fit}_R(N)$.

(5): If $m_1, \ldots, m_n$ is a set of generators for M as a module over R_2, then it is also a set of generators for M as a module over R_1 since f is surjective. Let A be

an $n \times n$ matrix with entries in R_1. The columns of A are relations on $m_1, \ldots, m_n$ when M is considered as an R_1 module if and only if the columns of $f(A)$ are relations on $m_1, \ldots m_n$ when M is considered as an R_2 module. Since

$$\det\left(f(A)\right) = f\left(\det(A)\right)$$

it follows that $f\left(\mathrm{Fit}_{R_1}(M)\right) \subset \mathrm{Fit}_{R_2}(M)$. To see the reverse containment, let

$$d = \sum_{i=1}^{k} r_i d_i$$

be an element of $\mathrm{Fit}_{R_2}(M)$, where each r_i is in R_2 and each d_i is the determinant of a matrix A_i of relations on some fixed generators of M. Since f is surjective, there exist elements $\tilde{r}_i$ in R_1 such that $f\left(\tilde{r}_i\right) = r_i$ for $i = 1, \ldots, k$. Also, there exist matrices $\tilde{A}_i$ with entries in R_1 such that $f\left(\tilde{A}_i\right) = A_i$ for $i = 1, \ldots, k$. Let $\tilde{d}_i$ be the determinant of the matrix A_i. Then by the above discussion, $\mathrm{Fit}_{R_1}(M)$ contains each $\tilde{d}_i$ and hence contains

$$\tilde{d} = \sum_{i=1}^{k} \tilde{r}_i \tilde{d}_i,$$

Since $f\left(\tilde{d}\right) = d$, the proof is complete.

(6): By the Primary Decomposition Theorem from Section 2.1, we can write

$$M \cong \bigoplus_{\mathfrak{p} \in I_R} \left(R/\mathfrak{p}^{e(\mathfrak{p},1)} \oplus R/\mathfrak{p}^{e(\mathfrak{p},2)} \oplus \cdots \oplus R/\mathfrak{p}^{e(\mathfrak{p},l(\mathfrak{p}))} \right).$$

The Fitting ideal of a module is an isomorphism invariant. Therefore, from properties 3 and 4 above, we have

$$\mathrm{Fit}_R(M) = \prod_{\mathfrak{p} \in I_R} \mathfrak{p}^{\sum_{i=1}^{l(\mathfrak{p})} e(\mathfrak{p},i)}.$$

Therefore,

$$\begin{aligned}
\mathfrak{N}\left(\mathrm{Fit}_R(M)\right) &= \prod_{\mathfrak{p} \in I_R} \prod_{i=1}^{l(\mathfrak{p})} \mathfrak{N}\left(\mathfrak{p}^{e(\mathfrak{p},i)}\right) \\
&= \prod_{\mathfrak{p} \in I_R} \prod_{i=1}^{l(\mathfrak{p})} \left| R/\mathfrak{p}^{e(\mathfrak{p},i)} \right| \\
&= |M|.
\end{aligned}$$

(7): This follows from the fact that the images in M_2 of a set of generators for M_1 are a set of generators for M_2. □

The following lemma will be important when working with groups of roots of unity.

Lemma 2.4.1. *Let R be the ring of integers in a number field, and let M be an R-module with finite cardinality that is cyclic as a $\mathbb{Z}$-module. Let p be a prime number, and let A_p denote the factor of the ideal $\mathrm{Ann}_R(M)$ supported at primes dividing p. Let p^t be the exact power of p dividing $|M|$. Then there exists a prime ideal $\mathfrak{P}$ in R dividing p and of residual degree 1 over $\mathbb{Q}$ such that*

$$A_p = \mathfrak{P}^t.$$

Proof. If M is cyclic as a $\mathbb{Z}$-module, then the p-part M_p of M must have the form $R/\mathfrak{P}^e$ for some prime ideal $\mathfrak{P}$ of R dividing p, hence $A_p = \mathfrak{P}^e$. The module $R/\mathfrak{P}$ is isomorphic to a quotient of M_p, hence is cyclic as a $\mathbb{Z}$-module. It is therefore cyclic as a $\mathbb{Z}/p\mathbb{Z}$-module, so that

$$R/\mathfrak{P} \cong \mathbb{Z}/p\mathbb{Z}.$$

It follows that $\mathfrak{P}$ has residual degree 1 over $\mathbb{Q}$ and $e = t$. □

2.5 Kummer Theory

References for this material are [4, Chapter III, §2] and [33, Chapter XI, §1]. Let k be a number field containing μ_n, the group of nth roots of unity. The following is the main theorem of Kummer theory.

Theorem 2.5.1. *There is a lattice isomorphism between the lattice of Abelian extensions K/k such that $\mathrm{Gal}(K/k)$ has exponent dividing n (Kummer extensions) and the lattice of subgroups Δ of $k^\times$ such that $k^{\times n} \subset \Delta \subset k^\times$. Given a subgroup Δ, the corresponding extension K_Δ of k is defined by*

$$K_\Delta = k\left(\sqrt[n]{\Delta}\right).$$

Conversely, given a Kummer extension K_Δ/k, the corresponding subgroup of $k^\times$ is

$$\Delta = K_\Delta^{\times n} \cap k^\times.$$

If $G = \mathrm{Gal}\,(K_\Delta/k)$, then there is a perfect pairing

$$G \times \Delta/k^{\times n} \to \mu_n,$$

called the Kummer pairing. It is given by

$$\left(\sigma, \overline{\delta}\right) \mapsto \frac{\sigma \sqrt[n]{\delta}}{\sqrt[n]{\delta}}.$$

This pairing induces an isomorphism of each one of G and $\Delta/k^{\times n}$ with the Pontryagin dual group of the other.

In addition, it can be shown that a *cyclic* extension of k of degree m dividing n is generated by the mth root of a single element of k. In other words, the corresponding group Δ can be written as

$$\Delta = k^{\times n} \cdot \langle \gamma \rangle$$

for some element γ in $k^\times$.

We will also need some information about the behavior of prime ideals in a Kummer extension.

Proposition 2.5.2. *Let p be a prime number and let k be a number field containing the pth roots of unity. Let $\mathfrak{q}$ be a prime ideal of k relatively prime to p. Let α be in $k^\times$. Then $\mathrm{ord}_\mathfrak{q}(\alpha)$ is divisible by p if, and only if, $\mathfrak{q}$ is unramified in $k\left(\sqrt[p]{\alpha}\right)/k$.*

For the proof of a stronger result for general Kummer extensions , see [12, Chapter I, Theorem 6.3].

2.6 Class field theory

We will only need a small amount of class field theory for number fields. The version involving generalized ideal class groups will be sufficient for our purposes. A reference for this material is [28].

2.6.1 The Artin map

Let K/k be a Galois extension of number fields with Galois group G. Let $\mathfrak{P}$ be a prime ideal of K lying above the prime ideal $\mathfrak{p}$ of k. We will denote the ring of integers in K by $\mathcal{O}_K$, the absolute norm of $\mathfrak{p}$ by $\mathfrak{N}\mathfrak{p}$, and the decomposition and inertia groups of $\mathfrak{P}$ over k by $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ respectively. There exists a unique coset mod $I_{\mathfrak{P}}$ in $\mathfrak{D}_{\mathfrak{P}}$ such that any σ in the coset satisfies

$$\sigma\alpha \equiv \alpha^{\mathfrak{N}\mathfrak{p}} \pmod{\mathfrak{P}},$$

for all α in $\mathcal{O}_K$. This coset generates the quotient group $D_{\mathfrak{P}}/I_{\mathfrak{P}}$. Any element of this coset will be called a Frobenius automorphism of $\mathfrak{P}$, and will be denoted by $(\mathfrak{P}, K/k)$. These automorphisms already appeared in the definition (1.2). When $\mathfrak{P}$ is unramified over $\mathfrak{p}$, this coset consists of a single automorphism. Now let σ be an arbitrary element of G. Then we have

$$(\mathfrak{P}^{\sigma}, K/k) = \sigma\,(\mathfrak{P}, K/k)\,\sigma^{-1}.$$

When $\mathfrak{p}$ ramifies in K/k, this relation says that the automorphism on the right is a Frobenius automorphism of $\mathfrak{P}$.

Assume further that K/k is an Abelian extension. The above relation shows that if $\mathfrak{p}$ is a prime ideal of k, unramified in K, then the Frobenius automorphisms of all of the prime ideals lying above $\mathfrak{p}$ are identical. In this case, we refer to *the* Frobenius automorphism of $\mathfrak{p}$. It will be denoted either by $(\mathfrak{p}, K/k)$ or by $\sigma_{\mathfrak{p}}$. It is characterized by the congruence

$$\sigma_{\mathfrak{p}}\alpha \equiv \alpha^{\mathfrak{N}\mathfrak{p}} \pmod{\mathfrak{p}\mathcal{O}_K}$$

for all α in $\mathcal{O}_K$.

We now extend the map

$$\mathfrak{p} \mapsto (\mathfrak{p}, K/k)$$

by multiplicativity to the subgroup of the ideal group $I_{K/k}$ of k comprising the ideals supported above primes that are unramified in K. Thus, if $\mathfrak{a}$ is such an ideal, and its prime decomposition is

$$\mathfrak{a} = \prod \mathfrak{p}^{e_{\mathfrak{p}}},$$

we then define

$$(\mathfrak{a}, K/k) = \prod (\mathfrak{p}, K/k)^{e_\mathfrak{p}} .$$

We call $(\mathfrak{a}, K/k)$ the Artin symbol of $\mathfrak{a}$, and the map

$$\mathfrak{a} \mapsto (\mathfrak{a}, K/k)$$

is called the Artin map for K/k.

The Artin symbol satisfies the following properties (see [33, p. 198]):

Properties of the Artin symbol.

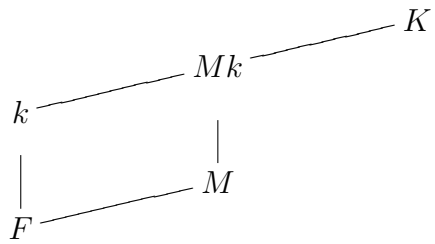
1. *Let $\sigma\colon K \to \sigma K$ be an isomorphism of number fields. Then for any fractional ideal $\mathfrak{a}$ in $I_{K/k}$,*
$$(\sigma\mathfrak{a}, \sigma K/\sigma k) = \sigma\,(\mathfrak{a}, K/k)\,\sigma^{-1}.$$

2. *Let $k \subset K \subset K'$ be a bigger Abelian extension, and let $\mathfrak{a}$ be an ideal in $I_{K'/k}$. Then*
$$\mathrm{Res}_K\,(\mathfrak{a}, K'/k) = (\mathfrak{a}, K/k)\,.$$

3. *Let K/k be Abelian and let E/k be finite. Let $\mathfrak{p}$ be a prime ideal in k unramified in K, and let $\mathfrak{P}$ be a prime ideal of E lying above $\mathfrak{p}$. Then*
$$\mathrm{Res}_K\,(\mathfrak{P}, KE/E) = \left(N_{E/k}\mathfrak{P}, K/k\right).$$
In particular, if $k \subset E \subset K$, then
$$(\mathfrak{P}, K/E) = \left(N_{E/k}\mathfrak{P}, K/k\right)$$

The following lemma is an immediate consequences of these properties:

Lemma 2.6.1. *Suppose that F, k, M, and K are number fields as in the following diagram.*



Assume that K/k and M/F are Abelian. (We do not assume that $M \cap k = F$). Let $\mathfrak{P}$ be a prime ideal of k, unramified in K/k. Suppose that the prime ideal of F divisible by $\mathfrak{P}$ is unramified in M. Then

$$(\mathfrak{p}, K/k)\Big|_M = \left(\mathrm{N}_{k/F}\,\mathfrak{p}, M/F\right).$$

2.6.2 Class fields

Let k be a number field. A modulus $\mathfrak{f} = \mathfrak{f}_0\mathfrak{f}_\infty$ of k is a formal product consisting of an integral ideal $\mathfrak{f}_0$ and a formal product of distinct real infinite places $\mathfrak{f}_\infty$. If α is in $k^\times$, we write $\alpha \equiv 1 \bmod^* \mathfrak{f}$ to mean that α has the following two properties:

1. If $\mathfrak{p}$ is a prime ideal of k with normalized valuation $v_\mathfrak{p}$, and if $\mathrm{ord}_\mathfrak{p}(\mathfrak{f}_0) > 0$, then $v_\mathfrak{p}(\alpha) \geq 0$ and
$$\alpha \equiv 1 \pmod{\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathfrak{f}_0)}}.$$

2. If v is a real place of k dividing $\mathfrak{f}_\infty$ and σ_v is the corresponding embedding of k in $\mathbb{R}$, then
$$\sigma_v\,\alpha > 0.$$

Let $I(\mathfrak{f})$ denote the group of nonzero fractional ideals of k that are relatively prime to $\mathfrak{f}_0$, and let $P_\mathfrak{f}$ denote the subgroup of $I(\mathfrak{f})$ consisting of the principal fractional ideals (α) where $\alpha \equiv 1 \bmod^* \mathfrak{f}$. Then $I(\mathfrak{f})/P_\mathfrak{f}$ is a finite group, called the ray class group modulo $\mathfrak{f}$. We denote the modulus where $\mathfrak{f}_0 = (1)$ and $\mathfrak{f}_\infty$ is devoid of places by 1. The ray class group modulo 1 is isomorphic to Cl_k, the class group of k. If $\mathfrak{f}$ and $\mathfrak{f}'$ are two moduli, then we say that $\mathfrak{f}$ divides $\mathfrak{f}'$ if $\mathfrak{f}_0$ divides $\mathfrak{f}'_0$ and each factor of $\mathfrak{f}_\infty$ is also a factor of $\mathfrak{f}'_\infty$. Under these assumptions, the ray class group modulo $\mathfrak{f}'$ maps surjectively onto the ray class group modulo $\mathfrak{f}$ by sending the class of an ideal in $I(\mathfrak{f}')$ to the class of the same ideal considered as an element of $I(\mathfrak{f})$.

We can now state the main theorems of class field theory.

Theorem 2.6.2. *Let K/k be an Abelian extension of number fields. Then there exists a minimal modulus $\mathfrak{f}$ (called the conductor of K/k) such that:*

1. *The places of k that ramify in K/k are precisely those that divide $\mathfrak{f}$.*

2. *If $\mathfrak{m}$ is a modulus with $\mathfrak{f}$ dividing $\mathfrak{m}$, then there exists a subgroup H with $P_{\mathfrak{m}} \subseteq H \subseteq I(\mathfrak{m})$ such that the Artin map induces an isomorphism*

$$I(\mathfrak{m})/H \cong \mathrm{Gal}(K/k).$$

Theorem 2.6.3. *Let $\mathfrak{m}$ be a modulus of k and let H be a subgroup of $I(\mathfrak{m})$ with $P_{\mathfrak{m}} \subseteq H \subseteq I(\mathfrak{m})$. Then there exists a unique finite Abelian extension K/k, ramified only at places dividing $\mathfrak{m}$ (although not necessarily at* all *places dividing $\mathfrak{m}$), such that the Artin map induces an isomorphism*

$$I(\mathfrak{m})/H \cong \mathrm{Gal}(K/k).$$

When $H = P_{\mathfrak{m}}$, the Abelian extension given by the above theorem is called the ray class field of k modulo $\mathfrak{m}$, and will be denoted by $k(\mathfrak{m})$. The Galois group $\mathrm{Gal}(k(\mathfrak{m})/k)$ is isomorphic to the ray class group modulo $\mathfrak{m}$. The ray class field modulo 1 is called the Hilbert class field of k, denoted H_k. It is the maximal unramified Abelian extension of k. The Galois group $\mathrm{Gal}(H_k/k)$ is isomorphic to Cl_k.

2.7 Group extensions

This section will provide some results concerning the concepts of the previous sections within the context of a group extension. A reference for the theory of group extensions is [19, Chapter 15].

We will say that a group G is an extension of a group N by another group H if N is a normal subgroup of G and $H \cong G/N$. We shall only be concerned with extensions where N is Abelian. For each h in H, we choose a representative $\tilde{h}$ in G whose coset $\tilde{h}N$ corresponds to h. The map $f_h \colon x \mapsto \tilde{h}x\tilde{h}^{-1}$ is an automorphism of N for each $\tilde{h}$. Since N is Abelian, f_h is independent of the representative $\tilde{h}$ chosen, and the map $H \to \mathrm{Aut}(N)$ given by $h \mapsto f_h$ is a well-defined group homomorphism. Each map f_h extends by $\mathbb{Z}$-linearity to a ring automorphism of the group ring $\mathbb{Z}[N]$, also denoted f_h.

Our first result concerns Fitting ideals.

Proposition 2.7.1. *Assume that M is a left $\mathbb{Z}[G]$-module which is finitely generated as a $\mathbb{Z}[N]$-module. For each h in H, $f_h\left(\mathrm{Fit}_{\mathbb{Z}[N]}(M)\right) = \mathrm{Fit}_{\mathbb{Z}[N]}(M)$.*

Proof. Let $m_1, \ldots, m_n$ be a set of generators of M as a $\mathbb{Z}[N]$-module. We shall first show that for each h in H, the elements $\tilde{h}m_1, \ldots, \tilde{h}m_n$ are also a set of generators of M as a $\mathbb{Z}[N]$-module. If m is in M, then we can write

$$\tilde{h}^{-1}m = \sum_{i=1}^{n} b_i m_i,$$

where each element b_i is in $\mathbb{Z}[N]$. Then

$$m = \sum_{i=1}^{n} \left(\tilde{h}b_i\tilde{h}^{-1}\right)\tilde{h}m_i,$$

and the coefficients $\tilde{h}b_i\tilde{h}^{-1}$ are in $\mathbb{Z}[N]$.

Now let $A = (a_{ij})$ be an $n \times n$ matrix with entries in $\mathbb{Z}[N]$ and columns satisfying

$$\sum_{j=1}^{n} a_{jr}m_j = 0$$

for $r = 1, \ldots n$. Then

$$f_h\left(\det(A)\right) = \begin{vmatrix} \tilde{h}a_{11}\tilde{h}^{-1} & \ldots & \tilde{h}a_{1n}\tilde{h}^{-1} \\ \vdots & \ddots & \vdots \\ \tilde{h}a_{n1}\tilde{h}^{-1} & \ldots & \tilde{h}a_{nn}\tilde{h}^{-1} \end{vmatrix}.$$

Each column of this matrix provides a relation on the generators $\tilde{h}m_i$, since

$$\sum_{i=1}^{n} \left(\tilde{h}a_{ir}\tilde{h}^{-1}\right)\tilde{h}m_i = \tilde{h}\left(\sum_{i=1}^{n} a_{ir}m_i\right) = 0$$

for $r = 1, \ldots, n$. Thus, by the first property of Fitting ideals in Section 2.4, f_h maps $\mathrm{Fit}_{\mathbb{Z}[N]}(M)$ into itself, and $f_{h^{-1}}$ is an inverse for this map. □

We now turn to Kummer theory. Recall that if K is a number field containing the nth roots of unity μ_n, then the Abelian extensions of K having Galois groups with exponents dividing n are completely understood through Kummer theory. If

K is an Abelian extension of k with Galois group G, the next result determines when a Kummer extension L of K is Galois over k. A classification of when L is central over K is in [10].

Proposition 2.7.2. *Let K/k be an Abelian extension of number fields with Galois group G, and assume that K contains the nth roots of unity. Let Δ be a subgroup of $K^\times$ such that $K^{\times n} \subset \Delta \subset K^\times$. Then $L = K\left(\sqrt[n]{\Delta}\right)$ is Galois over k if and only if Δ is a sub $\mathbb{Z}[G]$-module of $K^\times$.*

Proof. Assume that L/k is Galois. Let σ be in G, let δ be in Δ, and choose a lift $\tilde{\sigma}$ of σ to $\mathrm{Gal}(L/k)$. If η is an nth root of δ, then η is in L. By hypothesis, $\eta^{\tilde{\sigma}}$ is also in L. If δ^σ were not in Δ, then under the correspondence in Theorem 2.5.1, $\langle \Delta, \delta^\sigma \rangle$ would belong to a strictly larger field than L. As $\eta^{\tilde{\sigma}}$ is in L, this is not the case.

Assume now that Δ is a $\mathbb{Z}[G]$-submodule of $K^\times$. Let η be an nth root of some δ in Δ, so η is in L. If $\mathfrak{L}$ is a normal closure of L/k and $\tilde{\sigma}$ is in $\mathrm{Gal}(\mathfrak{L}/k)$, then $\tilde{\sigma}$ restricts to some σ in G. Then $\eta^{\tilde{\sigma}}$ is an nth root of δ^σ, which is in Δ by hypothesis. Thus, $\eta^{\tilde{\sigma}}$ is in L. Since L/K is generated by nth roots of elements of Δ, every automorphism in $\mathrm{Gal}(\mathfrak{L}/k)$ maps L onto L. Therefore, L/k is Galois. □

With notation and assumptions as in the proposition, $\mathrm{Gal}(L/k)$ is a group extension of $\mathrm{Gal}(L/K)$. Hence, $\mathrm{Gal}(L/K)$ has the structure of a $\mathbb{Z}[G]$-module. Furthermore, the three groups Δ, $K^{\times n}$, and μ_n appearing in the Kummer pairing, are all $\mathbb{Z}[G]$-submodules of $K^\times$. The next result shows that this pairing, and the homomorphisms it induces, are Galois equivariant.

Proposition 2.7.3. *With notation and assumptions as in the preceding proposition, the Kummer pairing*

$$\phi\colon\ \mathrm{Gal}(L/K) \times \Delta/K^{\times n} \to \mu_n$$

is Galois equivariant. Specifically, if g is in G, σ is in $\mathrm{Gal}(L/K)$, and $\overline{\delta}$ is in $\Delta/K^{\times n}$, then

$$\phi\left(\left(g\cdot\sigma, g\cdot\overline{\delta}\right)\right) \mapsto g\cdot\phi\left(\left(\sigma,\overline{\delta}\right)\right),$$

Furthermore, the group isomorphisms

$$\psi_1 \colon \operatorname{Gal}(L/K) \cong \operatorname{Hom}\left(\Delta/K^{\times n}, \mu_n\right)$$

and

$$\psi_2 \colon \Delta/K^{\times n} \cong \operatorname{Hom}\left(\operatorname{Gal}(L/K), \mu_n\right)$$

induced by the Kummer pairing become homomorphisms of $\mathbb{Z}[G]$-modules if the Hom groups are endowed with $\mathbb{Z}[G]$-module structures by letting an element g in G act as

$$(gf)(x) = gf(g^{-1}x)$$

in either case.

Proof. Choose g in G, σ in $\operatorname{Gal}(L/K)$, and δ in Δ representing the class $\overline{\delta}$ in $\Delta/K^{\times n}$. Let $\tilde{g}$ in $\operatorname{Gal}(L/k)$ be a lift of g. By direct calculation:

$$\begin{aligned}
\phi\left(\left(g\cdot\sigma, g\cdot\overline{\delta}\right)\right) &= \phi\left(\left(\tilde{g}\sigma\tilde{g}^{-1}, g\cdot\overline{\delta}\right)\right) \\
&= \frac{\tilde{g}\sigma\tilde{g}^{-1}\cdot\sqrt[n]{g\delta}}{\sqrt[n]{g\delta}} \\
&= \tilde{g}\,\frac{\sigma\left(\tilde{g}^{-1}\sqrt[n]{g\delta}\right)}{\tilde{g}^{-1}\sqrt[n]{g\delta}} \\
&= \tilde{g}\phi\left(\left(\sigma, \overline{\delta}\right)\right),
\end{aligned}$$

since $\phi\left(\left(\sigma, \overline{\delta}\right)\right)$ does not depend on which nth root of δ is chosen. As $\phi\left(\left(\sigma\overline{\delta}\right)\right)$ is in K, the first assertion follows.

With the same notation, for each $\overline{\delta}$ in $\Delta/K^{\times n}$, we have

$$\begin{aligned}
\psi_1(g\cdot\sigma)\left(\overline{\delta}\right) &= \phi\left(\left(g\cdot\sigma, \overline{\delta}\right)\right) \\
&= g\phi\left(\left(\sigma, g^{-1}\overline{\delta}\right)\right) \\
&= (g\cdot\psi_1(\sigma))(\overline{\delta}),
\end{aligned}$$

where the second equality follows from the Galois equivariance of ϕ. The Galois equivariance of ψ_2 follows by a similar argument. □

We will need the following Kummer-theoretic lemma in Chapter 6. Let K/k be an Abelian extension of number fields with Galois group G. Let $W_K = |\mu_K|$ be the

cardinality of the group of roots of unity in K. Let n be a divisor of W. Suppose that ε is an element of $k^\times$ whose W_Kth root generates a cyclic extension of K of degree n. Fix a W_Kth root η of ε. By Proposition 2.7.2, $K(\eta)$ is a Galois extension of k. Let $\tilde{G} = \mathrm{Gal}(K(\eta)/k)$ and let $H = \mathrm{Gal}(K(\eta)/K)$. Then $\tilde{G}$ is an extension of H by G, so G acts on H as at the beginning of this section. The elements of G act as homomorphisms of H, giving H the structure of a $\mathbb{Z}[G]$ module.

Lemma 2.7.4. *With notation as above,*

$$\mathrm{Ann}_{\mathbb{Z}[G]}\,\mu_K \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}\,H.$$

Proof. First, we will show that each element σ in G has a lift $\tilde{\sigma}$ of σ in $\tilde{G}$ such that

$$\tilde{\sigma}\eta = \eta.$$

Fix an nth root of unity ζ_n. Choose an element σ in G, and let $\tilde{\sigma}$ be an arbitrary lift of σ to $\tilde{G}$. Since ε is fixed by σ, there is an integer a such that

$$\tilde{\sigma}\eta = \zeta_n^a\eta.$$

Since $|H| = n$, there exists an element τ in H such that $\tau\eta = \zeta_n^{-a}\eta$. The element $\tau\tilde{\sigma}$ is then a lift of σ to $\tilde{G}$ satisfying

$$\tau\tilde{\sigma}\eta = \tau\zeta_n^a\eta = \zeta_n^a\zeta_n^{-a}\eta = \eta.$$

Each element σ of G acts on H by choosing an arbitrary lift $\tilde{\sigma}$ of σ in $\tilde{G}$ and conjugating H by $\tilde{\sigma}$. For each element σ in G, let us choose the lift $\tilde{\sigma}$ satisfying

$$\tilde{\sigma}\eta = \eta.$$

Also, for each element σ in G, choose a representative b_σ in $\mathbb{Z}$ of the image of σ under the homomorphism

$$G \to (\mathbb{Z}/n\mathbb{Z})^\times \tag{2.10}$$

giving the action of elements of G on the nth roots of unity. Let τ be an element in H, and let a be an integer such that

$$\tau(\eta) = \zeta_n^e\eta.$$

We find that for an arbitrary integer c,

$$\begin{aligned}\tilde{\sigma}\tau\tilde{\sigma}^{-1}\left(\zeta_n^c\eta\right) &= \tilde{\sigma}\tau\left(\zeta_n^{b_\sigma^{-1}c}\,\eta\right)\\ &= \tilde{\sigma}\left(\zeta_n^{b_\sigma^{-1}c}\zeta_n^e\eta\right)\\ &= \zeta_n^{c+b_\sigma e}\eta.\end{aligned}$$

Therefore, we find inductively that the action of an element $\alpha = \sum_{\sigma\in G} a_\sigma\sigma$ in $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)$ on τ is given by

$$\begin{aligned}(\alpha\cdot\tau)(\eta) &= \prod_{\sigma\in G}\left(\tilde{\sigma}\tau\tilde{\sigma}^{-1}\right)^{a_\sigma}(\eta)\\ &= \zeta_n^{\left(\sum_\sigma a_\sigma b_\sigma\right)e}\eta\\ &= (\alpha\cdot\zeta_n^e)\,\eta\\ &= \eta.\end{aligned}$$

Therefore, $\alpha\cdot\tau$ is the identity element of H for all τ.

□

Next, we give a result concerning class field theory. If K is a number field with class group Cl_K, then the p-primary part of Cl_K is a quotient group of Cl_K, and so corresponds through class field theory to a subextension H_K^p of the Hilbert class field of K. This field will be called the p-Hilbert class field of K.

Proposition 2.7.5. *If K/k is a Galois extension of number fields with Galois group G, p is a prime number, and H_K^p denotes the p-Hilbert class field of K, then H_K^p is a Galois extension of k. It follows that $\mathrm{Gal}(H_K^p/k)$ is a group extension of $\mathrm{Gal}(H_K^p/K)$, and hence $\mathrm{Gal}(H_K^p/K)$ is a $\mathbb{Z}[G]$-module. Denoting the p-primary part of Cl_K by Cl_K^p, the isomorphism of Theorem 2.6.2*

$$\phi\colon \mathrm{Cl}_K^p \cong \mathrm{Gal}(H_K^p/K)$$

given by the Artin map is an isomorphism of $\mathbb{Z}[G]$-modules.

Proof. Consider an algebraic closure $\mathbb{C}$ of k containing H_K^p. If σ is an embedding $\sigma\colon H_K^p\to\mathbb{C}$ that fixes k, then the image σH_K^p is an unramified Abelian p-extension

of $\sigma K = K$. Furthermore, $[\sigma H_K^p : K] = [H_K^p : K]$. Since H_K^p is the unique maximal unramified Abelian p-extension of K, $\sigma H_K^p = H_K^p$. The first assertion follows.

Let $H^p = \mathrm{Gal}\,(H_K^p/K)$. Let $\mathfrak{a}$ be a fractional ideal of K representing a class in Cl_K^p, and let σ be in G. Using property 1 of the Artin symbol in Section 2.6, we have

$$\phi\,(\sigma \cdot \overline{\mathfrak{a}}) = (\mathfrak{a}^\sigma, H_K^p/K) = \sigma\,(\mathfrak{a}, H_K^p/K)\,\sigma^{-1} = \sigma \cdot \phi\,(\overline{\mathfrak{a}})\,.$$

□

When an extension is both a Kummer extension and unramified, there is interplay between the previous results. As a first example, we present the following proposition. As usual, K/k is an Abelian extension of number fields with Galois group G, and N_G denotes the norm in $\mathbb{Z}[G]$.

Proposition 2.7.6. *Let p be a prime number. Assume that the p-Hilbert class field H_K^p of K is a cyclic extension of K of order n. Let μ_K be the group of roots of unity in K. Suppose that n divides $|\mu_K|$ and that $N_{K/k}(\zeta) = 1$ for all roots of unity ζ in μ. Suppose moreover that H_K^p is a Kummer extension, generated by the nth root of an element ε in $k^\times$. If $\mathfrak{a}$ is an ideal of K representing a class in Cl_K^p, then $\mathrm{N}_G \cdot \mathfrak{a}$ is principal.*

Proof. Let

$$\phi\colon \mathrm{Cl}_K^p \cong \mathrm{Gal}\,(H_K^p/K)$$

be the Artin map for the extension H_K^p/K. The group G acts on both Cl_K^p and $\mathrm{Gal}\,(H_K^p/K)$ by homomorphisms, so both Cl_K^p and $\mathrm{Gal}\,(H_K^p/K)$ are endowed with $\mathbb{Z}[G]$-module structures. Proposition 2.7.5 shows that ϕ is a $\mathbb{Z}[G]$-module isomorphism. By assumption, N_G is contained in $\mathrm{Ann}_{\mathbb{Z}[G]}\,(\mu_K)$. Applying Lemma 2.7.4, we find that if $\mathfrak{a}$ is an ideal of K representing a class in Cl_K^p, then

$$\phi\,(N_G \cdot \overline{\mathfrak{a}}) = N_G \cdot \phi\,(\overline{\mathfrak{a}}) = 1.$$

The class $N_G \cdot \overline{\mathfrak{a}}$ is therefore trivial in Cl_K^p, so the ideal $N_G \cdot \mathfrak{a}$ is principal.

□

Chapter 3

The Objects and Conjectures of Study

3.1 Properties of Artin L-functions

Let K/k be a Galois extension of number fields with Galois group G and let S be a set of places of k containing the Archimedean places. In this section, we will abuse notation by also using S to denote the set of places in an extension field of k dividing the places in S. The Artin L-function attached to a character χ of a representation of G was defined in equation (1.2), and the S-truncated version was defined at the beginning of section 1.2. These L-functions have the following functoriality properties:

Properties of Artin L-functions.

1. *For the trivial character $\chi = \mathbf{1}$,*

$$L_{K/k,S}(s, \mathbf{1}) = \zeta_{K,S}(s),$$

   the S-truncated Dedekind zeta function of K.

2. *(Additivity) If χ and χ' are characters of complex representations of* $\mathrm{Gal}(K/k)$*, then*

$$L_{K/k,S}(s, \chi + \chi') = L_{K/k,S}(s, \chi) L_{K/k,S}(s, \chi').$$

3. *(Inflation) If K' is a bigger Galois extension of k, $k \subset K \subset K'$, then write $G' = \mathrm{Gal}\,(K'/k)$. For each character χ on G, let $\mathrm{Infl}\,\chi = \chi \circ \pi$, where π is the projection from G' onto G. Then*

$$L_{K'/k,S}(s, \mathrm{Infl}\,\chi) = L_{K/k,S}(s, \chi)$$

4. *(Induction) If k' is an intermediate field, $k \subset k' \subset K$, and χ is the character of a representation of $\mathrm{Gal}(K/k')$, then*

$$L_{K/k,S}(s, \mathrm{Ind}\,\chi) = L_{K/k',S}(s, \chi)$$

Proof. For proofs when S contains only the Archimedean places of k, see [38, Chapter VII, Proposition 10.4]. For general S, property (a) follows by considering the definitions. To prove the other properties for general S, we observe that in the proofs of properties (b)-(c) in [38], equality is demonstrated by showing that the Euler factors in each function corresponding to a given prime in k are equal. Since adding prime ideals of k to S just removes the corresponding Euler factors from the L-functions, the same proof by consideration of Euler factors works for general sets S. On the other hand, for property (d), if $\mathfrak{p}$ is a prime ideal of k and $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ are the prime ideals of k' lying above $\mathfrak{p}$, then the proof in [38] shows that the Euler factor corresponding to $\mathfrak{p}$ in the L-function on the left equals the product of the Euler factors in the L-function on the right corresponding to the primes $\mathfrak{P}_\mathrm{i}$. Since adjoining the prime ideal $\mathfrak{p}$ to a given set S has the effect of removing these Euler factors, the proof again follows from the argument in [38]. □

We now restrict to the case where G is Abelian. The equivariant L-function $\theta_{K/k}$ was defined in (1.4), and its S-truncated variant was defined at the beginning of Section 1.2. Proposition 2.3.1 shows that $\theta_{K/k,S}(s)$ is characterized as the unique meromorphic function taking values in $\mathbb{C}[G]$ whose projection onto the χ component is $L_{K/k,S}\,(s, \chi^{-1})$. Being formed from Artin L-functions, it satisfies the following properties analogous to those above:

Properties of equivariant L-functions.

1. *For the trivial extension $K = k$,*

$$\theta_{K/k,S}(s) = \zeta_{K,S}(s).$$

(We are identifying $\mathbb{C}[G]$ with $\mathbb{C}$).

2. *(Inflation) If K' is a bigger Abelian extension of k, $k \subset K \subset K'$, write $G' = \mathrm{Gal}(K'/k)$. Let $\pi : \mathbb{C}[G'] \to \mathbb{C}[G]$ be the $\mathbb{C}$-linear extension of the canonical projection map. Then*

$$\pi\left(\theta_{K'/k,S}(s)\right) = \theta_{K/k,S}(s).$$

3. *(Induction) If k' is an intermediate field, $k \subset k' \subset K$, and if $H = \mathrm{Gal}(K/k')$, then*

$$\theta_{K/k',S}(s) = \prod_{\substack{\psi \in \widehat{G} \\ \psi(H)=1}} t_\psi\left(\theta_{K/k,S}(s)\right),$$

where t_χ denotes the twist by χ.

Proof. Property 1 follows immediately from the definition of $\theta_{K/k,S}(s)$ and property 1 of Artin L-functions. If K' and G' are as in property 2, then by definition,

$$\theta_{K'/k,S}(s) = \sum_{\chi \in \widehat{G'}} L_{K'/k,S}\left(s, \chi^{-1}\right) e_\chi$$

By Lemma 2.3.2 and the inflation property of Artin L-functions,

$$\begin{aligned}
\pi\left(\theta_{K'/k,S}(s)\right) &= \sum_{\chi \in \widehat{G'}} L_{K'/k,S}\left(s, \chi^{-1}\right) \pi\left(e_\chi\right) \\
&= \sum_{\chi \in \widehat{G}} L_{K/k,S}\left(s, \chi^{-1}\right) e_\chi \\
&= \theta_{K/k,S}(s).
\end{aligned}$$

Now let k' and H be as in property 3. We need to show that for every $\chi \in \widehat{H}$, χ applied to the right side of the equality in property 3 gives $L_{K/k',S}\left(s, \chi^{-1}\right)$. Let $\tilde{\chi}$

be any character on G whose restriction to H is χ. If ψ is any character on G, then by Lemma 2.3.3,

$$\begin{aligned} t_\psi\left(\theta_{K/k,S}(s)\right) &= t_\psi\left(\sum_{\phi\in\widehat{G}} L_{K/k,S}\left(s,\phi^{-1}\right) e_\phi\right) \\ &= \sum_{\phi\in\widehat{G}} L_{K/k,S}\left(s,\phi^{-1}\right) e_{\psi^{-1}\phi}. \end{aligned}$$

Thus,

$$\tilde{\chi}\left(t_\psi\left(\theta_{K/k,S}(s)\right)\right) = L_{K/k,S}\left(s,\psi^{-1}\tilde{\chi}^{-1}\right).$$

Applying $\tilde{\chi}$ to the right side of the equality in property 3 then yields

$$\prod_{\substack{\psi\in\widehat{G}\\ \psi(H)=1}} L_{K/k,S}\left(s,\psi^{-1}\tilde{\chi}^{-1}\right).$$

By the additivity property of Artin L-functions, this is equal to $L_{K/k,S}\left(s,\phi\right)$, where

$$\phi = \sum_{\substack{\psi\in\widehat{G}\\ \psi(H)=1}} \psi^{-1}\tilde{\chi}^{-1}.$$

The terms of this sum are those characters in $\widehat{G}$ whose restriction to H is χ^{-1}. Proposition 2.2.1 shows that this equals $\operatorname{Ind}\chi^{-1}$. By the induction property of Artin L-functions, $L_{K/k,S}\left(s,\phi\right) = L_{K/k',S}\left(s,\chi^{-1}\right)$. □

We will also need some properties of the L-function evaluator. Recall that this was defined in Section 1.2 as the special value of the equivariant L-function at $s=0$:

$$\theta_{K/k,S} = \theta_{K/k,S}(0).$$

Aside from inheriting the functorial properties of the equivariant L-functions provided above, θ also possesses the following additional properties:

Properties of L-function evaluators.

1. *If $\mathfrak{p}$ is not in S, then $\theta_{K/k,S\cup\{\mathfrak{p}\}} = \left(1-\sigma_{\mathfrak{p}}^{-1}\right)\theta_{K/k,S}$, where σ_p is the Frobenius automorphism of K/k associated with $\mathfrak{p}$.*

2. *Assume that* $|S| \geq 2$. *Let* v *be a place in* S. *Set* $N_v = \sum_{\sigma \in D_v} \sigma$, *the sum (in* $\mathbb{C}[G]$*) of the elements of the decomposition group* D_v *of* v. *Then*

$$N_v \theta_{K/k,S} = 0$$

Proof. For any character χ, $\sigma_p e_\chi = \chi(\sigma_p) e_\chi$ by property 1 of the idempotents e_χ in Section 2.3. Property 1 above then holds since

$$\begin{aligned}
\theta_{K/k,S\cup\{\mathfrak{p}\}} &= \sum_{\chi \in G} \left(1 - \chi\left(\sigma_{\mathfrak{p}}^{-1}\right)\right) L_{K/k,S}\left(0, \chi^{-1}\right) e_\chi \\
&= \sum_{\chi \in G} \left(1 - \sigma_{\mathfrak{p}}^{-1}\right) L_{K/k,S}\left(0, \chi^{-1}\right) e_\chi \\
&= \left(1 - \sigma_{\mathfrak{p}}^{-1}\right) \theta_{K/k,S}.
\end{aligned}$$

Property 2 follows from two facts. (For proofs, see [58, Chapter I, Proposition 3.4].) First, if v is a place in S, D_v is its decomposition group in G, χ is a nontrivial character on G, and $\chi(D_v) = 1$, then $L_{K/k,S}(0, \chi) = 0$. Second, $\zeta_{k,S}(0) = 0$ because $|S| \geq 2$. Now if $\chi(D_v) \neq 1$, then

$$\left(\sum_{\sigma \in D_v} \sigma\right) e_\chi = \left(\sum_{\sigma \in D_v} \chi(\sigma)\right) e_\chi = 0$$

by the orthogonality relations. Property 2 then results from the definition of θ. □

Remark. By property 2, $\theta_{K/k,S} = 0$ if any place in S splits completely in K/k. In particular, $\theta = 0$ unless k is totally real and K is totally complex.

Finally, in Chapter 6, we will need the relationship between the Artin L-functions of Abelian extensions of $\mathbb{Q}$ and the corresponding Dirichlet L-functions. Let K be an Abelian extension of $\mathbb{Q}$ of conductor $f\infty$, $f \in \mathbb{N}$. Let $\chi \neq \mathbf{1}$ be a complex-valued character on $\mathrm{Gal}(K/\mathbb{Q})$. This induces a character on

$$\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_f\right)/\mathbb{Q}\right) \cong \left(\mathbb{Z}/f\mathbb{Z}\right)^\times.$$

We denote this Dirichlet character by $\tilde{\chi}$. The following proposition gives the relationship between the Artin L-function corresponding to χ and the Dirichlet L-function corresponding to $\tilde{\chi}$:

Proposition 3.1.1. *With notation as above,*

$$L_{K/\mathbb{Q}}(s,\chi) = \prod_{p\in S} \frac{1}{1-\chi(p)p^{-s}} \cdot L\left(s,\tilde{\chi}\right),$$

where $S = \{\, p \;\big|\; p \mid f \text{ and } \chi\left(I_p\right) = 1 \,\}$, I_p *being the inertia group of* p *in* $\mathrm{Gal}(K/\mathbb{Q})$.

3.2 Partial Zeta Functions

Throughout this section, we assume that K/k is an Abelian extension of number fields with Galois group G. We let S be a finite set of places of k containing the Archimedean places and the prime ideals that ramify in K. Closely related to the Artin L-functions associated with the extension K/k are the partial zeta functions of the extension. If $\mathfrak{a}$ is a fractional ideal of k that is relatively prime to the conductor of K/k, we write $(\mathfrak{a}, K/k)$ for the Artin symbol of $\mathfrak{a}$. An S-truncated partial zeta function is associated with each automorphism σ in G. It is defined by

$$\zeta_{K/k,S}(s,\sigma) = \sum_{\substack{(\mathfrak{a},S)=1 \\ (\mathfrak{a},K/k)=\sigma}} \frac{1}{\mathfrak{N}\,\mathfrak{a}^s}.$$

The sum is taken over all integral ideals in the ring of integers of k that are relatively prime to the ideals in S and that have image σ under the Artin map. Because this is a subsum of the series defining the Dedekind zeta function of k, the series converges absolutely to an analytic function on the half-plane $\Re(s) > 1$. The S-truncated Artin L-functions and the S-truncated partial zeta functions are closely related.

Proposition 3.2.1. *For each* σ *in* G, *the* S*-truncated partial zeta function has a meromorphic continuation to the complex plane, the only pole being a simple pole at* $s = 1$. *It satisfies*

$$\zeta_{K/k,S}(s,\sigma) = \frac{1}{[K:k]} \sum_{\chi\in\widehat{G}} \overline{\chi(\sigma)} L_{K/k,S}(s,\chi).$$

Furthermore, for every $\chi \in \widehat{G}$, *we have*

$$L_{K/k,S}(s,\chi) = \sum_{\sigma\in G} \chi(\sigma)\zeta_{K/k,S}(s,\sigma).$$

The second relationship is proved, for $\Re(s) > 1$, using absolute convergence to rewrite the series for $L_{K/k,S}(s, \chi)$. The first then follows from the orthogonality relations. The existence of a meromorphic continuation of the partial zeta functions follows from that of the L-functions. For details, see [45, Proposition 15.10].

Usually, working with Artin L-functions is preferable to working with partial zeta functions because of the functoriality properties of Artin L-functions and the usefulness of decomposing modules into character components. However, the values of partial zeta functions are sometimes easier to manipulate, so at times we will focus on them. The above proposition allows one to transition easily from one viewpoint to the other.

We will now see that partial zeta functions associated with with $k' \subseteq k \subseteq K$, such that K/k' and k/k' are Galois. Let $\tilde{G} = \mathrm{Gal}(K/k')$ and $H = \mathrm{Gal}(k/k')$. Then $\tilde{G}$ is an extension of G by H, and there is a group homomorphism $\phi\colon H \to \mathrm{Aut}(G)$ as described in Section 2.7.

Proposition 3.2.2. *Let $k' \subset k \subset K$, G, $\tilde{G}$, H, and S be as defined above. Assume that S is stable under the action of H on the ideal group of k. If σ_1 and σ_2 are elements of G and $\phi(\tau)(\sigma_1) = \sigma_2$ for some $\tau \in H$, then*

$$\zeta_{K/k,S}(s, \sigma_1) = \zeta_{K/k,S}(s, \sigma_2).$$

Proof. Let $\tilde{\tau}$ be a lift of τ to $\tilde{G}$. Since k/k' is Galois, $\tilde{\tau}(k) = k$. From Section 2.7, $\phi(\tau)$ is the automorphism of H given by conjugation by $\tilde{\tau}$. It follows that

$$\tilde{\tau}^{-1}\sigma_2\tilde{\tau} = \sigma_1.$$

Thus, for $\Re(s) > 1$, the partial zeta function corresponding to σ_2 is given by

$$\begin{aligned}
\zeta_{K/k,S}(s, \sigma_2) &= \sum_{\substack{(\mathfrak{a},S)=1 \\ (\mathfrak{a},K/k)=\sigma_2}} \frac{1}{\mathfrak{N}\,\mathfrak{a}^s} \\
&= \sum_{\substack{(\mathfrak{a},S)=1 \\ (\tilde{\tau}(\mathfrak{a}),K/k)=\sigma_2}} \frac{1}{\mathfrak{N}\,\mathfrak{a}^s} \\
&= \sum_{\substack{(\mathfrak{a},S)=1 \\ \tilde{\tau}(\mathfrak{a},K/k)\tilde{\tau}^{-1}=\sigma_2}} \frac{1}{\mathfrak{N}\,\mathfrak{a}^s} \\
&= \sum_{\substack{(\mathfrak{a},S)=1 \\ (\mathfrak{a},K/k)=\sigma_1}} \frac{1}{\mathfrak{N}\,\mathfrak{a}^s} \\
&= \zeta_{K/k,S}(s, \sigma_1).
\end{aligned}$$

Since these meromorphic functions are equal for $\Re(s) > 1$, they are equal for $s \neq 1$. □

Next, we will discuss the special values of partial zeta functions. Building on prior work of Helmut Klingen ([30]), Carl Ludwig Siegel ([52]) proved the following deep result. It was later proved by Takuro Shintani ([51]) using different methods.

Theorem 3.2.3 (Siegel, Shintani)**.** *For every σ in G and each integer $n \geq 0$, $\zeta_S(-n, \sigma)$ is rational.*

Actually, they proved this when K is a ray class field of k and S is the minimal set $S^{\min}$ of places of k composed of the Archimedean places and the primes that ramify in K. To demonstrate the more general statement, consider a field K' with $k \subseteq K \subseteq K'$ with K'/k Abelian. Suppose that each non-Archimedean prime of k that ramifies in K also ramifies in K'. By considering the behavior of the Artin map under restriction, one shows that for each σ in G,

$$\sum_{\tau|_K=\sigma} \zeta_{K'/k,S^{\min}}(s, \tau) = \zeta_{K/k,S^{\min}}(s, \sigma).$$

The sum is over those elements τ in $\mathrm{Gal}(K'/k)$ whose restriction to K is σ. Let K' be the ray class field of k with conductor equal to that of K/k. Then since the

values on the left side are rational for non-positive integers $s = -n$, the value on the right is as well. To prove the theorem for larger sets S, we consider first what happens when we augment the set S by a single prime ideal $\mathfrak{p}$ in k. Writing $\sigma_{\mathfrak{p}}$ for the Frobenius automorphism of $\mathfrak{p}$ in G, for $\Re(s) > 1$, we have

$$\begin{aligned}
\zeta_{K/k,S\cup\{\,\mathfrak{p}\,\}}(s,\sigma) &= \sum_{\substack{(\mathfrak{a},S)=1\\(\mathfrak{a},K/k)=\sigma}} \frac{1}{N\mathfrak{a}^s} - \sum_{\substack{(\mathfrak{a},S)=1,\mathfrak{p}|\mathfrak{a}\\(\mathfrak{a},K/k)=\sigma}} \frac{1}{N\mathfrak{a}^s} \\
&= \sum_{\substack{(\mathfrak{a},S)=1\\(\mathfrak{a},K/k)=\sigma}} \frac{1}{N\mathfrak{a}^s} - N\mathfrak{p}^{-s} \sum_{\substack{(\mathfrak{a},S)=1\\(\mathfrak{a},K/k)=\sigma\sigma_{\mathfrak{p}}^{-1}}} \frac{1}{N\mathfrak{a}^s} \\
&= \zeta_{K/k,S}(s,\sigma) - N\mathfrak{p}^{-s}\zeta_{K/k,S}\left(s,\sigma\sigma_{\mathfrak{p}}^{-1}\right). \qquad (3.1)
\end{aligned}$$

Since this holds for $\Re(s) > 1$, it holds for all $s \neq 1$. If the partial zeta functions on the right side take rational values for non-positive integers $s = -n$, then the partial zeta function on the left side does as well. The result of the theorem for general sets S containing $S^{\min}$ follows by induction.

Now for any function ε on G with values in a $\mathbb{Q}$-vector space V, the formula

$$L_{K/k,S}(-n,\varepsilon) = \sum_{\sigma\in G} \varepsilon(\sigma)\zeta_{K/k,S}(-n,\sigma),$$

provides the *definition* of values $L(-n,\varepsilon)$ in V for integers $n \geq 0$. When χ is a complex-valued character on G, Proposition 3.2.1 shows that these are the values of S-truncated Artin L-functions at nonpositive integers $-n$. Theorem 3.2.3 shows that these values lie in the field of values of the corresponding character. When $\varepsilon : G \to \mathbb{Q}[G]$ is the homomorphism sending $\sigma \mapsto \sigma^{-1}$, we have

$$L_{K/k,S}(0,\varepsilon) = \sum_{\sigma\in G} \zeta_{K/k,S}(0,\sigma)\sigma^{-1} = \theta_{K/k,S}, \qquad (3.2)$$

the L-function evaluator associated with K/k and S. This follows by comparing the coefficient of σ^{-1} in the definition of $\theta_{K/k,S}$ with the right side of the first relation in proposition 3.2.1. Thus, the coefficients of θ are rational. Another case of interest is when ε is a character with values in the algebraic closure of the p-adic numbers for some prime number p. When ε has order dividing $p-1$, the L-values lie in $\mathbb{Q}_p$.

Following Theorem 3.2.3, the next discovery about the special values of partial zeta functions for nonpositive integers $s = -n$ was the determination of explicit bounds for their denominators. Such bounds follow from relationships between the values of partial zeta functions used as axioms by John Coates while constructing p-adic zeta functions associated with totally real fields (see [6]). The validity of these congruences was later confirmed independently by Daniel Barsky, Pierette Cassou-Noguès, and Deligne-Ribet. We will only need to consider the values of partial zeta functions at $s = 0$, in which case we have the following theorem:

Theorem 3.2.4 (Barsky, Cassou-Noguès, Deligne-Ribet)**.** *With notation as at the beginning of this section, the group μ of roots of unity in K is a $\mathbb{Z}[G]$-module. It is linked to $\theta_{K/k,S}$ through the inclusion*

$$Ann_{\mathbb{Z}[G]}(\mu)\,\theta_{K/k,S} \in \mathbb{Z}[G].$$

This ideal is called the Stickelberger ideal.

In particular, if W is the number of roots of unity in K, then $W\theta$ is in $\mathbb{Z}[G]$. It follows from equation (3.2) that the denominators of the rational numbers $\zeta_{K/k,S}(0,\sigma)$ are divisors of W for all σ in G.

To apply Theorem 3.2.4, the following lemma is sometimes useful (see [58, Chapter IV, Lemma 1.1]):

Lemma 3.2.5. *Let k, K, G, and S be as at the beginning of the section, and assume that S contains the prime ideals dividing W. Then $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)$ is generated as a $\mathbb{Z}$-module by the elements $\sigma_p - \mathfrak{N}\mathfrak{p}$, where $\mathfrak{p}$ runs through the prime ideals of k outside of S, σ_p denotes the Frobenius element for K/k associated with $\mathfrak{p}$, and $\mathfrak{N}\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$.*

3.3 Components of the equivariant L-function

Throughout this section, we continue to assume that K/k is an Abelian extension of number fields with Galois group G, and that S is a set of places of k containing the Archimedean places. We let $W = |\mu|$ be the cardinality of the group of roots of unity in K.

Let χ be a complex-valued character on G of order n. The smallest subfield of $\mathbb{C}$ containing the values of χ is $\mathbb{Q}(\zeta_n)$, the field of values of χ. If σ is in $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, then we can produce another character χ^σ on G by defining

$$\chi^\sigma(g) = \chi(g)^\sigma$$

for all g in G. The relation $\chi \sim \psi$ if there exists an automorphism σ in $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ such that $\chi^\sigma = \psi$ is an equivalence relation, and partitions the characters of G into classes of conjugate characters. To such a class $\mathfrak{C}$ of characters, we will associate a function $\theta_{K/k,S,\mathfrak{C}}(s)$ as follows:

$$\theta_{K/k,S,\mathfrak{C}}(s) = \sum_{\chi \in \mathfrak{C}} L_{K/k,S}\left(s, \chi^{-1}\right) e_\chi,$$

where the e_χ are once again the idempotents of equation (1.3). We will call this function the $\mathfrak{C}$-component of the equivariant L-function. Similarly, we will denote the special value of this function at $s = 0$ by $\theta_{K/k,S,\mathfrak{C}}$, or often simply by $\theta_{\mathfrak{C}}$. We will refer to $\theta_{\mathfrak{C}}$ as the $\mathfrak{C}$-component of the L-function evaluator. By the definitions, we have

$$\theta_{K/k,S}(s) = \sum_{\mathfrak{C}} \theta_{K/k,S,\mathfrak{C}}(s).$$

First, we consider the functoriality properties of the components of the L-function evaluator. Let K' be a bigger Abelian extension of k, $k \subseteq K \subseteq K'$. Write $G' = \mathrm{Gal}(K'/k)$ and $H = \mathrm{Gal}(K'/K)$. Let $\pi\colon \mathbb{C}[G'] \to \mathbb{C}[G]$ be the $\mathbb{C}$-linear extension of the projection map. Let N_H denote the norm element in $\mathbb{Z}[H]$.

Properties of components of L-function evaluators.

1. *Suppose that χ is a character on G' satisfying $\chi(H) = 1$. Let $\mathfrak{C}'$ be the equivalence class of χ, and let $\mathfrak{C}$ be the equivalence class of χ when considered as a character on G. Then*

$$\pi\left(\theta_{K'/k,S,\mathfrak{C}'}\right) = \theta_{K/k,S,\mathfrak{C}}.$$

2. *If χ and $\mathfrak{C}'$ are as in property 1, and if β is any lift of $\theta_{K/k,S,\mathfrak{C}}$ to $\mathbb{C}[G']$, then*

$$\theta_{K'/k,S,\mathfrak{C}'} = \frac{N_H}{|H|}\beta.$$

3. *If χ is a character on G' and $\chi(H) \neq 1$, then*

$$\pi\left(\theta_{K'/k,S,\mathfrak{C}'}\right) = 0.$$

4. *Assume that $|S| \geq 2$. Let v be a place in S, and let $N_v = \sum_{\sigma \in D_v} \sigma$, the sum of the elements of the decomposition group D_v of v. Suppose that χ is a character on G representing the class $\mathfrak{C}$. Then*

$$N_v \theta_{K/k,S,\mathfrak{C}} = 0.$$

Proof. If χ, $\mathfrak{C}$, and $\mathfrak{C}'$ are as defined in property 1 and σ is in $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, then $\chi^\sigma(H) = 1$, so χ^σ can be considered as a character on G. As such, χ^σ is in the same class $\mathfrak{C}$ as χ. The map $\mathfrak{C}' \to \mathfrak{C}$ sending each character χ^σ in $\mathfrak{C}'$ to χ^σ considered as a character on G is a bijection. Using this observation, as well as Lemma 2.3.2 and the inflation property of Artin L-functions, we have

$$\begin{aligned}
\pi\left(\theta_{K'/k,S,\mathfrak{C}'}\right) &= \sum_{\chi \in \mathfrak{C}'} L_{K'/k,S}\left(0, \chi^{-1}\right) \pi\left(e_\chi\right) \\
&= \sum_{\chi \in \mathfrak{C}} L_{K'/k,S}\left(0, \chi^{-1}\right) e_\chi \\
&= \theta_{K/k,S,\mathfrak{C}}.
\end{aligned}$$

Now let β and γ be any lifts of $\theta_{K/k,S,\mathfrak{C}}$ to $\mathbb{C}\left[G'\right]$. Then

$$\pi\left(\beta - \gamma\right) = 0.$$

Let $\tau_1, \ldots, \tau_{|G|}$ be representatives of the cosets G'/H. We may write

$$\beta - \gamma = \sum_{i=1}^{|G|} \sum_{\sigma \in H} a_{i\sigma} \tau_i \sigma.$$

The condition on $\beta - \gamma$ can then be rewritten as

$$\sum_{\sigma \in H} a_{i\sigma} = 0$$

for $1 \leq i \leq |G|$. It follows that

$$\frac{N_H}{|H|}\left(\beta - \gamma\right) = \frac{1}{|H|} \sum_{i=1}^{|G|} \left(\sum_{\sigma \in H} a_{i\sigma} \right) N_H \tau_i = 0.$$

Therefore,

$$\frac{N_H}{|H|}\beta$$

is independent of the choice of lift β. In particular, by property 1, we may choose

$$\beta = \theta_{K'/k,S,\mathfrak{C}'}.$$

We have

$$\begin{aligned}\frac{N_H}{|H|}\theta_{K'/k,S,\mathfrak{C}'} &= \frac{N_H}{|H|}\sum_{\chi\in\mathfrak{C}'} L_{K/k,S}\left(0,\chi^{-1}\right)e_\chi \\ &= \frac{N_H}{|H|}\sum_{\sigma\in G'}\left(\sum_{\chi\in\mathfrak{C}'} L_{K/k,S}\left(0,\chi^{-1}\right)\chi^{-1}(\sigma)\right)\sigma.\end{aligned}$$

Since $\chi(H)=1$ for each character χ in $\mathfrak{C}'$, the coefficients in the above double sum of the elements in a fixed coset G/H are identical. Thus, we may write

$$\sum_{\sigma\in G'}\left(\sum_{\chi\in\mathfrak{C}'} L_{K/k,S}\left(0,\chi^{-1}\right)\chi^{-1}(\sigma)\right)\sigma = N_H\alpha,$$

for some α in $\mathbb{C}[G']$. Then

$$\frac{N_H}{|H|}\theta_{K'/k,S,\mathfrak{C}'} = \frac{N_H}{|H|}(N_H\alpha) = N_H\alpha = \theta_{K'/k,S,\mathfrak{C}'}.$$

Property 2 follows.

Property 3 is a consequence of the definition of $\theta_{K'/k,S,\mathfrak{C}'}$ and Lemma 2.3.2. Property 4 follows from the same proof as that of property 2 of L-function evaluators in Section 3.1. □

We now make the additional assumption that S contains the prime ideals of k that ramify in K. We have the following rationality result concerning $\theta_{K/k,S,\mathfrak{C}}$:

Proposition 3.3.1. *Let $\mathfrak{C}$ be a class of conjugate characters on G, each of order n. Then the coefficients of $\theta_{K/k,S,\mathfrak{C}}$ are rational. Moreover,*

$$|G|\,\mathfrak{N}\left(\chi\left(\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)\right)\right)\theta_{K/k,S,\mathfrak{C}} \subseteq \mathbb{Z}[G],$$

where χ is the $\mathbb{C}$-linear extension of any character in $\mathfrak{C}$ and $\mathfrak{N}$ is the absolute norm on ideals in $\mathbb{Q}(\zeta_n)$.

Proof. $\mathfrak{C}$ contains $\phi(n)$ characters, taking their values in $\mathbb{Q}(\zeta_n)$. Let χ be any character in $\mathfrak{C}$. By Theorem 3.2.4, $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\theta_{K/k,S}$ is contained in $\mathbb{Z}[G]$. Applying χ, we find that

$$\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right) L_{K/k,S}\left(0,\chi^{-1}\right) \subseteq \mathbb{Z}\left[\zeta_n\right].$$

It follows that

$$\mathfrak{N}\left(\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)\right) L_{K/k,S}\left(0,\chi^{-1}\right) \subseteq \mathbb{Z}\left[\zeta_n\right] \tag{3.3}$$

for every character χ in $\mathfrak{C}$.

Now set $\mathfrak{G} = \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right)$. If σ is in $\mathfrak{G}$, then by Theorem 3.2.3 and the second formula of Proposition 3.2.1,

$$L_{K/k,S}\left(0,\chi\right)^{\sigma} = L_{K/k,S}\left(0,\chi^{\sigma}\right).$$

For any τ in G, the coefficient of τ in $\theta_{K/k,S,\mathfrak{C}}$ is

$$\begin{aligned}\frac{1}{|G|}\sum_{\sigma\in\mathfrak{G}} L_{K/k,S}\left(0,\left(\chi^{\sigma}\right)^{-1}\right)\chi^{\sigma}\left(\tau^{-1}\right) &= \frac{1}{|G|}\sum_{\sigma\in\mathfrak{G}}\left(L_{K/k,S}\left(0,\chi^{-1}\right)\chi\left(\tau^{-1}\right)\right)^{\sigma}\\ &= \frac{1}{|G|}\mathrm{Tr}\left(L_{K/k,S}\left(0,\chi^{-1}\right)\chi\left(\tau^{-1}\right)\right),\end{aligned}$$

where Tr denotes the trace from $\mathbb{Q}\left(\zeta_n\right)$ to $\mathbb{Q}$. Therefore, the coefficients of $\theta_{K/k,S,\mathfrak{C}}$ are rational. By (3.3), the last expression becomes integral after multiplication by $|G|\,\mathfrak{N}\left(\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)\right)$. □

Example. Let $k = \mathbb{Q}$, $K = \mathbb{Q}\left(\zeta_7\right)$, and $S = \{7, \infty\}$, the prime number 7 and the Archimedean place of $\mathbb{Q}$. Then G is cyclic of order 6, so there are 4 equivalence classes of characters, consisting of those characters of orders 6, 3, 2, and 1. If χ has order 3 or 1, then χ is trivial on the decomposition group of the place ∞. By [58, Chapter I, Proposition 3.4], we know that $L_{K/k,S}\left(0,\chi^{-1}\right) = 0$. Thus, the L-function evaluator has at most two nonzero components, corresponding to the class $\mathfrak{C}_6$ of characters of order 6 and the class $\mathfrak{C}_2$ consisting of the character of order 2.

The partial zeta functions of K/k are the classical Hurwitz zeta functions, whose values at non-positive integers are known. In particular,

$$\theta_{K/k,S} = \sum_{n=1}^{6}\left(\frac{1}{2} - \frac{a^{-1}}{7}\right)\sigma_a,$$

where σ_a is the automorphism in G sending ζ_7 to ζ_7^a, and a^{-1} denotes the least positive integer inverse to a mod 7. We may also determine from the definitions that

$$\theta_{K/k,S,\mathfrak{C}_2} = \frac{1}{6}\sum_{a=1}^{6}\left(\frac{a}{7}\right)\sigma_a.$$

Therefore, it follows that

$$\theta_{K/k,S,\mathfrak{C}_6} = \left(\frac{4}{21}\sigma_1 - \frac{5}{21}\sigma_2 + \frac{1}{21}\sigma_4\right)(1-\sigma_6).$$

To compare with the denominators given by Proposition 3.3.1, observe that $2-\sigma_2$ is in $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)$. If χ is the character in G of order 2, then $\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)$ is an ideal in $\mathbb{Z}$ containing $2-\chi(\sigma_2) = 1$. Thus, the proposition shows that the denominators of $\theta_{K/k,S,\mathfrak{C}_2}$ divide $|G| = 6$. If χ is a character of order 6, then since σ_2 has order 3 in G, we find that $\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)$ is an ideal in $\mathbb{Z}[\zeta_3]$ containing $2-\chi(\sigma_2) = \frac{5\pm\sqrt{-3}}{2}$. Thus, $\mathfrak{N}\left(\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)\right)$ divides

$$\frac{5+\sqrt{-3}}{2}\,\frac{5-\sqrt{-3}}{2} = 7.$$

On the other hand, since the denominators of the coefficients of $\theta_{K/K,S,\mathfrak{C}_6}$ are 21, the proposition shows that

$$\mathfrak{N}\left(\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)\right) = 7.$$

Conversely, assuming this fact, the proposition shows that $\theta_{K/k,S,\mathfrak{C}_6}$ has denominators dividing 42.

We see from this example that the bound on the denominators of the components of the L-function evaluator given in the proposition can sometimes be achieved. Furthermore, we see that the denominators can exceed W. When this occurs, the coefficients of the various components must satisfy relations ensuring that the denominators of $\theta_{K/k}$ are divisors of W. The possibility of the coefficients of the components $\theta_{\mathfrak{C}}$ having denominators exceeding W will ultimately create a serious barrier to proving Brumer's Conjecture. On the other hand, this phenomenon will also enable the proofs of statements about class number divisibility.

3.4 The Brumer and Brumer-Stark Conjectures

Since the Stickelberger ideal from Theorem 3.2.4 is contained in $\mathbb{Z}[G]$, it is natural to apply its elements to $\mathbb{Z}[G]$-modules associated with K. This section describes two conjectures about how the Stickelberger ideal acts on the class group Cl_K. Other references about these conjectures and their connections with other annihilation and Stark-type conjectures can be found in [59], [58] and [15].

3.4.1 Statement of the conjectures

In this subsection, K/k is a fixed Abelian extension of number fields with Galois group G. Moreover, k is totally real and K is totally complex. In addition, S is a set of places of k containing the Archimedean places and the prime ideals of k that ramify in K, $\theta = \theta_{K/k,S}$ is the associated L-function evaluator, μ is the group of roots of unity in K, and W is its cardinality. By Theorem 3.2.4, $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\,\theta$ is contained in $\mathbb{Z}[G]$. First, we have

Brumer's Conjecture (B).

$$\mathrm{Ann}_{\mathbb{Z}[G]}\left(\mu\right)\theta_{K/k,S} \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}\left(\mathrm{Cl}_K\right).$$

This conjecture will be referred to simply as (B). It is analogous to the statement that the rational factor of the coefficient in equation (1.1) is the class number divided by the number of roots of unity. We note that Brumer's Conjecture implies that $W\theta$ annihilates Cl_K.

The second conjecture says that if we restrict attention to the element $W\theta$ in the Stickelberger ideal, we can say much more. We need a definition:

Definition 3.4.1.

1. *An element α in $K^\times$ is called an anti-unit if $|\sigma\alpha| = 1$ for all embeddings $\sigma\colon K \to \mathbb{C}$. The set of anti-units in K will be denoted by K^o.*

2. *Let K/k be an Abelian extension of number fields, let α be in $K^\times$, and let n be a positive divisor of W. Then α is called n-Abelian if $K\left(\sqrt[n]{\alpha}\right)/k$ is Abelian.*

We observe that $K\left(\sqrt[v]{\alpha}\right)/K$ is Abelian by Kummer theory. In contrast, the condition of being n-Abelian is highly non-trivial.

We may now state the second conjecture:

The Brumer-Stark Conjecture (BS). *If $\mathfrak{a}$ is a fractional ideal of K, then $\mathfrak{a}^{W\theta}$ is principal, and has a generator $\alpha \in K^{\times}$ satisfying*

1. *α is an anti-unit*

2. *α is W-Abelian.*

This conjecture will be referred to as (BS).

Each of the above conjectures has local variants. If p is a prime number, the local version (B_p) of Brumer's conjecture is obtained from Brumer's conjecture by replacing Cl_K by the p-primary part of Cl_K. The local version (BS_p) of the Brumer-Stark conjecture is obtained from the Brumer-Stark conjecture by the following modifications: $\mathfrak{a}$ is restricted to be in the p-primary part of Cl_K, and W-Abelian is replaced by W_p-Abelian, where W_p is the largest power of p dividing W. The truth of each conjecture is equivalent to the truth of the corresponding local conjectures for all prime numbers p. This is explained in detail in [18].

We will now describe several results, each demonstrating an instance where the general conjecture (BS) follows from a special case. For proofs, see [59], [47], [24], and [42].

1. The set of ideals $\mathfrak{a}$ satisfying the conditions in (BS) forms a subgroup of the ideal group I_K. This subgroup contains the principal ideals. Thus, to verify the conjecture, it suffices to show that a set of ideals generating the ideal class group Cl_K satisfies the conditions in (BS).

2. Assume that (BS) holds for the extension K/k and the set S. If $\mathfrak{p}$ is a prime ideal of k outside of S, then (BS) also holds for the extension K/k and the set $S \cup \mathfrak{p}$. Thus, to prove the conjecture for the extension K/k and arbitrary allowable sets S, it suffices to prove the conjecture for the minimal set $S^{\min}$ composed of the Archimedean places of k and the prime ideals of k that ramify in K. We then say that (BS) holds for the extension K/k without mentioning a set S.

3. **(Top Change)** Let k' be an intermediate field, $k \subset k' \subset K$. If (BS) holds for the extension K/k and a set S, then it also holds for the extension k'/k and the set S. It must be noted that if there exists a prime ideal $\mathfrak{p}$ of k ramified in K/k but not in k'/k, then the minimal allowable set S for the extension k'/k is smaller than that for the extension K/k. In this situation, one cannot assert that (BS) for the extension K/k implies (BS) for the extension k'/k.

4. **(Base Change)** Again, let k' be an intermediate field, $k \subset k' \subset K$. Let S be a set of places of k and let S' be the set of places of k' lying above those in S. Then (BS) for the extension K/k and the set S implies (BS) for the extension K/k' and the set S'. If there exists a prime ideal of k that ramifies in K/k but not in K/k', then one cannot assert that (BS) for the extension K/k implies (BS) for the extension k'/k.

Finally, we will present results describing the relationship between Brumer's conjecture and the Brumer-Stark conjecture. First, there is the following general result (see [43, §3, Remark 3]):

Theorem 3.4.2. *The Brumer-Stark conjecture for an extension K/k and a set S implies Brumer's conjecture for the same extension K/k and set S.*

The next result shows that the converse is sometimes true locally. If p is a prime number, let μ_p denote the group of p-power roots of unity in the field K.

Proposition 3.4.3. *If K/k, G, and S are as above, $p \neq 2$, and μ_p is G-cohomologically trivial, then* (B_p) *is equivalent to* (BS_p).

For the proof, see [18, Proposition 1.2].

Remark. There is another collection of ideas related to the Brumer-Stark conjecture. These stem from Eisenstein's proof of his reciprocity law in the middle of the nineteenth century, which preceded Stickelberger's theorem. Gauss sums played a prominent role in this proof, as they do in the proof of the Brumer-Stark conjecture for cyclotomic extensions of $\mathbb{Q}$. In two famous papers ([61] and [62]), Andre Weil proved that Gauss and Jacobi sums can be used to define Hecke characters in number fields that are Abelian over $\mathbb{Q}$. The values of Weil's Jacobi sum Hecke

characters reappeared as the generators of the principal ideals given in Sands's proof of the Brumer-Stark conjecture for extensions K/k with K abelian over $\mathbb{Q}$ (and some restrictions on S). These results have been extended by David Hayes ([22], [23], and [20]) and Tong-Hai Yang ([65]; note that there is a mistake in the part of this paper concerning (BS_2)). However, they will play no role in this work.

3.4.2 The state of knowledge

Since the Brumer-Stark conjecture for an extension K/k and a set S implies Brumer's conjecture for the same extension K/k and set S, we begin by describing the cases where the Brumer-Stark conjecture or its local versions have been proved.

1. (BS) has a function field analog which was proved by Deligne using his 1-motives (see [58, Chapter 5]) and independently by David Hayes using the theory of rank-1 Drinfeld modules ([21]).

2. (BS) is true when $k = \mathbb{Q}$ ([58, Chapter 4, Proposition 6.7]). It is a refinement of the classical theorem of Stickelberger describing the factorization of principal ideals generated by Gauss sums.

3. (BS) is true when $G = \mathrm{Gal}(K/k)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ ([59, §3, case (c)]) or to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ ([48]).

4. (BS) is true in almost all cases where G is 2-elementary ([48, §3, case (3)] and [9]).

5. (BS) is true when there exists a field k' such that $k' \subseteq k \subseteq K$, with K/k' Galois having non-Abelian Galois group of order 8 ([59, §3, case (e)]).

6. If p is an odd prime number, then (BS_p) is true when G is isomorphic to $\mathbb{Z}/2p\mathbb{Z}$ and K/k is not one of two relatively rare types of extensions called case II(b) and case $\flat$ in the paper [18]. (Note: in their paper, the cases II(b) and $\sharp$ are erroneously conflated; case II(b) is actually a subcase of $\sharp$). In case II(b), ζ_p is in K and no place of k splits in $k(\zeta_p)$ and ramifies in K. In case $\flat$, ζ_p is not in K, no prime of k splits in the quadratic subextension of K/k and

ramifies in K, and $K^{\mathrm{cl}} \subset \left(K^{\mathrm{cl}}\right)^{+}(\zeta_p)$, where cl denotes the normal closure over $\mathbb{Q}$.

7. (BS_2) holds for Abelian sextic extensions ([18]). In addition, I have been informed through a private communication with the authors that they have a proof of (BS_2) when the 2-part of G is cyclic and the odd part of G is trivial or of prime order p such that 2 is a primitive root mod p. Also, they have a proof of (BS_2) when G is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and the maximal totally real subfield of K is not cyclic over k. Proofs of each of the above cases excepting the last, independently discovered, will be presented in Chapter 5.

8. If p is an odd prime, the Iwasawa μ invariant for p and K vanishes, and K/k is a nice extension, then (BS_p) is true (see [43], where something much stronger is proved – for the definition and examples of nice extensions, see [14] or [43]).

9. If p is an odd prime number, then (BS_p) is true in a case with "no trivial zeros" ([15, §4.4]).

Remark. In the last two examples, a strong form of (BS_p) was proved by exhibiting a close relationship between θ and the $\mathbb{Z}[G]$-Fitting ideal of part of the class group Cl_K.

We now turn to cases where (B) or its local variants are known to hold, excepting those which follow from the above examples by Theorem 3.4.2 or Proposition 3.4.3.

1. If p is an odd prime number relatively prime to $|G|$, then (B_p) is true when certain restrictions on S are met ([64]; note that there is a mistake in this paper in the proof of (B_p) for primes p dividing $|G|$) and ([18, Proposition 1.3]).

2. If p is an odd prime number, then (B_p) holds in a case with "no trivial zeros" ([16, Corollaries 2 and 3], and the remark following Theorem 3.13 in [15]).

3.5 Hayes's Conjecture

Let K/k be an Abelian extension of number fields with Galois group G, let S be a set of places of k containing the Archimedean places and the prime ideals that ramify in K, and let $W = |\mu|$ be the cardinality of the group of roots of unity in K. Theorem 3.2.4 shows that the denominators of the coefficients of the L-function evaluator are divisors of W. As will be seen in Chapter 6, when these coefficients are written in lowest terms, all of the denominators are identical. Often, this common denominator is a proper divisor of W. David Hayes recently proposed a conjecture providing a condition under which this is true.

Hayes's condition generalizes the following observation. Let

$$K = k = \mathbb{Q}\left(\sqrt{-d}\right)$$

be an imaginary quadratic field containing only two roots of unity. Then the equivariant L-function for K/k is the Dedekind zeta function of k, and

$$\theta_{K/k} = \frac{h}{W},$$

where h is the class number of k and $W = 2$. The observation is that when this number is written in lowest terms, the denominator is 2 unless $2 \mid h$. Thus, if there exists an unramified quadratic extension of k (a Kummer extension), then θ is actually integral. More generally, if $K = k$ is a totally complex field containing W roots of unity, and if there exists an unramified Kummer extension of k of degree n dividing W, then the denominator when the rational part of the coefficient in equation (1.1) is written in lowest terms is a divisor of W/n.

David Hayes conjectured a generalization of this idea while studying Hecke characters whose values satisfy reciprocity laws. He has actually given two formulations of his conjecture. The first is in an unpublished manuscript ([25]):

Hayes's Conjecture (Strong Version). *Let K/k, G, S, and W be as above, and denote the totally positive units in k by U_k^+. Let H_W be the intersection of $K\left(\sqrt[W]{U_k^+}\right)$ with the Hilbert class field of K, and let e be the exponent of* $\mathrm{Gal}\,(H_W/K)$. *Then*

1. *$W\theta_{K/k,S}$ is contained in $e\mathbb{Z}[G]$.*

2. *$\frac{W}{e}\theta$ annihilates Cl_K.*

Remark. He also includes the condition that K contains the narrow Hilbert class field of k. We have removed this condition because, as we will see, it appears to be unnecessary. The above conjecture was also mentioned in Hayes's work ([20]) on Hecke characters and reciprocity laws. The condition on the narrow Hilbert class field of k is included in that paper to ensure that the norm of each ideal of K down to k is principal and generated by a totally positive number. This is necessary for applying the W_Kth power reciprocity law. Perhaps a generalization of Proposition 2.7.6 would obviate the need for the extra condition.

In Chapter 6, we will see evidence supporting the veracity of statement 1 in his conjecture. However, we will also give a counterexample to statement 2, in which even the annihilation statement of (BS) is false when $W\theta$ is replaced by $\frac{W}{e}\theta$. Foreseeing this, we will focus solely on statement 1 until the counterexample to statement 2 is presented.

There is a local formulation of statement 1 of the strong version:

Hayes's Conjecture (Strong Local Version). *Let K/k, G, S, and W be as above, and let p^r be a prime power divisor of W. If there exists an element ε in U_k^+ whose p^rth root generates an unramified extension of K of degree p^r, then $W\theta_{K/k,S}$ is contained in $p^r\mathbb{Z}[G]$.*

The strong version of Hayes's conjecture is equivalent to the collection of local versions for all prime numbers p. This can be seen by considering the primary decomposition of $\mathrm{Gal}\,(H_W/K)$ and using the fact that a cyclic Kummer extension can be generated by the root of a single element of the base field.

The second formulation of Hayes's conjecture is in the introduction of [26].

Hayes's Conjecture (Weak Local Version). *Let K/k, G, S, and W be as above. Let p be a prime divisor of W that does not ramify in K/k. Assume that the subfield H_p of the Hilbert class field of K generated by the pth roots of the totally positive units in k properly contains K. Then $W\theta_{K/k,S}$ is in $p\mathbb{Z}[G]$.*

Actually, the assumption that H_p properly contains K was not explicitly included in [26]. It was included here to ensure that the two versions of the conjecture are similar.

With one exception, we will examine only the weak local version of the conjecture. The investigations in Chapter 6 suggest that the condition that p is unramified in K/k is unnecessary. We will therefore disregard it. The resulting conjecture is a special case of the strong local version as formulated above. In fact, the results in the present work indicate that a modification of the strong local version is true.

Hayes's Conjecture (Modified Strong Local Version). *With notation as above, let p^r be a prime power divisor of W. If there exists a totally positive element ε in k whose p^rth root generates an unramified extension of K of degree p^r, then $W\theta_{K/k,S}$ is contained in $p^r\mathbb{Z}[G]$.*

We note that the element ε in this version is not required to be a unit. For the remainder of this work, the term Hayes's p-local conjecture will mean this version of the conjecture, and we will denote it by (H_p).

Remark. One might also wonder if the condition that ε is totally positive in the above conjecture is also superfluous. If p is odd and ε is as specified in (H_p), then ε^2 is totally positive and also satisfies the condition on ε in the conjecture. Thus, we may dispense with the condition that ε is totally positive when p is odd. In several examples, it can be shown that the condition that ε is totally positive is unnecessary when $p = 2$. As we will primarily be considering (H_p) when p is odd, we will not comment on this further.

The above conjectures are equivariant generalizations of the simple observation about Dedekind zeta functions mentioned at the beginning of the section. Similarly, one may wonder if there are generalizations of this observation for the individual Artin L-functions associated with K/k. We will have more to say about this in Chapter 6, after we have determined some information about the values of Artin L-functions. This is the subject of the next chapter.

Chapter 4

L-values of Cyclic Extensions

4.1 Overview

One of the primary barriers to further progress on the Brumer and Brumer-Stark conjectures is a dearth of specific information about the values at $s = 0$ of Artin L-functions associated with Abelian extensions. The initial cases that were proved primarily fall into two classes: extensions with 2-elementary Galois groups, and extensions K/k with K an Abelian extension of $\mathbb{Q}$. These also happen to be the two cases where arithmetic interpretations of the value at $s = 0$ of the associated Artin L-functions were known classically.

When the extension K/k has 2-elementary Abelian Galois group G, the characters all have order 2. By the inflation property of Artin L-functions, the L-function associated with a nontrivial character on G may be identified with the L-function of a quadratic subextension of K/k. An expression for the value of such an L-function at $s = 0$ has long been known. Indeed, the L-function can fortuitously be written as the quotient of two zeta functions, and the value can then be determined using the analytic class number formula. All of the progress on the Brumer and Brumer-Stark conjectures for 2-elementary extensions has been made by squeezing as much as possible out of the expression for the value at $s = 0$ of the L-function associated with a quadratic extension.

As mentioned in the introduction, the L-functions associated with an extension K/k where K is an Abelian extension of $\mathbb{Q}$ are Dirichlet L-functions. The values

of these functions involve generalized Bernoulli numbers. It is not this description, however, that has been used to study the Brumer and Brumer-Stark conjectures. Instead, when $k = \mathbb{Q}$, the conjectures follow from Stickelberger's Theorem and the particularly simple description of values of the Hurwitz Zeta Functions (the partial zeta functions of this example) at $s = 0$. For more general k, progress has been made by starting with the case $k = \mathbb{Q}$ and using the induction property of Artin L-functions.

Much of the recent progress on these conjectures, beginning with the work of Wiles ([63]), has involved taking projective limits of the various objects that appear in the conjectures while ascending a cyclotomic $\mathbb{Z}_p$-extension of number fields. This perspective allows application of the immensely powerful Main Conjecture of Iwasawa theory for totally real fields ([64]). When p is an odd prime number, the L-function evaluators of the extensions of a totally real field in its p-power cyclotomic Iwasawa tower form a projective system with respect to the restriction maps on the Galois groups. The projective limit of the L-function evaluators is related to the p-adic L-functions of the base field. The Main Conjecture connects the p-adic L-functions to the projective limit of the p-primary parts of the class groups in the tower. Descending back to finite extensions of number fields imposes complications, but eventually the L-function values are related to class groups. This method allows proofs of broad results, but necessarily focuses on the local versions of the conjectures. One of its main drawbacks is that the lack of an analog of the Main Conjecture when $p = 2$ impedes proving the global versions using Iwasawa theory. Rather, much of the progress has resulted in partial proofs only of the "odd parts" of the conjectures. Apart from the particularly problematic behavior of the prime number 2, further difficulties are introduced by the common practice of decomposing modules into their isotypic components; this prevents analyzing the p-primary parts of the conjectures for prime numbers p dividing the order of the Galois group.

It is desirable, then, to have an arithmetic description of the values of Artin L-functions associated with characters of order larger than 2. Such a description can provide information that is lost in the process of ascending an Iwasawa tower,

using Iwasawa theory, and then descending again. It can also provide more direct and conceptually simpler proofs. In particular, it can provide information regarding the 2-primary parts of these conjectures. Furthermore, the arithmetic description of the values of L-functions associated with quadratic extensions has many applications apart from the Brumer and Brumer-Stark conjectures, and it is possible that a description of other L-function values would be applicable in these instances as well.

In this chapter, we will develop expressions describing the values at $s = 0$ of Artin L-functions for some characters of order greater than two. Along the way, we will give applications of these expressions, proving some formulas about divisibility of class numbers. In particular, we shall prove a generalization of Kummer's Reflection Theorem.

By the inflation property of Artin L-functions, L-functions of general Abelian extensions can be identified with L-functions associated with cyclic subextensions. We will study cyclic extensions of order $2^m p^n$, where p is a prime number. The value at $s = 0$ of an L-function for such an extension lies in a cyclotomic field. A description of such an L-function value will be given in terms of the arithmetic of the fields K and k defining the extension. For a rational L-function value, this description involves the order of a class group and the order of a group of roots of unity. As we shall see, for an L-function whose value lies in the cyclotomic field $\mathbb{Q}(\zeta_n)$, the description involves arithmetically meaningful groups which can be given $\mathbb{Z}(\zeta_n)$-module structures. In this context, the role of the order of a finite $\mathbb{Z}$-module is played by the Fitting ideal of a finite $\mathbb{Z}(\zeta_n)$-module.

4.2 L-values for quadratic extensions

Our arithmetic expressions for the values of L-functions at $s = 0$ will be derived from the arithmetic expression for the value of the L-function of a quadratic extension. We will use a variant of this expression given by John Tate in his proof of the Brumer-Stark conjecture for quadratic extensions ([59, §3, case (c)]). Let K/k be a quadratic extension of number fields, and let S be a set of places of k containing

the Archimedean places and the prime ideals that ramify in K. We denote S-class group of K (k) by $\mathrm{Cl}_{K,S}$ ($\mathrm{Cl}_{k,S}$). These are formed by taking the quotient of the ideal class group by the subgroup generated by the classes of the ideals in S. Let τ be the generator of $\mathrm{Gal}(K/k)$, and let χ be the nontrivial character on $\mathrm{Gal}\,(K/k)$. Let W be the number of roots of unity in K.

If any prime of S splits in K/k, then $L_{K/k,S}\,(0,\chi) = 0$ and $\theta_{K/k,S} = 0$ by property 2 of L-function evaluators in Section 3.1. Otherwise, Tate's expression is

$$L_{K/k,S}(0,\chi) = \frac{2^{|S|-1}\,|\mathrm{Coker}|}{W}, \tag{4.1}$$

where "Coker" is the cokernel of the canonical map $\mathrm{Cl}_{k,S} \to \mathrm{Cl}_{K,S}$ given by lifting ideals. It follows that

$$\theta_{K/k,S} = \frac{2^{|S|-1}\,|\mathrm{Coker}|}{W}\frac{1-\tau}{2}. \tag{4.2}$$

A different expression for the value of the L-function is often presented, with the minus class number h^- appearing instead of $|\mathrm{Coker}|$. This is obtained by writing $L_{K/k,S}(s,\chi)$ as a ratio of zeta functions multiplied by fudge factors corresponding to primes in S. One then applies the analytic class number formula and rewrites the quotient h/h^+ that appears as h^-. However, the power of 2 appearing in the resulting formula is complicated. The advantage of Tate's formula is that although Coker is more cumbersome than h^-, the power of 2 appearing in Tate's formula is simple. This becomes especially important for proving (BS_2) for quadratic extensions. In fact, Tate's expression (4.1) is only valid when all of the places in S are nonsplit in K. One can verify that $|\mathrm{Coker}|$ and h^- differ only by a power of 2 in this case.

4.3 Norms of L-values for degree 2^m extensions

In this section, we begin the project outlined in section 4.1 by analyzing the case where G is cyclic of order $2^m, m \geq 1$. The method will be a model for those used later in this chapter.

Let k_m/k_0 be a cyclic extension of degree 2^m with Galois group G. We denote the group of complex-valued characters on G by $\widehat{G}$. Assume that k_m is totally

complex and k_0 is totally real. For r such that $1 \leq r \leq m-1$, let k_r/k_0 be the unique subextension of k_m/k_0 of degree 2^r. Fix a generator σ of G. Let $\tau = \sigma^{2^{m-1}}$ be the element of G of order 2; τ is the complex conjugation corresponding to each Archimedean place of K. Thus, all of the fields k_r with $1 \leq r \leq m-1$ are totally real. Let χ be a generator of $\widehat{G}$, and let ζ_{2^m} be the primitive 2^mth root of unity such that $\chi(\sigma) = \zeta_{2^m}$. Finally, let $W = |\mu|$ be the cardinality of the group of roots of unity in k_m.

Let S_0 be a set of places of k_0 including the Archimedean places. For each integer r with $1 \leq r \leq m$, let S_r be the set of places of k_r lying above the places in S_0. Finally, for $0 \leq r \leq m-1$, let $\theta_r = \theta_{k_m/k_r,S_r}$. By property 2 of L-function evaluators in Section 3.1, we may write

$$\theta_0 = \left(\sum_{i=0}^{2^{m-1}-1} a_i \sigma^i \right) \frac{1-\tau}{2}, \qquad a_i \in \mathbb{Q}.$$

By property 3 of equivariant L-functions from the same section,

$$\begin{aligned} \theta_1 &= \theta_0 \, t_{\chi^{2^{m-1}}}(\theta_0) \\ &= \left(\sum_{i=0}^{2^{m-1}-1} a_i \sigma^i \right) \left(\sum_{i=0}^{2^{m-1}-1} (-1)^i a_i \sigma^i \right) \frac{1-\tau}{2}. \end{aligned}$$

Thus, applying the $\mathbb{C}$-linear extension of χ, we find that

$$\chi(\theta_1) = N_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}\left(\zeta_{2^{m-1}}\right)}\left(\chi(\theta_0)\right).$$

Alternatively,

$$\mathrm{N}_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}\left(\zeta_{2^{m-1}}\right)} L_{k_m/k_0,S_0}(0,\psi) = L_{k_m/k_1,S_1}(0,\psi),$$

for all generating characters ψ of $\widehat{G}$. While we obtained this result from the inductive property of equivariant L-functions, it also follows from the inductive property of Artin L-functions.

We find inductively that the elements $\chi(\theta_r)$ form a norm-coherent sequence, meaning

$$\chi(\theta_r) = \mathrm{N}_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}\left(\zeta_{2^{m-r}}\right)}\left(\chi(\theta_0)\right)$$

for $1 \leq r \leq m-1$. In particular,

$$\chi(\theta_{m-1}) = N_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}}(\chi(\theta_0)). \tag{4.3}$$

Next, assume that S_0 contains the prime ideals that ramify in k_m/k_0, and assume that no place in S_0 splits completely in k_m. Since G is cyclic and no place of S_0 splits completely in k_m, no place in S_{m-1} splits completely in k_m. Thus, since k_m/k_{m-1} is a quadratic extension, (4.2) shows that

$$N_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}}(\chi(\theta_0)) = \frac{2^{|S_{m-1}|-1}\,|\mathrm{Coker}|}{W} \tag{4.4}$$

where Coker is the cokernel of the canonical map $\mathrm{Cl}_{k_{m-1},S_{m-1}} \to \mathrm{Cl}_{k_m,S_m}$. Alternatively,

$$N_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}}\left(L_{K/k,S}(0,\chi)\right) = \frac{2^{|S_{m-1}|-1}\,|\mathrm{Coker}|}{W}$$

for all generating characters χ of $\widehat{G}$. We remark that this norm is positive.

We denote the absolute norm on ideals of $\mathbb{Q}(\zeta_{2^m})$ by $\mathfrak{N}$. We will now determine $\mathfrak{N}\left(\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)\right)$. The group μ is annihilated by $1+\tau$. It is therefore a module over $\mathbb{Z}[G]/(1+\tau)$. Lemma 2.3.4 shows that the $\mathbb{Z}$-linear extension of χ gives a ring isomorphism

$$\chi : \mathbb{Z}[G]/(1+\tau) \cong \mathbb{Z}[\zeta_{2^m}]. \tag{4.5}$$

Thus, χ provides μ with the structure of a module over the Dedekind domain

$$\mathcal{O} := \mathbb{Z}[\zeta_{2^m}].$$

Being a cyclic group, μ is also a cyclic $\mathcal{O}$-module. By property 3 and property 6 of Fitting ideals in Section 2.4, it follows that

$$W = \mathfrak{N}(\mathrm{Fit}_{\mathcal{O}}(\mu)) = \mathfrak{N}(\mathrm{Ann}_{\mathcal{O}}(\mu)) = \mathfrak{N}\left(\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\right)\right). \tag{4.6}$$

Let us summarize what we have now determined in a proposition.

Proposition 4.3.1. *Let notation be that from the beginning of this section. If χ generates $\widehat{G}$, then*

$$N_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}}\left(L_{k_m/k_0,S_0}(0,\chi)\right) = \frac{2^{|S_{m-1}|-1}\,|\mathit{Coker}|}{W},$$

where "Coker" is the cokernel of the canonical map $\mathrm{Cl}_{k_{m-1},S_{m-1}} \to \mathrm{Cl}_{k_m,S_m}$. *In addition,*

$$\mathfrak{N}\left(\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\theta_0\right)\right) = 2^{|S_{m-1}|-1}\left|\mathrm{Coker}\right|.$$

We will now present an alternative version of the second formula in the proposition. The ideal class group of k_m is a $\mathbb{Z}[G]$-module. Since each place of k_m lying above a place in S_0 is in S_m, the subgroup of the ideal group of k_m supported above S_m is stable under the action of G. Since the group of lifts of ideals from k_{m-1} to k_m is also stable under G, the quotient group Coker is also a $\mathbb{Z}[G]$-module. Given a representative $\mathfrak{a}$ of a class in Coker, the ideal $\mathfrak{a}^{1+\tau}$ is the lift of an ideal from k_{m-1}, hence is trivial in Coker. Thus, Coker is a module over $\mathbb{Z}\left[G\right]/(1+\tau)$. Coker is therefore an $\mathcal{O}$-module through the isomorphism (4.5).

Let (λ) be the prime ideal of $\mathcal{O}$ dividing 2. By property 6 of Fitting ideals and equation (4.6), we may rewrite the second equation in the above proposition as

$$\mathfrak{N}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mu\right)\chi\left(\theta_0\right)\right) = \mathfrak{N}\left((\lambda)^{|S_{m-1}|-1}\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right)\right). \tag{4.7}$$

Since these ideals have the same absolute norm, it is natural to ask if the ideals themselves are conjugate. Observe that the above Fitting ideals depend on the choice of character providing the $\mathcal{O}$-module structure. As χ runs through the characters that generate $\widehat{G}$, the Fitting ideals run through a set of conjugate ideals in $\mathcal{O}$. A consequence of Brumer's conjecture for k_m/k_0 is that $\mathrm{Fit}_{\mathcal{O}}\left(\mu\right)\chi\left(\theta_0\right)$ annihilates Coker when both μ and Coker have $\mathcal{O}$-module structures provided by the character χ. Thus, we pose the question:

Question. *Let notation be that from the beginning of this section. Fix a character* χ *that generates* $\widehat{G}$. *Is it true that*

$$Fit_{\mathcal{O}}\left(\mu\right)\chi\left(\theta_0\right) = \lambda^{|S_{m-1}|-1}Fit_{\mathcal{O}}\left(Coker\right), \tag{4.8}$$

if μ *and Coker are both endowed with the* $\mathcal{O}$*-module structures induced by* χ *?*

In what follows, if k_m/k_0 is any cyclic extension of degree 2^m and S_0 is a set of places of k_0 containing the Archimedean places and the prime ideals that ramify in k_m, we will refer to this question for the extension k_m/k_0 and the set S_0 as

$\mathrm{Q}_{2^m}(k_m/k_0, S_0)$. If $\mathrm{Q}_{2^m}(k_m/k_0, S_0)$ has an affirmative answer for the minimal set $S_0 = S_0^{\min}$, then it also does if S_0 is any set containing $S_0^{\min}$. We will refer to this special case as $\mathrm{Q}_{2^m}(k_m/k_0)$ without mentioning a set S_0. If p is a prime number, then the question of whether the factors supported at primes dividing p on each side of equation 4.8 will be referred to as the p-primary part of $\mathrm{Q}_{2^m}(k_m/k_0, S_0)$. When $m = 1$, equation 4.8 says precisely that the principal ideals generated by the two sides of equation (4.1) are equal. We note that the relation (4.8), when valid, implies that $\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})$ and $\mathrm{Fit}_{\mathcal{O}}(\mu)$ represent the same class in the ideal class group of $\mathcal{O}$.

Example. Let $k_0 = \mathbb{Q}$ and $k_m = \mathbb{Q}(\zeta_p)$, where $p = 2^m + 1$ is a Fermat prime. Let $S_0 = S^{\min}$. In this case, it is known that ([60, Theorem 4.2])

$$L_{k_m/k_0, S_0}(0, \chi) = -B_{1,\chi},$$

where $B_{1,\chi}$ denotes a generalized Bernoulli number. If χ is odd, it follows that

$$N_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}}\left(L_{k_m/k_0, S_0}(0, \chi)\right) = \prod_{\psi \,\mathrm{odd}} -B_{1,\psi}.$$

The set $S^{\min}$ of places of $\mathbb{Q}$ consists of the Archimedean place and the prime ideal (p). The set S_{m-1} then contains 2^{m-1} Archimedean places and the lone prime ideal of k_{m-1} lying above p. Thus, $|S_{m-1}| - 1 = 2^{m-1}$. Finally, since the prime ideal lying above p in the fields k_{m-1} and k_m is principal, $|\mathrm{Coker}| = h^-$. Putting all of this together with the first formula of Proposition 4.3.1, we find the well-known expression for the relative class number of K as a product of generalized Bernoulli numbers ([60, Theorem 4.17]):

$$h_{k_m}^- = W \prod_{\psi \,\mathrm{odd}} \left(-\frac{1}{2} B_{1,\psi}\right).$$

Now let us specialize to the case where

$$2^m + 1 = p = 257.$$

257 is an irregular prime, so the 257-primary part of Coker is nontrivial. Since $257 \equiv 1 \pmod{2^m}$, the prime ideal (257) of $\mathbb{Q}$ splits completely in $\mathbb{Q}(\zeta_{2^m})$. In

formula (4.7), each of $\mathrm{Fit}_{\mathcal{O}}(\mu)\chi(\theta_0)$ and $\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})$ must be divisible by one of the 128 prime ideals of $\mathbb{Q}(\zeta_{2^m})$ lying above 257. It does not follow immediately from formula (4.7) that these must be the same prime ideal. Thus, formula (4.8) is possibly a stronger statement than formula (4.7).

Although formula (4.7) does not immediately imply formula (4.8), when p is a prime number that is inert in $\mathbb{Q}(\zeta_{2^m})$, equation (4.7) implies that the p-primary parts of both sides of (4.8) are equal. Similarly, if (λ) is the prime ideal of $\mathbb{Q}(\zeta_{2^m})$ dividing 2, then the (λ)-primary parts of both sides of (4.8) are equal.

Proposition 4.3.2. $\mathrm{Q}_{2^m}(k_m/k_0)$ *has an affirmative answer when* $m = 1$.

All of the above claims follow from the fact that (4.7) implies the p-primary part of $\mathrm{Q}_{2^m}(k_m/k_0)$ for any prime p having only one prime divisor in $\mathbb{Q}(\zeta_{2^m})$.

We can say more when Coker is a cyclic $\mathcal{O}$-module.

Proposition 4.3.3. *Let notation be that from the beginning of the section. If* (B) *is true for the extension* k_m/k_0 *and the set* S_0*, and if Coker is cyclic as an* $\mathcal{O}$*-module, then equation* (4.8) *is valid.*

Proof. Since (B) holds for the extension k_m/k_0 and the set S_0, we know that

$$\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\,\theta_0 \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{Cl}_{k_m}) \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{Coker}).$$

Let χ be a generator of $\widehat{G}$. Then χ provides both μ and Coker with $\mathcal{O}$-module structures, and

$$\mathrm{Ann}_{\mathcal{O}}(\mathrm{Coker}) = \chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{Coker})\right).$$

Thus,

$$\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu)\,\theta_0\right) \subseteq \mathrm{Ann}_{\mathcal{O}}(\mathrm{Coker}).$$

Since μ and Coker are cyclic, we find that

$$\mathrm{Fit}_{\mathcal{O}}(\mu)\chi(\theta_0) \subseteq \mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker}).$$

Therefore, there exists an integral ideal $\mathfrak{a}$ in $\mathcal{O}$ such that

$$\mathrm{Fit}_{\mathcal{O}}(\mu)\chi(\theta_0) = \mathfrak{a}\,\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker}).$$

Taking absolute norms and using equation (4.7), we find that $\mathfrak{a} = (\lambda)^{|S_{m-1}|-1}$, so relation (4.8) holds. □

4.4 L-values for degree 2^m extensions

Obtaining a statement as precise as (4.8) in general seems to be beyond the capabilities of the above methods. The problem is that the analytic class number formula can only provide information about a product of L-function values. One cannot rely on this formula alone to obtain information about the values of individual L-functions. However, we may look to Tate's proof of the full Brumer-Stark conjecture for certain quartic extensions (item 5 in the list in Subsection 3.4.2) for a hint as to how partial results can be obtained in this direction. Tate's result applies to the situation where there exists a field k' such that $k' \subset k \subset K$ is a tower of fields with K/k' Galois and non-Abelian of order 8 and with K/k Abelian of order 4. He then manages to prove the full Brumer-Stark conjecture for K/k. To accomplish this, he shows that $\chi\left(\theta_{K/k}\right)$ is rational, and then equation (4.1) and a representation theoretic argument show that $\theta_{K/k}$ annihilates the ideal class group of K. When K/k is cyclic of order 4, let us reconsider his proof in view of the discussion in Section 4.3. We can describe what is occurring by saying that the added structure imposed on Coker by virtue of its being a module over $\mathrm{Gal}\left(K/k'\right)$ places a restriction on its Fitting ideal when considered as an $\mathcal{O}$-module. It turns out that this restriction is enough to prove (4.8) in this case.

In this section, we will generalize this idea to obtain more refined information about values of L-functions than that given by Proposition 4.3.1. We use the same notation as in Section 4.3. In addition, we assume that there exists a field k' such that $k' \subset k_0 \subset k_m$, with k_m/k' and k_0/k' Galois. Assume further that S_0 is stable under the action of $\mathrm{Gal}\left(k_0/k'\right)$ on the ideal group of k_0. Let $H = \mathrm{Gal}\left(k_0/k'\right)$. Then H acts on $\mathbb{Z}[G]$, as described in Section 2.7. Since the action of H fixes the unique element τ of G of order 2, we have an induced homomorphism

$$\phi\colon H \to \mathrm{Aut}_{\mathbb{Z}}\left(\mathbb{Z}\left[G\right]/(1+\tau)\right) \cong \mathrm{Aut}_{\mathbb{Z}}\left(\mathcal{O}\right) \cong \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{2^m}\right)/\mathbb{Q}\right).$$

We need a preliminary lemma.

Lemma 4.4.1. *If $|\phi(H)| \geq 2$, then $W = 2$.*

Proof. Since $|\phi(H)| \geq 2$, there exists an h in H that acts nontrivially on G. Choose an element $\tilde{h}$ in $\mathrm{Gal}\left(K/k'\right)$ that restricts to h. Set $h \cdot \sigma = \sigma^c$, where c is an integer

such that $c \not\equiv 1 \pmod{2^m}$. If ζ is a primitive Wth root of unity, assume that $\tilde{h}(\zeta) = \zeta^r$ and $\sigma(\zeta) = \zeta^s$ where $(rs, W) = 1$. Then

$$\sigma^c(\zeta) = \tilde{h}\sigma\tilde{h}^{-1}(\zeta) = \zeta^{rsr^{-1}} = \zeta^s. \tag{4.9}$$

Since $c \not\equiv 1 \pmod{2^m}$, we can find an integer k such that

$$2^k(c-1) \equiv 2^{m-1} \pmod{2^m}.$$

Then

$$\sigma^{2^k c}(\zeta) = \tau\sigma^{2^k}(\zeta) = \zeta^{-s^{2^k}}.$$

On the other hand, from (4.9), we have

$$\sigma^{2^k c}(\zeta) = \zeta^{s^{2^k}},$$

so that

$$s^{2^k} \equiv -s^{2^k} \pmod{W}.$$

Since $(s, W) = 1$, it follows that $W = 2$. □

The principal result of this section is the following proposition.

Proposition 4.4.2. *With notation as above, $\chi(\theta_0)$ is an element of $\mathbb{Q}(\zeta_{2^m})^{\phi(H)}$. Furthermore, if $\lambda = 1 - \zeta_{2^m}$, then $Fit_{\mathcal{O}}(Coker)$ can be written as a power of the ideal (λ) times the lift of an ideal of $\mathbb{Q}(\zeta_{2^m})^{\phi(H)}$.*

Proof. By the preceding lemma and equation (4.6), we know that $\mathrm{Fit}_{\mathcal{O}}(\mu)$ is the prime ideal of $\mathcal{O}$ lying above 2, hence is fixed by every automorphism of $\mathbb{Q}(\zeta_{2^m})$. We write

$$\theta = \left(\sum_{i=0}^{2^m-1} a_i\sigma^i\right).$$

Let h be in H, and let $h \cdot \sigma = \sigma^c$. Let $\tilde{h}$ be an element of $\mathrm{Gal}(k_m/k')$ that restricts to h. For any i such that $0 \leq i \leq 2^m - 1$, we have

$$h \cdot \sigma^i = \sigma^{ic}.$$

By Proposition 3.2.2, we have an equality of partial zeta functions

$$\zeta_{k_m/k_0,S_0}\left(s, \sigma^i\right) = \zeta_{k_m/k_0,S_0}\left(s, \sigma^{ic}\right)$$

for $i = 0, \ldots, 2^m - 1$. Thus, $a_i = a_{ic}$ for all i (where it is understood that a_{ic} stands for the coefficient of σ^{ic} even if $ic \notin [0, 2^m - 1]$). It follows that

$$\chi(\theta) = \sum_{i=0}^{2^m-1} a_i \zeta_{2^m}^i$$

is fixed by $\phi(h)$, which is the automorphism of $\mathbb{Q}(\zeta_{2^m})$ that sends ζ_{2^m} to $\zeta_{2^m}^c$. Since h was an arbitrary element of H, this proves the first part of the proposition.

Since S_0 was assumed to be stable under the action of $\mathrm{Gal}(k_m/k')$, Coker is a $\mathbb{Z}[\mathrm{Gal}(k_m/k')]$-module. If h is in H, Proposition 2.7.1 shows that

$$f_h\left(\mathrm{Fit}_{\mathbb{Z}[G]}(\mathrm{Coker})\right) = \mathrm{Fit}_{\mathbb{Z}[G]}(\mathrm{Coker}).$$

We apply the map $\chi\colon \mathbb{Z}[G] \to \mathbb{Z}(\zeta_{2^m})$ to this equation. Since χ is surjective, property 5 of Fitting ideals shows that

$$\phi(h)(\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})) = \mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker}).$$

Therefore, $\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})$ is fixed by $\phi(H)$. The second statement now follows from the fact that (2) is the only prime ideal of $\mathbb{Q}$ that ramifies in $\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}$. □

Corollary 4.4.3. *Write*

$$L = \mathbb{Q}(\zeta_{2^m})^{\phi(H)}.$$

Assume that $d = |\phi(H)| = [\mathbb{Q}(\zeta_{2^m}) : L] \geq 2$. *Also, set*

$$Fit_{\mathcal{O}}(Coker) = (\lambda)^e \mathfrak{a}\mathcal{O},$$

where $\mathfrak{a}$ *is an integral ideal of* L. *Let* $\mathfrak{N}_L$ *denote the absolute norm on ideals of* L. *Then*

$$\mathfrak{N}_L(\chi(\theta_0)) = 2^{\frac{|S_{m-1}|+e-2}{d}} \mathfrak{N}_L(\mathfrak{a}).$$

In particular, equation (4.8) *is valid when* $L = \mathbb{Q}$.

Proof. Since $\chi(\theta_0)$ and $\mathfrak{a}$ are in L and $\mathrm{Fit}_{\mathcal{O}}(\mu) = (\lambda)$ by lemma 4.4.1, we can rewrite (4.7) as

$$(\mathfrak{N}_L(\chi(\theta)))^d = 2^{|S_{m-1}|+e-2} (\mathfrak{N}_L(\mathfrak{a}))^d.$$

Therefore, $|S_{m-1}| + e - 2$ is divisible by d and the corollary follows. □

Corollary 4.4.4. *If $h_S = |\mathrm{Cl}_{k_m,S_m}|$ is the S_m-class number of k_m, then*

$$2^r \mid h_S,$$

where r is the smallest nonnegative residue of $2 - |S_{m-1}| \pmod d$.

Proof. By the definition of e, |Coker| is divisible by 2^e. From the proof of the preceding corollary,

$$e \equiv 2 - |S_{m-1}| \pmod d. \qquad \square$$

Remark. If K/k is a cyclic extension of number fields, then Lemma 4.1 in Chapter 13 of [32] gives a formula for the size of the part of Cl_K fixed by $\mathrm{Gal}(K/k)$. Lang summarizes its content, saying "The next lemma implies that highly ramified primes have a tendency to generate independent ideal classes, and that the obstruction to this is contained in some cohomology." A weaker result is Proposition 2 in [35]. In the course of the proof, the authors show that if K is a CM field and K^+ is its maximal totally real subfield, then the relative class number of K is divisible by $2^t - 1$, where t is the number of prime ideals that ramify in K/K^+. If it is not always true that

$$|S_{m-1}| \equiv 2 \pmod d, \tag{4.10}$$

then the above corollary is remarkable in that it implies a connection between the number of primes ramifying in a cyclic extension K/k of degree 2^m which is part of a larger non-Abelian extension and the number of classes in the S-ideal class group of K when S contains the primes that ramify in K/k. In other words, even after taking the quotient of the ideal class group of K by the classes of the prime ideals that ramify in K/k, the presence of a suitable number of such prime ideals will ensure that there are still more classes in Cl_K with 2-power order. Perhaps it is more plausible that the congruence (4.10) can be shown to hold, making this corollary devoid of content. However, Corollary 4.7.4 in Section 4.7 is a similar result, and the example provided immediately following it is a nontrivial application. It might seem strange that one can add primes to S_{m-1}, thereby varying the divisibility result in the corollary. This will be elucidated somewhat in the following example.

Example. Let k_2 be the splitting field of the polynomial

$$x^8 + 72x^6 + 1332x^4 + 2448x^2 + 36.$$

The following information was determined using PARI/GP. k_2 is totally complex and $\mathrm{Gal}(k_2/\mathbb{Q})$ is isomorphic to the group of quaternions. The real quadratic field $k_0 = \mathbb{Q}\left(\sqrt{2}\right)$ is contained in k_2, and k_2/k_0 is cyclic of degree 4. There are two prime ideals in k_0 that ramify in k_2, namely (3) and the prime ideal dividing 2. Both of these ideals are totally ramified in k_2/k_0. Also, k_2 has class number 2, and the nontrivial class is represented by the prime ideal dividing 2. Since $\mathrm{Gal}(k/\mathbb{Q})$ acts nontrivially on G, the degree d in the above corollary is 2.

The minimal set S_0 that we may choose consists of the two Archimedean places of k_0, the prime ideal (3), and the prime lying above 2. With this choice, the set S_1 contains four Archimedean places and two finite places. Let $\mathfrak{P}$ be a prime ideal of k_2 dividing the rational prime $p \neq 2, 3$. Since the decomposition group of $\mathfrak{P}$ over $\mathbb{Q}$ is cyclic, there are four possibilities:

1. p splits in $k_0/\mathbb{Q}$ and remains inert in k_2/k_0;
2. p is inert in $k_0/\mathbb{Q}$, splits in k_1/k_0, and is inert in k_2/k_1;
3. p splits completely in the biquadratic extension $k_1/\mathbb{Q}$ and remains inert in k_2/k_1;
4. p splits completely in $k_2/\mathbb{Q}$.

Let $\mathfrak{p}$ be the prime ideal of k_0 divisible by $\mathfrak{P}$. In each of the cases 2, 3, and 4, adjoining $\mathfrak{p}$ to S_0 increases $|S_1|$ by an even number. In the first case, we must adjoin both prime ideals of k_0 dividing p to S_0 to produce a set that is stable under the action of $\mathrm{Gal}\,(k_2/\mathbb{Q})$ (since $\mathrm{Gal}\,(k_2/\mathbb{Q})$ acts nontrivially on the Frobenius automorphism $(\mathfrak{p}, k_2/k_0)$). Therefore, the set S_1 in this example must have even cardinality. It follows that $r = 0$, so the congruence (4.10) holds and the corollary says nothing about this example. In fact, the above information shows that $h_S = 1$ in this case. No example has been found where (4.10) fails to hold.

4.5 Norms of L-values for degree $2^m p$ extensions

Let p be an odd prime number. In this section, we will use the expressions from Proposition 4.3.1 to derive similar ones for cyclic extensions of degree $2^m p$. Let k_0 be a number field, and let K_1 be a cyclic extension field of k_0 of degree $2^m p$ with Galois group G. We assume that k_0 is totally real and K_1 is totally complex. If k_1 and K_0 are the extensions of k_0 of degrees p and 2^m respectively contained in K_1, then k_1 is totally real and K_0 and K_1 are CM fields. Let K_0^+ and K_1^+ be the maximal totally real subfields of K_0 and K_1 respectively. Let $S^{\min}$ denote the set of places of k_0 consisting of the Archimedean places and the prime ideals of k_0 that ramify in K_1. Let S^{ns} denote the set consisting of the places in $S^{\min}$ that do not split completely in the extension K_0/k_0, and note that S^{ns} contains the Archimedean places.

Let σ be a generator of $H = \mathrm{Gal}\,(K_1/K_0)$, let σ' be a generator of $H' = \mathrm{Gal}\,(K_1/k_1)$, and let $\tau = {\sigma'}^{2^{m-1}}$ denote complex conjugation. Let χ be a generator of $\widehat{G}$. Let ζ_p and ζ_{2^m} be the primitive pth and 2^mth roots of unity such that

$$\chi^{2^m}(\sigma) = \zeta_p$$

and

$$\chi^p(\sigma') = \zeta_{2^m}.$$

We denote the number of roots of unity in K_0 by W_0 and the number of roots of unity in K_1 by W_1.

If $k_0 = \mathbb{Q}$, then at least one prime ideal of k_0 ramifies in K_1. If $k_0 \neq \mathbb{Q}$, then $S^{\min}$ contains at least two Archimedean places. It follows that $\left|S^{\min}\right| \geq 2$. Thus, for each even integer $2t$,

$$L_{K_1/k_0,S^{\min}}\left(0, \chi^{2t}\right) = 0,$$

since χ^{2t} is an even character (see [58, Chapter I, Proposition 3.4]). The odd characters fall into two equivalence classes under the equivalence relation from Section 3.3: $\mathfrak{C}_{2^m p}$ comprises the characters of order $2^m p$, and $\mathfrak{C}_{2^m}$ comprises the characters of order 2^m. To simplify notation, we write $\theta^{\min}$ and θ^{ns} instead of $\theta_{K_1/k_0,S^{\min}}$ and $\theta_{K_1/k_0,S^{\mathrm{ns}}}$. Similarly, we write $\theta_{\mathfrak{C}}^{\min}$ and $\theta_{\mathfrak{C}}^{\mathrm{ns}}$, where the class $\mathfrak{C}$ is either $\mathfrak{C}_{2^m}$ of $\mathfrak{C}_{2^m p}$.

We can decompose $\theta^{\min}$ as

$$\theta^{\min} = \theta^{\min}_{\mathfrak{C}_{2^m p}} + \theta^{\min}_{\mathfrak{C}_{2^m}}. \tag{4.11}$$

Any primes in $S^{\min} \setminus S^{\mathrm{ns}}$ split completely in K_0/k_0 and are totally ramified in k_1/k_0. If $\mathfrak{p}$ is such a prime and the character χ^i is nontrivial on $\mathrm{Gal}\,(K_1/K_0)$, then the inertia group of $\mathfrak{p}$ acts nontrivially on $\mathbb{C}$ through the representation corresponding to χ^i. Comparing with equation (1.2), we see that the corresponding Euler factor in $L_{K_1/k_0,S^{\min}}(s,\chi^i)$ is trivial. It follows that for each character χ^i in $\mathfrak{C}_{2^m p}$,

$$L_{K_1/k_0,S^{\min}}\left(0,\overline{\chi}^i\right) = L_{K_1/k_0,S^{\mathrm{ns}}}\left(0,\overline{\chi}^i\right),$$

and hence,

$$\theta^{\min}_{\mathfrak{C}_{2^m p}} = \theta^{\mathrm{ns}}_{\mathfrak{C}_{2^m p}}.$$

Thus, we may write

$$\theta^{\mathrm{ns}} = \theta^{\min}_{\mathfrak{C}_{2^m p}} + \theta^{\mathrm{ns}}_{\mathfrak{C}_{2^m}}. \tag{4.12}$$

We will now see that $\theta^{\mathrm{ns}}_{\mathfrak{C}_{2^m}}$ is nonzero. Property 1 of components of L-function evaluators from Section 3.3 shows that

$$\pi\left(\theta^{\mathrm{ns}}_{\mathfrak{C}_{2^m}}\right) = \theta_{K_0/k_0,S^{\mathrm{ns}}}, \tag{4.13}$$

where π is the $\mathbb{C}$-linear extension of the projection map $G \to \mathrm{Gal}\,(K_0/k_0)$. Let K_0^+ be the maximal real subfield of K_0, and let S_0^+ be the set of places of K_0^+ lying above those in S^{ns}. Formula (4.3) shows that for each generating character ψ of the character group of $\mathrm{Gal}\,(K_0/k_0)$,

$$\psi\left(\theta_{K_0/K_0^+,S_0^+}\right) = N_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}}\left(\psi\left(\theta_{K_0/k_0,S^{\mathrm{ns}}}\right)\right).$$

Since no place in S^{ns} splits completely in K_0/k_0 and K_0/k_0 is cyclic, no place in S_0^+ splits in K_0/K_0^+. In addition, S_0^+ contains all of the Archimedean places of K_0^+ and all of the prime ideals of K_0^+ that ramify in K_0. Therefore, Tate's expressions (4.1) and (4.2) for the value of the L-function and the L-function evaluator of a quadratic extension apply to $\theta_{K_0/K_0^+,S_0^+}$. They show that the left side of the above equation is nonzero, so that $\theta^{\mathrm{ns}}_{\mathfrak{C}_{2^m}}$ is nonzero. The point of this discussion is that

we can analyze the term $\theta^{\min}_{\mathfrak{C}_{2^m p}}$ appearing in expression (4.11) for $\theta^{\min}$ by analyzing the exact same term appearing in the expression (4.12) for θ^{ns}, and the term $\theta^{\mathrm{ns}}_{\mathfrak{C}_{2^m}}$ in expression (4.12) is nonzero.

For this analysis, we will need to consider the $\mathbb{C}$-linear extensions of the characters $\chi^a \colon \mathbb{C}[G] \to \mathbb{C}$, as well as their restrictions to $\mathbb{C}[H]$. When p divides a, $\chi^a \big|_{\mathbb{C}[H]}$ is just the augmentation map on $\mathbb{C}[H]$. We will use t_a to denote the twist by χ^a. By property 3 of equivariant L-functions in Section 3.1, if $S^{\mathrm{ns}}_{k_1}$ is the set of places of k_1 sitting above the set of places in S^{ns}, then

$$\theta_{K_1/k_1, S^{\mathrm{ns}}_{k_1}} = \prod_{a=0}^{p-1} t_{2^m a}\left(\theta^{\mathrm{ns}}\right).$$

Following the notation in [47, Proposition 3.1], we let

$$\beta = \prod_{a=1}^{p-1} t_{2^m a}\left(\theta^{\mathrm{ns}}\right),$$

so we have just removed the factor θ^{ns} from the earlier product.

Since $G = H' \times H$, equation (2.3) gives an isomorphism

$$\mathbb{C}[G] \cong \mathbb{C}[H'][H].$$

Under this identification, write

$$\theta^{\min}_{\mathfrak{C}_{2^m p}} = \sum_{i=0}^{p-1} a_i \sigma^i,$$

where the coefficients a_i are in $\mathbb{C}[H']$. If ϕ is in $\widehat{G}$, let ϕ_H and $\phi_{H'}$ denote the restrictions of ϕ to H and H'. By the definition of $\theta^{\min}_{\mathfrak{C}_{2^m p}}$ and property 6 of idempotents from Section 2.3, we have the equality in $\mathbb{C}[H'][H]$

$$\theta^{\min}_{\mathfrak{C}_{2^m p}} = \sum_{\phi \in \mathfrak{C}_{2^m p}} L_{K_1/k_0, S^{\min}}\left(0, \phi^{-1}\right) e_{\phi_{H'}} e_{\phi_H}. \tag{4.14}$$

By the orthogonality relations,

$$\mathbf{1}_H\left(e_{\phi_H}\right) = 0$$

when $\phi_H \neq \mathbf{1}_H$. Therefore, applying the $\mathbb{C}[H']$-linear extension of the trivial character $\mathbf{1}_H$ to the expression (4.14) gives 0. It follows that $\sum_{i=0}^{p-1} a_i = 0$, so $\theta^{\min}_{\mathfrak{C}_{2^m p}}$ is in the H-relative augmentation ideal of $\mathbb{C}[G]$.

Property 2 of components of L-function evaluators from Section 3.3 shows that we may write

$$\theta^{\mathrm{ns}}_{\mathfrak{C}_{2^m}} = \frac{N_H}{p}\tilde{\theta}^{ns}_0,$$

where $\tilde{\theta}^{\mathrm{ns}}_0$ is a lift of $\theta_{K_0/k_0,S^{\mathrm{ns}}}$ to $\mathbb{C}[G]$. We choose $\tilde{\theta}^{\mathrm{ns}}_0$ to be in the subring $\mathbb{C}[H']$ of $\mathbb{C}[G]$. Thus, we have

$$\theta^{\mathrm{ns}} = \sum_{i=0}^{p-1} a_i\sigma^i + \frac{\tilde{\theta}^{\mathrm{ns}}_0}{p}N_H,$$

where each term is written as en element of $\mathbb{C}[H'][H]$.

We now substitute this expression into the product defining β. The result is a product of sums, and we will first consider the one term found by choosing the first term in each sum when this product is expanded. The result is

$$\prod_{a=1}^{p-1} t_{2^m a}\left(\sum_{i=0}^{p-1} a_i\sigma^i\right). \tag{4.15}$$

For each integer a such that $1 \le a \le p-1$, $t_{2^m a}$ acts as the identity on $\mathbb{C}[H']$. The factor

$$t_{2^m a}\left(\sum_{i=0}^{p-1} a_i\sigma^i\right) = \sum_{i=0}^{p-1} a_i\zeta_p^{ai}\sigma^i$$

in the product (4.15) maps to 0 under the $\mathbb{C}[H']$-linear extension of χ_H^{-a}. As a runs through the integers from 1 to $p-1$, χ_H^{-a} runs through the nontrivial characters on H. Thus, the image of the product (4.15) under the $\mathbb{C}[H']$-linear extension of any nontrivial character on H is 0. Writing this product as a $\mathbb{C}[H']$-linear combination of the idempotents corresponding to the distinct characters on H, we find that it is a multiple of the idempotent corresponding to the trivial character. In other words, we may rewrite (4.15) as

$$\prod_{a=1}^{p-1} t_{2^m a}\left(\sum_{i=0}^{p-1} a_i\sigma^i\right) = cN_H \tag{4.16}$$

for some element c in $\mathbb{C}[H']$.

We can find a more useful expression for c by applying χ^p to the expres-

sion (4.15), which yields

$$\begin{aligned}\chi^p\left(\prod_{a=1}^{p-1} t_{2^m a}\left(\sum_{i=0}^{p-1} a_i\sigma^i\right)\right) &= \chi^p\left(\prod_{a=1}^{p-1}\left(\sum_{i=0}^{p-1} a_i\zeta_p^{ai}\sigma^i\right)\right)\\ &= \prod_{a=1}^{p-1}\left(\sum_{i=0}^{p-1}\chi^p\left(a_i\right)\zeta_p^{ia}\right)\\ &= N_{\mathbb{Q}\left(\zeta_{2^m p}\right)/\mathbb{Q}\left(\zeta_{2^m}\right)}\left(\sum_{i=0}^{p-1}\chi^p\left(a_i\right)\zeta_p^{i}\right).\end{aligned}$$

Applying χ^p to the right side of expression (4.16), it follows that

$$\chi^p(c) = \frac{1}{p} N_{\mathbb{Q}\left(\zeta_{2^m p}\right)/\mathbb{Q}\left(\zeta_{2^m}\right)}\left(\sum_{i=0}^{p-1}\chi^p\left(a_i\right)\zeta_p^{i}\right). \tag{4.17}$$

In summary, when the expression

$$\sum_{i=0}^{p-1} a_i\sigma^i + \frac{\tilde{\theta}_0^{\mathrm{ns}}}{p} N_H$$

is substituted into the product defining β, the resulting expression can be written as

$$cN_H + \alpha,$$

where c is in $\mathbb{C}\left[H'\right]$ and satisfies equation (4.17).

Observe that each term entering into the expression defining α is a product of factors, at least one of which is of the form

$$t_{2^m a}\left(\frac{\tilde{\theta}_0^{\mathrm{ns}}}{p}\right)\cdot t_{2^m a}\left(N_H\right)$$

for some a such that $1 \le a \le p-1$. Since

$$\mathbf{1}_H\left(t_{2^m a}\left(N_H\right)\right) = \sum_{i=0}^{p-1}\zeta_p^i = 0,$$

each such term is in the augmentation ideal in $\mathbb{C}\left[H'\right][H]$. Hence, so is α.

Putting everything together and using the fact that $\sum_{i=0}^{p-1} a_i\sigma^i$ and α are both

in the augmentation ideal of $\mathbb{C}[H'][H]$, we find that

$$\begin{aligned}\theta_{K_1/k_1,S_{k_1}^{\mathrm{ns}}} &= \theta^{\mathrm{ns}}\,\beta \\ &= \left(\sum_{i=0}^{p-1} a_i\sigma^i + \frac{\tilde{\theta}_0^{\mathrm{ns}}}{p}N_H\right)(cN_H+\alpha) \\ &= \left(c\,\tilde{\theta}_0^{\mathrm{ns}}N_H + \sum_{i=0}^{p-1} a_i'\sigma^i\right),\end{aligned}$$

where $\alpha\sum_{i=0}^{p-1} a_i\sigma^i = \sum_{i=0}^{p-1} a_i'\sigma^i$ and $\sum_{i=0}^{p-1} a_i' = 0$ in $\mathbb{C}[H']$. However, $\theta_{K_1/k_1,S_{k_1}^{\mathrm{ns}}}$ is contained in the subalgebra $\mathbb{C}[H']$ of $\mathbb{C}[G]$. It follows that

$$a_i' = -c\,\tilde{\theta}_0^{\mathrm{ns}}.$$

for $1 \le i \le p-1$, and hence,

$$a_0' = (p-1)\,c\,\tilde{\theta}_0^{\mathrm{ns}}.$$

Thus, we find that

$$\theta_{K_1/k_1,S_{k_1}^{\mathrm{ns}}} = pc\,\tilde{\theta}_0^{\mathrm{ns}}.$$

Our initial choices imply that the restriction $\chi_{H'}^p$ is the character on H' satisfying $\chi_{H'}^p(\sigma') = \zeta_{2^m}$. Also, χ^p is trivial on H and can thus be considered as a character on $\mathrm{Gal}(K_0/k_0)$, satisfying $\chi^p\left(\sigma'\,\big|_{K_0}\right) = \zeta_{2^m}$. Thus, $\chi^p\left(\tilde{\theta}_0^{\mathrm{ns}}\right) = \chi^p\left(\theta_{K_0/k_0,S^{\mathrm{ns}}}\right)$. Applying χ^p to both sides of the equation above yields

$$L_{K_1/k_1,S_{k_1}^{\mathrm{ns}}}\left(0,\chi_{H'}^{-p}\right) = p\chi^p(c)\,L_{K_0/k_0,S^{\mathrm{ns}}}\left(0,\chi^{-p}\right).$$

Equation (4.17) then gives

$$N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}(\zeta_{2^m})}\left(\sum_{i=0}^{p-1}\chi^p(a_i)\,\zeta_p^i\right) = \frac{L_{K_1/k_1,S_{k_1}^{\mathrm{ns}}}\left(0,\chi_{H'}^{-p}\right)}{L_{K_0/k_0,S^{\mathrm{ns}}}\left(0,\chi^{-p}\right)}.$$

Let S_0^+ and S_1^+ denote the sets of places in K_0^+ and K_1^+ respectively that lie above places in S^{ns}, and let $S_{K_0}^{\mathrm{ns}}$ and $S_{K_1}^{\mathrm{ns}}$ denote the sets of places of K_0 and K_1 lying above the places in S^{ns}. Also, let Coker_0 and Coker_1 denote the cokernels of the canonical maps $\mathrm{Cl}_{K_0^+,S_0^+} \to \mathrm{Cl}_{K_0,S_{K_0}^{\mathrm{ns}}}$ and $\mathrm{Cl}_{K_1^+,S_1^+} \to \mathrm{Cl}_{K_1,S_{K_1}^{\mathrm{ns}}}$ respectively. If we

now take the norm of each side of the above equation from $\mathbb{Q}(\zeta_{2^m})$ down to $\mathbb{Q}$, then Proposition 4.3.1 shows that

$$N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(\sum_{i=0}^{p-1}\chi^p(a_i)\,\zeta_p^i\right) = 2^{|S_1^+|-|S_0^+|}\frac{W_0}{W_1}\frac{|\mathrm{Coker}_1|}{|\mathrm{Coker}_0|}.$$

Let S^{spl} be the places in K_0 lying above places in S^{ns} that split in k_1/k_0. Then

$$\left|S_1^+\right| - \left|S_0^+\right| = (p-1)\left|S^{\mathrm{spl}}\right|.$$

Furthermore, since $\chi^p(H) = 1$ and $\chi^{2^m}(H') = 1$, we have

$$\chi^{2^m+p}\left(a_i\sigma^i\right) = \chi^p(a_i)\,\zeta_p^i.$$

As $2^m + p$ is relatively prime to both 2^m and p, the character χ^{-2^m-p} generates $\widehat{G}$. It follows that

$$\begin{aligned}
N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(\sum_{i=0}^{p-1}\chi^p(a_i)\,\zeta_p^i\right) &= N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(\chi^{2^m+p}\left(\sum_{i=0}^{p-1}a_i\sigma^i\right)\right)\\
&= N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(\chi^{2^m+p}\left(\theta^{\min}_{\mathfrak{C}_{2^m p}}\right)\right)\\
&= N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(L_{K_1/k_0,S^{\min}}\left(0,\chi^{-2^m-p}\right)\right).
\end{aligned}$$

The characters that generate $\widehat{G}$ are precisely the characters in $\mathfrak{C}_{2^m p}$. By Proposition 3.2.1 and Theorem 3.2.3, as ψ runs through the characters that generate $\widehat{G}$, the values

$$L_{K_1/k_0,S^{\min}}(0,\psi)$$

run through a set of algebraic conjugates in $\mathbb{Q}(\zeta_{2^m p})$ (possibly more than once).

We have arrived at the following description of the L-function evaluator for K_1/k_0:

$$\theta^{\min} = \theta^{\min}_{\mathfrak{C}_{2^m p}},$$

if any prime of k_0 splits completely in K_0 and ramifies in k_1, and otherwise

$$\theta^{\min} = \theta^{\min}_{\mathfrak{C}_{2^m p}} + \frac{1}{p}\tilde{\theta}_0 N_H,$$

where $\tilde{\theta}_0$ is the lift of $\theta_{K_0/k_0,S^{\min}}$ to $\mathbb{C}[H']$. In either case, $\theta^{\min}_{\mathfrak{C}_{2^m p}}$ satisfies

$$\begin{aligned}
N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(\psi\left(\theta^{\min}_{\mathfrak{C}_{2^m p}}\right)\right) &= N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(L_{K_1/k_0,S^{\min}}\left(0,\psi^{-1}\right)\right)\\
&= 2^{(p-1)|S^{\mathrm{spl}}|}\frac{W_0}{W_1}\frac{|\mathrm{Coker}_1|}{|\mathrm{Coker}_0|},
\end{aligned} \tag{4.18}$$

for any generator ψ of $\widehat{G}$.

We may now find similar formulae for the L-function evaluators corresponding to more general sets S of places of k_0 containing $S^{\min}$. Consider the effect of the adjunction of a single prime ideal $\mathfrak{p}$ to $S^{\min}$. We will use property 1 of L-function evaluators from Section 3.1, which says

$$\theta_{K_1/k_0,S\cup\{\,\mathfrak{p}\,\}} = \left(1-\sigma_p^{-1}\right)\theta_{K_1/k_0,S}.$$

First, assume that

$$\sigma_{\mathfrak{p}}^{-1} = \sigma^a$$

for some a such that $1 \le a \le p-1$, so that $\mathfrak{p}$ splits completely in K_0/k_0 and is inert in k_1/k_0. Multiplying $\theta^{\min}_{\mathfrak{C}_{2^m p}}$ inside the expression on the left side of (4.18) by $(1-\sigma^a)$ has the effect of multiplying the expression on the right side by $p^{2^{m-1}}$.

Next, assume that

$$\sigma_{\mathfrak{p}}^{-1} = \sigma'^b\sigma^a$$

for some integers a and b such that $(a,p)=1$ and $(b,2)=1$. Multiplying $\theta^{\min}_{\mathfrak{C}_{2^m p}}$ inside the expression on the left side of (4.18) by $\left(1-\sigma'^b\sigma^a\right)$ when $\psi = \chi^{2^m+p}$ does not change the value of that expression since

$$\chi^{2^m+p}\left(1-\sigma'^b\sigma^a\right) = 1-\zeta_{2^m}\zeta_p$$

is a cyclotomic unit with absolute norm 1 ([60, Proposition 2.8]). Thus, the same is true when ψ is any character that generates $\widehat{G}$.

Finally, assume that

$$\sigma_{\mathfrak{p}}^{-1} = \sigma'^b$$

for some b such that the exact power of 2 dividing b is 2^r, with $0 \le r < m$. Multiplying the $\theta_{\mathfrak{C}_{2^m p}}$ inside the expression on the left side of (4.18) by $\left(1-\sigma_{\mathfrak{p}}^{-1}\right)$ has the effect of multiplying the expression on the right side by $2^{(p-1)2^r}$.

The following proposition follows from the previous analysis by an inductive argument.

Proposition 4.5.1. *Let S be an arbitrary set of places of k_0 containing S^{min} and such that no prime in S splits completely in K_1/k_0. If any prime in S splits completely in K_0/k_0, then*

$$\theta_{K_1/k_0,S} = \theta_{K_1/k_0,S,\mathfrak{C}_{2^m p}}, \tag{4.19}$$

and otherwise,

$$\theta_{K_1/k_0,S} = \theta_{K_1/k_0,S,\mathfrak{C}_{2^m p}} + \frac{1}{p}\tilde{\theta}_{K_0/k_0,S} N_H, \tag{4.20}$$

where $\tilde{\theta}_{K_0/k_0,S}$ is a lift of $\theta_{K_0/k_0,S}$ to $\mathbb{C}[H']$. In either of these cases, if ψ is in $\mathfrak{C}_{2^m p}$, then $\theta_{K_1/k_0,S,\mathfrak{C}_{2^m p}}$ satisfies

$$N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(\psi\left(\theta_{K_1/k_0,S,\mathfrak{C}_{2^m p}}\right)\right) = 2^{(p-1)|S_1|} p^{2^{m-1}|S_2|} \frac{W_0}{W_1} \frac{|Coker_1|}{|Coker_0|}, \tag{4.21}$$

where S_1 is the set of places in K_0 lying above places in S that split in k_1/k_0, and S_2 is the set of places in S that split completely in K_0/k_0 and are inert in k_1/k_0.

We remark once again that the above norm is positive.

The following lemma is crucial.

Lemma 4.5.2. *The norm map*

$$N\colon Coker_1 \to Coker_0$$

is surjective.

Proof. Observe that if $\mathfrak{a}$ is an ideal of K_1, then $\mathfrak{a}^\tau\,\mathfrak{a}$ is the lift of an ideal of K_1^+, so τ acts on Coker_1 by inversion. Similarly, τ acts on Coker_0 by inversion.

Let H_1 and H_0 be the extension fields of K_1 and K_0 corresponding to Coker_1 and Coker_0 through class field theory, and let H_{K_1} and H_{K_0} be the Hilbert class fields of K_1 and K_0. Proposition 2.7.5 shows that the extension H_{K_1}/k_1 is Galois, and that the Artin map $\mathrm{Cl}_{K_1} \to \mathrm{Gal}(H_{K_1}/K_1)$ is an H'-equivariant isomorphism. Similarly, the Artin map for H_{K_0}/K_0 is $\mathrm{Gal}(K_0/k_0)$-equivariant. Since $[K_1 : K_0] = p$, if $K_1 \cap H_0 \neq K_0$, then $K_1 \subset H_0$. But this is impossible, since $|H|$ is odd and the complex conjugation τ acts trivially on $H = \mathrm{Gal}(K_1/K_0)$ and acts by inversion on $\mathrm{Gal}(H_0/K_0)$. Thus, $K_1 \cap H_0 = K_0$.

We observe that K_1H_0 is contained in H_{K_1}. First, $\mathrm{Gal}\,(K_1H_0/K_1)$ injects into $\mathrm{Gal}\,(H_0/K_0)$ by restriction, so K_1H_0 is Abelian over K_0. Second, if $\mathfrak{p}$ is a prime ideal in K_0, then since $\mathfrak{p}$ is unramified in H_0/K_0, the inertia group $I_{\mathfrak{p}}$ of $\mathfrak{p}$ in $\mathrm{Gal}\,(K_1H_0/K_0)$ is contained in $\mathrm{Gal}\,(K_1H_0/H_0)$. Let $\tilde{\mathfrak{P}}$ be a prime ideal of K_1H_0 lying above $\mathfrak{p}$, and let $\mathfrak{P}$ be the prime ideal of K_1 lying below $\tilde{\mathfrak{P}}$. Let σ be an element of the inertia group of $\tilde{\mathfrak{P}}$ over K_1. By definition, σ fixes $\tilde{\mathfrak{P}}$, and

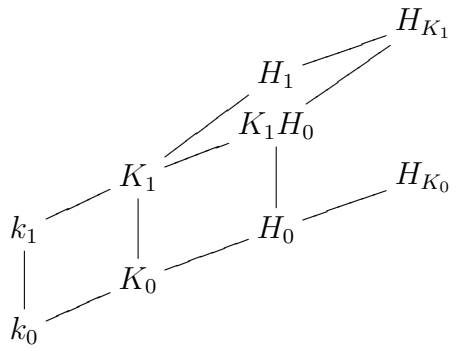
$$\sigma(\alpha) \equiv \alpha \pmod{\tilde{\mathfrak{P}}}$$

for all elements α in the ring of integers in K_1H_0. But by definition, this implies that σ is in the inertia group $I_{\mathfrak{p}}$ of $\tilde{\mathfrak{P}}$ over K_0. Hence,

$$\sigma \in \mathrm{Gal}\,(K_1H_0/K_1) \cap \mathrm{Gal}\,(K_1H_0/H_0) = 1.$$

The inertia group of $\tilde{\mathfrak{P}}$ over K_1 is therefore trivial. Thus, no prime ideal ramifies in K_1H_0/K_1. Furthermore, no Archimedean places ramify in K_1H_0/K_1, since K_1 is totally complex. Since H_{K_1} is the maximal unramified Abelian extension of K_1, it follows that K_1H_0 is contained in H_{K_1}.

We have the following diagram of fields:



Let $\mathfrak{a}$ be an ideal of K_1 whose class in Coker_1 is trivial. We may write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}\,(\gamma)$, where $\mathfrak{b}$ is an ideal of K_1 supported at prime ideals dividing those in S^{ns}, $\mathfrak{c}$ is the lift of an ideal from K_1^+, and γ is in $K_1^\times$. If N denotes the norm map on ideals from K_1 to K_0, then

$$N\mathfrak{a} = N\mathfrak{b}N\mathfrak{c}\,(N\gamma)\,.$$

Setting $\mathfrak{c} = \mathfrak{c}'\mathcal{O}_{K_1}$ where $\mathfrak{c}'$ is an ideal in K_1^+ and $\mathcal{O}_{K_1}$ is the ring of integers in K_1, we have

$$N\mathfrak{c} = N_{K_1^+/K_0^+}\,(\mathfrak{c}')\,\mathcal{O}_{K_0},$$

which is the lift of an ideal from K_0^+ to K_0. Also, $N\mathfrak{b}$ is supported at primes dividing those in S^{ns}. Therefore, the class of $N\mathfrak{a}$ in Coker_0 is trivial. It follows from Lemma 2.6.1 that

$$(\mathfrak{a}, H_{K_1}/K_1)\Big|_{H_0} = (N\mathfrak{a}, H_0/K_0) = (N\mathfrak{a}, H_{K_0}/K_0)\Big|_{H_0} = \text{id},$$

since H_0 is the subfield of H_{K_0} fixed by the automorphisms $(\mathfrak{c}, H_{K_0}/K_0)$ for ideals $\mathfrak{c}$ in K_0 representing the trivial class in Coker_0. Therefore, K_1H_0 is contained in the field fixed by the automorphisms $(\mathfrak{c}, H_{K_1}/K_1)$ for ideals $\mathfrak{c}$ representing the trivial class in Coker_1. By definition, this is the field H_1, so $K_1H_0 \subset H_1$. There is thus a restriction map

$$\text{Res}\colon \text{Gal}\left(H_1/K_1\right) \to \text{Gal}\left(H_0/K_0\right),$$

which is surjective since $K_1 \cap H_0 = K_0$. It follows that the corresponding norm map $N\colon \text{Coker}_1 \to \text{Coker}_0$ is surjective. □

Therefore, we may rewrite (4.21) as

$$N_{\mathbb{Q}\left(\zeta_{2^m p}\right)/\mathbb{Q}}\left(\psi\left(\theta_{K_1/k_0,S,\mathfrak{E}_{2^m p}}\right)\right) = \frac{1}{q} 2^{(p-1)|S_1|} p^{2^{m-1}|S_2|} \,|\,\text{Ker}\,|\,. \tag{4.22}$$

where q is defined by $W_1 = qW_0$ and "Ker" designates the kernel of the map $N\colon \text{Coker}_1 \to \text{Coker}_0$.

Remark. We make a couple of remarks about roots of unity. First, $p \mid W_0$ if and only if $p \mid W_1$. Second, if $p \mid W_0$, let p^a be the exact power of p dividing W_0 and p^b be the exact power of p dividing W_1. Then $\mathbb{Q}\left(\zeta_{p^b}\right) \cap K_0 = \mathbb{Q}\left(\zeta_{p^a}\right)$. Also, $K_0\left(\zeta_{p^b}\right) = K_0$ if $a = b$, and $K_0\left(\zeta_{p^b}\right) = K_1$ if $a < b$, since there are no intermediate fields between K_0 and K_1. Therefore, if $a < b$, then $p^{b-a} = \left[\mathbb{Q}\left(\zeta_{p^b}\right) : \mathbb{Q}\left(\zeta_{p^a}\right)\right] = [K_1 : K_0] = p$. Consequently, the exact power of p dividing q is either 0 or 1.

We have arrived at our desired expression for $\theta_{K_1/k_0,S}$, which will be restated here as a theorem.

Theorem 4.5.3. *Let notation be as above. Let S be any set of places of k_0 containing the Archimedean places and the primes that ramify in K_1/k_0. Write $\theta_{K_1/k_0,S,\mathfrak{E}_{2^m}} = \theta_{\mathfrak{E}_{2^m}}$ and $\theta_{K_1/k_0,S,\mathfrak{E}_{2^m p}} = \theta_{\mathfrak{E}_{2^m p}}$. Then*

$$\theta_{K_1/k_0,S} = \theta_{\mathfrak{E}_{2^m p}} + \theta_{\mathfrak{E}_{2^m}}.$$

If ψ is any character in $\mathfrak{C}_{2^m p}$, then $\overline{\theta}_{\mathfrak{C}_{2^m p}}$ satisfies

$$N_{\mathbb{Q}(\zeta_{2^m p})/\mathbb{Q}}\left(\psi\left(\overline{\theta}_{\mathfrak{C}_{2^m p}}\right)\right) = \frac{1}{q} 2^{(p-1)|S_1|} p^{2^{m-1}(|S_2|-1)} \left|\, Ker \,\right|, \tag{4.23}$$

where Ker and q were defined immediately following equation (4.22)*. Furthermore, $\theta_{\mathfrak{C}_{2^m}}$ is given by*

$$\theta_{\mathfrak{C}_{2^m}} = \frac{N_H}{p} \tilde{\theta}_0,$$

where $\tilde{\theta}_0$ is a lift of $\theta_{K_0/k_0,S}$ to $\mathbb{C}[G]$. In particular, $\theta_{\mathfrak{C}_{2^m}}$ is 0 if any prime of S splits completely in K_0/k_0.

4.6 Norms of L-values for degree $2^m p^n$ extensions

Let p be an odd prime and let m and n be positive integers. In this section, we will use the expressions in Theorem 4.5.3 to derive similar ones for cyclic extensions of degree $2^m p^n$. Let K_n/k_0 be a cyclic extension of number fields of degree $2^m p^n$. We assume that k_0 is totally real and that K_n is totally complex. For $0 \leq r \leq n$, let k_r and K_r be the unique extension fields of k_0 contained in K_n with $[k_r : k_0] = p^r$ and $[K_r : k_0] = 2^m p^r$. The fields k_r are all totally real and the fields K_r are all CM fields. Let K_r^+ denote the maximal totally real subfield of K_r. Let S_0 be a set of places of k_0 containing the set $S_0^{\min}$ consisting of the Archimedean places and the prime ideals of k_0 that ramify in K_n. For $0 \leq r \leq n$, let S_r denote the set of places in k_r lying above the places in S_0. We denote the number of roots of unity in K_r by W_r.

Set $G = \mathrm{Gal}\,(K_n/k_0)$, $G' = \mathrm{Gal}\,(K_n/k_1)$, $H = \mathrm{Gal}\,(K_n/K_0)$, and finally set $H' = \mathrm{Gal}\,(K_n/k_n)$. Fix a generator σ of H, a generator σ' of H', and let $\tau = {\sigma'}^{2^{m-1}}$ denote complex conjugation. Furthermore, let

$$N_p = \sum_{i=0}^{p-1} \sigma^{ip^{n-1}}$$

be the norm element in $\mathbb{C}[H]$ corresponding to the extension K_n over K_{n-1}. Let χ be a generator of $\widehat{G}$. For $1 \leq r \leq n$, let ζ_{p^r} be the primitive p^rth root of unity such that

$$\chi^{2^m}\left(\sigma^{p^{n-r}}\right) = \zeta_{p^r}.$$

Let ζ_{2^m} be the primitive 2^mth root of unity such that

$$\chi^{p^n}(\sigma') = \zeta_{2^m}.$$

If $k_0 = \mathbb{Q}$, then at least one prime ideal of k_0 ramifies in K_n. If $k_0 \neq \mathbb{Q}$, then S_0 contains at least two Archimedean places. It follows that $|S_0| \geq 2$. Thus, for each even integer $2t$,

$$L_{K_n/k_0,S_0}\left(0, \chi^{2t}\right) = 0,$$

since χ^{2t} is an even character (see [58, Chapter I, Proposition 3.4]). The odd characters fall into $n+1$ equivalence classes under the equivalence relation from Section 3.3: for $0 \leq r \leq n$, $\mathfrak{C}_{2^m p^r}$ comprises the characters of order $2^m p^r$. To simplify notation, we write θ instead of $\theta_{K_n/k_0,S_0}$. Similarly, we write $\theta_{\mathfrak{C}_{2^m p^r}}$ instead of $\theta_{K_n/k_0,S_0,\mathfrak{C}_{2^m p^r}}$.

We can decompose θ as

$$\theta = \sum_{r=0}^{n} \theta_{\mathfrak{C}_{2^m p^r}}. \tag{4.24}$$

Consider $\theta_{\mathfrak{C}_{2^m p^n}}$ as an element of $\mathbb{Q}[H'][H]$ and write

$$\theta_{\mathfrak{C}_{2^m p^n}} = \sum_{i=0}^{p^n-1} a_i \sigma^i,$$

where each a_i is an element of $\mathbb{Q}[H']$. Property 2 of components of L-function evaluators from Section 3.3 shows that we can write

$$\theta = \sum_{i=0}^{p^n-1} a_i \sigma^i + cN_p, \tag{4.25}$$

where c is an element of $\mathbb{Q}[G]$.

Since the case $n = 1$ was examined in the last section, we will now assume that $n \geq 2$. Let t_a denote the twist by χ^a. By property 3 of equivariant L-functions in Section 3.1,

$$\theta_{K_n/k_1,S_1} = \prod_{v=0}^{p-1} t_{2^m p^{n-1} v} \left(\sum_{i=0}^{p^n-1} a_i \sigma^i + cN_p \right). \tag{4.26}$$

Applying $\chi^{2^m+p^n}$ to the first term formed when this product is expanded yields

$$\begin{aligned}\chi^{2^m+p^n}\left(\prod_{v=0}^{p-1} t_{2^m p^{n-1} v}\left(\sum_{i=0}^{p-1} a_i\sigma^i\right)\right) &= \chi^{2^m+p^n}\left(\prod_{v=0}^{p-1}\left(\sum_{i=0}^{p^n-1} a_i\zeta_p^{iv}\sigma^i\right)\right)\\ &= \prod_{v=0}^{p-1}\left(\sum_{i=0}^{p^n-1}\chi^{p^n}(a_i)\,\zeta_p^{iv}\zeta_{p^n}^{i}\right)\\ &= N_{\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}\left(\zeta_{2^m p^{n-1}}\right)}\left(\sum_{i=0}^{p^n-1}\chi^{p^n}(a_i)\,\zeta_{p^n}^{i}\right)\\ &= N_{\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}\left(\zeta_{2^m p^{n-1}}\right)}\left(\chi^{2^m+p^n}\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)\right).\end{aligned}$$

(We have used the assumption that $n \geq 2$). For each $v = 0, \ldots, p-1$, the assumption that $n \geq 2$ also implies that the twist $t_{2^m p^{n-1} v}$ fixes N_p. Therefore, the other terms that appear when the product (4.26) is expanded are all multiples of N_p.

We have found that when $n \geq 2$, there is a decomposition

$$\theta_{K_n/k_1,S_1} = \alpha + c' N_p \tag{4.27}$$

where α is in $\mathbb{C}[G]$ and satisfies

$$\chi^{2^m+p^n}(\alpha) = N_{\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}\left(\zeta_{2^m p^{n-1}}\right)}\left(\chi^{2^m+p^n}\left(\theta_{\mathfrak{C}^{2^m p^n}}\right)\right).$$

For $0 \leq r \leq n-1$, let $\mathfrak{c}_{2^m p^r}$ denote the equivalence class in $\widehat{G'}$ containing the characters of order $2^m p^r$. The decomposition of $\theta_{K_n/k_1,S_1}$ into components is

$$\theta_{K_n/k_1,S_1} = \sum_{r=0}^{n-1}\theta_{\mathfrak{c}_{2^m p^r}}. \tag{4.28}$$

By property 2 of components of L-function evaluators, the partial sum

$$\sum_{r=0}^{n-2}\theta_{\mathfrak{c}_{2^m p^r}}$$

is a multiple of N_p. Property 3 of components of L-function evaluators shows that $N_p\theta_{\mathfrak{c}_{2^m p^{n-1}}} = 0$. It also shows that $N_p\sum_{i=0}^{p-1} a_i\sigma^i = 0$. Therefore, since $t_{2^m p^{n-1} v}$ fixes N_p,

$$N_p\,\alpha = N_p\prod_{v=0}^{p-1} t_{2^m p^{n-1} v}\left(\sum_{i=0}^{p-1} a_i\sigma^i\right) = 0.$$

Multiplying the expressions (4.27) and (4.28) for $\theta_{K_n/k_1,S}$ by N_p/p shows that

$$c' N_p = \sum_{r=0}^{n-2} \theta_{\mathfrak{c}_{2^m p^r}}.$$

Comparing the two expressions for $\theta_{K_n/k_1,S_1}$ then yields

$$\alpha = \theta_{\mathfrak{c}_{2^m p^{n-1}}}.$$

Finally, applying $\chi^{2^m+p^n}$ shows that

$$\chi^{2^m+p^n}\left(\theta_{\mathfrak{c}_{2^m p^{n-1}}}\right) = N_{\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}\left(\zeta_{2^m p^{n-1}}\right)}\left(\chi^{2^m+p^n}\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)\right). \tag{4.29}$$

Each extension K_n/k_r with $0 \leq r \leq n-2$ is a degree $2^m p^{n-r}$ cyclic extension with $n - r \geq 2$. Therefore, the above analysis can be conducted on each such extension. For $r = 1, \ldots, n$, let $\mathcal{C}_{2^m p^r}$ be the equivalence class of characters on $\mathrm{Gal}\left(K_n/k_{n-r}\right)$ of order $2^m p^r$. An inductive argument shows that the elements $\chi^{2^m+p^n}\left(\theta_{K_n/k_r,S_r,\mathcal{C}_{2^m p^r}}\right)$ in $\mathbb{Q}\left(\zeta_{2^m p^r}\right)$ for $1 \leq r \leq n$ form a norm-coherent sequence. In particular,

$$\chi^{2^m+p^n}\left(\theta_{K_n/k_1,S_{n-1},\mathcal{C}_{2^m p}}\right) = \mathrm{N}_{\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}\left(\zeta_{2^m p}\right)}\left(\chi^{2^m+p^n}\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)\right).$$

Set

$$q = \frac{W_n}{W_{n-1}}.$$

Since k_n/k_0 is cyclic, the set of places in K_{n-1} lying above places in S_{n-1} that split in k_n/k_{n-1} is also the set of places in K_{n-1} lying above places in S_0 that split completely in k_n/k_0. Let $\tilde{S}_1$ be the set of places in K_0 lying above places in S_0 that split completely in k_n/k_0. The cardinality of the set of places in K_{n-1} lying above places in S_{n-1} that split in k_n/k_{n-1} is $p^{n-1}\left|\tilde{S}_1\right|$. Let $\tilde{S}_2$ be the set of places in K_n lying above places in S_0 that split completely in K_0/k_0 and are unramified in k_n/k_0. We abuse notation by letting S_r^{ns} denote both the set of places in K_r^+ and the set of places in K_r lying above the places in $S_0^{\min}$ that do not split completely in K_0/k_0. Let Coker_{n-1} be the cokernel of the map

$$\mathrm{Cl}_{K_{n-1}^+,S_{n-1}^{\mathrm{ns}}} \to \mathrm{Cl}_{K_{n-1},S_{n-1}^{\mathrm{ns}}},$$

and let Coker_n be the cokernel of the map

$$\mathrm{Cl}_{K_n^+,S_n^{\mathrm{ns}}} \to \mathrm{Cl}_{K_n,S_n^{\mathrm{ns}}}.$$

Finally, let Ker denote the kernel of the norm map $\mathrm{N}\colon \mathrm{Coker}_n \to \mathrm{Coker}_{n-1}$. Since the extension K_n/k_{n-1} is a degree $2p$ cyclic extension, Theorem 4.5.3 shows that

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}}\left(\chi^{2^m+p^n}\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)\right) &= \mathrm{N}_{\mathbb{Q}\left(\zeta_{2^m p}\right)/\mathbb{Q}}\left(\chi^{2^m+p^n}\left(\theta_{K_n/k_{n-1},S_{n-1},\mathcal{C}_{2^m p}}\right)\right)\\ &= \frac{1}{q}2^{p^{n-1}(p-1)\left|\tilde{S}_1\right|}p^{2^{m-1}\left|\tilde{S}_2\right|}\left|\mathrm{Ker}\right|.\end{aligned}$$

The characters that generate $\widehat{G}$ are precisely the characters in $\mathfrak{C}_{2^m p^n}$. By Proposition 3.2.1 and Theorem 3.2.3, as ψ runs through the characters that generate $\widehat{G}$, the values

$$L_{K_n/k_0,S_0}(0,\psi) = \psi^{-1}\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)$$

run through a set of algebraic conjugates in $\mathbb{Q}\left(\zeta_{2^m p^n}\right)$ (possibly more than once). We have thus proved the following theorem.

Theorem 4.6.1. *Let S_0 be an arbitrary set of places of k_0 containing S_0^{min} and such that no prime in S_0 splits completely in K_n/k_0. The decomposition of θ into components is*

$$\theta = \sum_{r=0}^{n}\theta_{\mathfrak{C}_{2^m p^r}},$$

where the class $\mathfrak{C}_{2^m p^r}$ consists of the characters in $\widehat{G}$ of order $2^m p^r$. If ψ is in $\mathfrak{C}_{2^m p^n}$, then

$$\begin{aligned}N_{\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}}\left(L_{K_n/k_0,S_0}(0,\psi)\right) &= N_{\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}}\left(\psi^{-1}\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)\right)\\ &= \frac{1}{q}2^{p^{n-1}(p-1)\left|\tilde{S}_1\right|}p^{2^{m-1}\left|\tilde{S}_2\right|}\left|Ker\right|. \qquad (4.30)\end{aligned}$$

where q, $\tilde{S}_1$, $\tilde{S}_2$, and Ker were defined in the preceding paragraph.

Remark. The norms of the values at $s = 0$ of the other L-functions for K_n/k_0 can be found using property 2 of components of L-function evaluators, Proposition 4.3.1, and equation (4.30).

Example. Let p and $l = 2^m p^n + 1$ be odd prime numbers. We will examine the case where $k_0 = \mathbb{Q}$ and $K_n = \mathbb{Q}(\zeta_l)$. Then $q = l$ and the set $S_0^{\min}$ of places of $\mathbb{Q}$ consists of the Archimedean place and the prime ideal (l). For each character χ in $\widehat{G}$, let $B_{1,\chi}$ be the generalized Bernoulli number defined by

$$B_{1,\chi} = \frac{1}{l} \sum_{a=1}^{l-1} a\chi(a).$$

It is known that ([60, Theorem 4.2])

$$L_{K_n/k_0,S_0^{\min}}(0,\chi) = -B_{1,\chi},$$

Assuming that as ψ runs through the characters in $\mathfrak{C}_{2^m p^n}$, the algebraic conjugates $B_{1,\psi}$ are distinct, it follows that

$$N_{\mathbb{Q}(\zeta_{2^m p^n})/\mathbb{Q}}\left(L_{K_n/k_0,S_0^{\min}}(0,\chi)\right) = \prod_{\psi} -B_{1,\psi},$$

where the product is over the characters of order $2^m p^n$. The set $\tilde{S}_1$ consists of 2^{m-1} Archimedean places, and the set $\tilde{S}_2$ is empty. Thus,

$$p^{n-1}(p-1)\left|\tilde{S}_1\right| = 2^{m-1}p^{n-1}(p-1)$$

and

$$2^{m-1}\left|\tilde{S}_2\right| = 0.$$

Putting all of this together with equation (4.30), we find a formula analogous to the well-known expression for the minus class number of K_n as a product of generalized Bernoulli numbers ([60, Theorem 4.17]):

$$|\mathrm{Ker}| = l \prod_{\psi} -\frac{1}{2} B_{1,\psi}.$$

Again, the product is over the characters of order $2^m p^n$. Also, $|\mathrm{Ker}|$ is the quotient of the relative class number of K_n by the relative class number of K_{n-1}. This generalizes a formula used by Peter Stevenhagen in [57] to study the parity of certain relative class numbers.

We will now derive another version of formula (4.30). The ideal class group of K_n is a $\mathbb{Z}[G]$-module. The subgroup of the ideal group of K_n supported above S_n^{ns} is stable under the action of G. The group of lifts of ideals from K_n^+ to K_n is also stable under G. Therefore, the quotient group Coker_n is a $\mathbb{Z}[G]$-module. Similarly, Coker_{n-1} is a $\mathbb{Z}[G]$-module. We will show that Ker is a $\mathbb{Z}[G]$-submodule of Coker_n.

Remark. We must be careful not to confuse Ker with the $\mathbb{Z}[G]$-submodule of Coker_n annihilated by N_p. Ker, the kernel of the norm *map* $N\colon \mathrm{Coker}_n \to \mathrm{Coker}_{n-1}$, is necessarily only contained in the $\mathbb{Z}[G]$-submodule of Coker_n annihilated by N_p. If the canonical map

$$\mathrm{Coker}_{n-1} \to \mathrm{Coker}_n$$

is not injective, then this containment might be strict.

An ideal $\mathfrak{a}$ is a representative of a class in Ker if and only if the ideal $\mathrm{N}_p \cdot \mathfrak{a}$ is the lift of an ideal of K_{n-1} whose class in Coker_{n-1} is trivial. If $\mathfrak{a}$ is such an ideal and g is in G, then $\mathrm{N}_p\, g \cdot \mathfrak{a} = g\, \mathrm{N}_p \cdot \mathfrak{a}$. Since Coker_{n-1} is a $\mathbb{Z}[G]$-module, $\mathrm{N}_p\, g \cdot \mathfrak{a}$ is also the lift of an ideal in K_{n-1} whose class in Coker_{n-1} is trivial. It follows that Ker is a $\mathbb{Z}[G]$-submodule of Coker_n.

As Coker_n is annihilated by $1+\tau$, so is Ker. Since Ker is also annihilated by the action of N_p, Lemma 2.3.4 shows that Ker has the structure of a module over the Dedekind domain

$$\mathcal{O} = \mathbb{Z}\left[\zeta_{2^m p^n}\right].$$

Set $\tilde{\mu} = \mu_n/\mu_{n-1}$. Since $\tilde{\mu}$ is annihilated by $1+\tau$ and by N_p, it is also an $\mathcal{O}$-module. By property 6 of Fitting ideals and the fact that $\tilde{\mu}$ is a cyclic $\mathcal{O}$-module, we may rewrite equation (4.30) as

$$\mathfrak{N}\left(\mathrm{Fit}_{\mathcal{O}}\left(\tilde{\mu}\right)\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)\right) = \mathfrak{N}\left(\left(1-\zeta_{2^m}\right)^{\left|\tilde{S}_1\right|}\left(1-\zeta_{p^n}\right)^{\left|\tilde{S}_2\right|}\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right). \tag{4.31}$$

It is now natural to pose a question similar to that of Section 4.3.

Question. *If ψ is a generator of $\widehat{G}$ and $\tilde{\mu}$ and Ker are endowed with the $\mathcal{O}$-module structures induced by ψ, then is it true that*

$$Fit_{\mathcal{O}}\left(\tilde{\mu}\right)\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right) = \left(1-\zeta_{2^m}\right)^{\left|\tilde{S}_1\right|}\left(1-\zeta_{p^n}\right)^{\left|\tilde{S}_2\right|} Fit_{\mathcal{O}}\left(Ker\right)? \tag{4.32}$$

In what follows, we will refer to this question for an extension K_n/k_0 and a set S_0 as $\mathrm{Q}_{2^m p^n}(K_n/k_0, S_0)$. If $\mathrm{Q}_{2^m p^n}(K_n/k_0, S_0)$ has an affirmative answer for the minimal set $S_0 = S_0^{\min}$, then it also does if S_0 is any set containing $S_0^{\min}$. In this case, we will say that $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer without mentioning a set S_0. If p is a prime number, then then hypothesized equality of the factors supported above primes dividing p on each side of equation (4.8) are equal will be referred to as the p-primary part of $\mathrm{Q}_{2^m p^n}(K_n/k_0, S_0)$. We note that the relation (4.32), when valid, implies that $\mathrm{Fit}_{\mathcal{O}}(\mathrm{Ker})$ and $\mathrm{Fit}_{\mathcal{O}}(\tilde{\mu})$ are in the same ideal class in $\mathcal{O}$.

Although formula (4.31) does not immediately imply formula (4.32), if p' is a prime number with only one prime ideal divisor in $\mathbb{Q}(\zeta_{2^m p^n})$, then equation (4.31) implies that the p'-primary part of $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer. It does not seem immediately clear that the p'-primary parts are equal for other prime numbers p'. However, if the 2-primary or the p-primary parts are equal when $S_0 = S_0^{\min}$, then they are equal when S_0 is any set of places containing $S_0^{\min}$.

Next, we will give a result concerning $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)$.

Proposition 4.6.2. *Let ψ be in $\mathfrak{C}_{2^m p^n}$ and let $\mathfrak{N}$ denote the absolute norm on ideals of $\mathbb{Z}[\zeta_{2^m p^n}]$. If $(p, W_n) = 1$, then*

$$\mathfrak{N}\left(\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)\right)\right) = q.$$

Otherwise,

$$\mathfrak{N}\left(\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)\right)\right) = p^e q$$

for some exponent e such that $0 \leq e \leq p^{n-1}$.

Proof. The quotient group μ_n/μ_{n-1} is a $\mathbb{Z}[G]$-module of order q. It is annihilated by both N_p and $1 + \tau$. Lemma 2.3.4 shows that it is a module over the Dedekind domain

$$\mathcal{O} = \mathbb{Z}[\zeta_{2^m p^n}].$$

Being a cyclic group, μ_n/μ_{n-1} is also a cyclic $\mathcal{O}$-module. By property 3 and

property 6 of Fitting ideals in Section 2.4, it follows that

$$\begin{aligned} q = \mathfrak{N}\left(\mathrm{Fit}_{\mathcal{O}}(\mu_n/\mu_{n-1})\right) &= \mathfrak{N}\left(\mathrm{Ann}_{\mathcal{O}}(\mu_n/\mu_{n-1})\right) \\ &= \mathfrak{N}\left(\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n/\mu_{n-1})\right)\right). \end{aligned} \tag{4.33}$$

Let $\mathfrak{N}'$ denote the absolute norm on ideals of $\mathbb{Z}[\zeta_{2^m}]$. Equation (4.6) shows that

$$\mathfrak{N}'\left(\psi_{H'}\left(\mathrm{Ann}_{\mathbb{Z}[H']}(\mu_{n-1})\right)\right) = \mathfrak{N}'\left(\mathrm{Fit}_{\mathbb{Z}[\zeta_{2^m}]}(\mu_{n-1})\right) = W_{n-1}.$$

Also, since $1-\sigma^{p^{n-1}}$ annihilates μ_{n-1},

$$\left(1-\zeta_p, \mathrm{Fit}_{\mathbb{Z}[\zeta_{2^m}]}(\mu_{n-1})\right) \subseteq \psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_{n-1})\right).$$

If $p \nmid W_{n-1}$, it follows that

$$\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_{n-1})\right) = \mathcal{O}.$$

(We note that p divides W_{n-1} if and only if p divides W_n.) Let δ be an element of $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_{n-1})$ such that $\psi(\delta)=1$, and let $\beta_1,\ldots,\beta_r$ be a set of elements of $\mathbb{Z}[G]$ such that $\psi(\beta_1),\ldots,\psi(\beta_r)$ generate $\mathrm{Fit}_{\mathcal{O}}(\mu_n/\mu_{n-1})$. Then

$$\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n/\mu_{n-1})\right) = \left(\psi(\delta\beta_1),\ldots,\psi(\delta\beta_r)\right) \subseteq \psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)\right).$$

Since $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n) \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n/\mu_{n-1})$, it follows from equation (4.33) that

$$\mathfrak{N}\left(\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)\right)\right) = q.$$

Otherwise, assume that the exact power of p dividing W_{n-1} is p^t. Also, assume that the ideal factorization of $(1-\zeta_{p^n})$ in $\mathcal{O}$ is

$$(1-\zeta_{p^n}) = \prod_{i=1}^{g} \mathfrak{P}_i.$$

Let $\mathfrak{A}_p$ be the part of $\mathrm{Ann}_{\mathbb{Z}[\zeta_{2^m}]}(\mu_{n-1})$ supported at primes dividing p. By Lemma 2.4.1, there exists an i such that

$$\mathfrak{A}_p\mathcal{O} = \mathfrak{P}_i^{p^{n-1}(p-1)t}.$$

Then for this i,

$$\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_{n-1})\right) \supseteq \left(1-\zeta_p, \mathrm{Ann}_{\mathbb{Z}[\zeta_{2^m}]}(\mu_{n-1})\right) = \mathfrak{P}_i^{p^{n-1}}.$$

Reasoning as in the case where $p \nmid W_{n-1}$, it follows that

$$\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}\left(\mu_n\right)\right) = \psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}\left(\mu_n/\mu_{n-1}\right)\right)\mathfrak{P}^e \tag{4.34}$$

for some exponent e such that $0 \leq e \leq p^{n-1}$. Therefore, since the residual degree of $\mathfrak{P}$ over $\mathbb{Q}$ is 1,

$$\mathfrak{N}\left(\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}\left(\mu_n\right)\right)\right) = p^e q. \qquad \square$$

Next, we investigate the denominators of the coefficients of $\theta_{\mathfrak{C}_{2^m p^n}}$. We again write $\theta_{\mathfrak{C}_{2^m p^n}} = \sum_{i=0}^{p^n-1} a_i \sigma^i$ with the coefficients a_i in $\mathbb{Q}[H']$. Since N_p annihilates $\theta_{\mathfrak{C}_{2^m p^n}}$, it follows that for each j such that $0 \leq j \leq p^{n-1}-1$, $\sum_{i=0}^{p-1} a_{ip^{n-1}+j} = 0$. It will turn out to be in our interest to factor $(1-\sigma^{p^{n-1}})$ out of $\theta_{\mathfrak{C}_{2^m p^n}}$ by writing $\theta_{\mathfrak{C}_{2^m p^n}} = \left(1-\sigma^{p^{n-1}}\right)\overline{\theta}_{\mathfrak{C}_{2^m p^n}}$ with

$$\overline{\theta}_{\mathfrak{C}_{2^m p^n}} = \sum_{i=0}^{p-2}\sum_{j=0}^{p^{n-1}-1} b_{ip^{n-1}+j}\,\sigma^{ip^{n-1}+j} \tag{4.35}$$

and

$$b_{ip^{n-1}+j} = \sum_{k=0}^{i} a_{kp^{n-1}+j}. \tag{4.36}$$

We now give a bound on the denominators of the coefficients of $\overline{\theta}_{\mathfrak{C}_{2^m p^n}}$, stronger than that given by Proposition (3.3.1).

Proposition 4.6.3. *With notation as above,*

$$\overline{\theta}_{\mathfrak{C}_{2^m p^n}} \in \frac{1}{pq}\mathbb{Z}\left[G\right].$$

If the p-primary part of $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ *has an affirmative answer and either* $\left|\tilde{S}_2\right| \geq p^{n-1}$ *or* $p \mid q$*, then*

$$\overline{\theta}_{\mathfrak{C}_{2^m p^n}} \in \frac{1}{q}\mathbb{Z}\left[G\right].$$

Proof. Let μ_n and μ_{n-1} be the groups of roots of unity in K_n and K_{n-1} respectively. The definition of q shows that

$$q\left(1-\sigma^{p^{n-1}}\right) \in \mathrm{Ann}_{\mathbb{Z}[G]}\left(\mu_n\right).$$

By Theorem 3.2.4,

$$q(1-\sigma^{p^{n-1}})\theta \in \mathbb{Z}[G].$$

Equation (4.25) shows that

$$q\left(1-\sigma^{p^{n-1}}\right)\theta = q\left(1-\sigma^{p^{n-1}}\right)\theta_{\mathfrak{C}_{2^m p^n}}.$$

It follows that

$$q\left(\prod_{i=1}^{p-1}\left(1-\sigma^{ip^{n-1}}\right)\right)\theta_{\mathfrak{C}_{2^m p^n}} \in \mathbb{Z}\left[G\right].$$

Under the second isomorphism in Lemma 2.3.4 (using an element ψ in $\mathfrak{C}_{2^m p^n}$ for the character in that lemma), $\prod_{i=1}^{p-1}(1-\sigma^i)$ has the same image as p. Properties 3 and 4 of components of L-function evaluators in Section 3.3 show that $\theta_{\mathfrak{C}_{2^m p^n}}$ is annihilated both by $1+\tau$ and by N_p. It follows that

$$pq\theta_{\mathfrak{C}_{2^m p^n}} = q\left(\prod_{i=1}^{p-1}\left(1-\sigma^{ip^{n-1}}\right)\right)\theta_{\mathfrak{C}_{2^m p^n}} \in \mathbb{Z}\left[G\right].$$

Therefore,

$$\theta_{\mathfrak{C}_{2^m p^n}} \in \frac{1}{pq}\mathbb{Z}\left[G\right].$$

(The example following Proposition 3.3.1 shows that pq can be the exact denominator when the coefficients are written in lowest terms.) Finally, expressions (4.35) and (4.36) show that

$$\overline{\theta}_{\mathfrak{C}_{2^m p^n}} \in \frac{1}{pq}\mathbb{Z}\left[G\right].$$

Now assume that the p-primary part of $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ has an affirmative answer. In particular, the factors supported above prime ideals dividing p on both sides of the equation

$$\mathrm{Fit}_{\mathcal{O}}\left(\tilde{\mu}\right)\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right) = \left(1-\zeta_{2^m}\right)^{\left|\tilde{S}_1\right|}\left(1-\zeta_{p^n}\right)^{\left|\tilde{S}_2\right|}\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)$$

are equal, where ψ generates $\widehat{G}$. We will use this formula to prove the second part of the proposition.

The first part of this proposition shows that $q\psi\left(\theta^{\min}_{\mathfrak{C}_{2^m p^n}}\right)$ is integral up to prime ideals in $\mathcal{O}$ dividing p. The p-primary part of $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ and equation (4.33) then show that for each ψ in $\mathfrak{C}_{2^m p^n}$,

$$q\psi\left(\theta^{\min}_{\mathfrak{C}_{2^m p^n}}\right) \in \mathbb{Z}\left[\zeta_{2^m p^n}\right].$$

Hence,

$$q\left(1-\zeta_p\right)\psi\left(\overline{\theta}^{\min}_{\mathfrak{C}_{2^m p^n}}\right)\in\mathbb{Z}\left[\zeta_{2^m p^n}\right].$$

The argument in the paragraph preceding Proposition 4.5.1 shows that adjoining a set of prime ideals to S_0 with a corresponding addition of k primes to $\tilde{S}_2$ multiplies the integral ideal $\psi\left(\left(pq\overline{\theta}_{\mathfrak{C}_{2^m p^n}}\right)\right)$ by a factor of $\left(1-\zeta_{p^n}\right)^k$. If we now let S_0 be a set formed by adjoining primes to $S_0^{\min}$ that split completely in K_0/k_0, and if these additional primes are enough to make $\left|\tilde{S}_2\right|\geq p^{n-1}$, then we have

$$q\psi\left(\overline{\theta}_{\mathfrak{C}_{2^m p^n}}\right)=q\left(1-\zeta_{p^n}\right)^{\left|\tilde{S}_2\right|}\psi\left(\overline{\theta}^{\min}_{\mathfrak{C}_{2^m p^n}}\right)\in\mathbb{Z}\left[\zeta_{2^m p^n}\right].$$

It follows that $q\psi\left(\overline{\theta}_{\mathfrak{C}_{2^m p^n}}\right)$ is integral for any set S_0 for which $\left|\tilde{S}_2\right|\geq p^{n-1}$.

Next, if p divides q, then p is the exact power of p dividing q (see the remark preceding Theorem 4.5.3). It follows from the p-primary part of $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ that

$$\left(1-\zeta_{p^n}\right)\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)$$

is $\mathfrak{P}$-integral for all primes $\mathfrak{P}$ of $\mathbb{Q}\left(\zeta_{2^m p^n}\right)$ dividing p. Therefore, since

$$p^{n-1}(p-1)-1\geq p^{n-1},$$

the first part of this proposition and (4.33) show that

$$q\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)\in\left(1-\zeta_p\right)\mathbb{Z}\left[\zeta_{2^m p^n}\right].$$

Hence,

$$q\psi\left(\overline{\theta}_{\mathfrak{C}_{2^m p^n}}\right)\in\mathbb{Z}\left[\zeta_{2^m p^n}\right].$$

We have now shown that under either of the hypotheses $\left|\tilde{S}_2\right|\geq p^{n-1}$ or $p\mid q$, $q\psi\left(\overline{\theta}_{\mathfrak{C}_{2^m p^n}}\right)$ is integral.

Set $\psi=\chi^{2^m+p^n}$. Using the expressions (4.35) and (4.36) for $\overline{\theta}_{\mathfrak{C}_{2^m p^n}}$, we have

$$q\sum_{i=0}^{p^{n-1}(p-1)-1}\chi^{p^n}\left(b_i\right)\zeta_{p^n}^i\in\mathbb{Z}\left[\zeta_{2^m p^n}\right].$$

The numbers $\zeta_{p^n}^i$ for $i=0,\ldots,p^{n-1}(p-1)-1$ form a relative integral basis for $\mathbb{Z}\left[\zeta_{2^m p^n}\right]$ over $\mathbb{Z}\left[\zeta_{2^m}\right]$. It follows that the numbers $q\chi^{p^n}\left(b_i\right)$ in $\mathbb{Q}\left(\zeta_{2^m}\right)$ are algebraic integers.

Let τ denote complex conjugation. Property 4 of components of L-function evaluators shows that

$$\theta_{\mathfrak{C}_{2^m p^n}} = \sum_{i=0}^{p^n-1} a_i \sigma^i$$

is annihilated by $1+\tau$. Thus, $(1+\tau)a_i = 0$ for all i, and hence $(1+\tau)b_i = 0$ for all i. For each i such that $0 \leq i \leq p^{n-1}(p-1)-1$, we may therefore write

$$b_i = \sum_{j=0}^{2^{m-1}-1} \beta_{ij} \sigma'^j \frac{1-\tau}{2}$$

for some rational numbers β_{ij}. Then

$$q\chi^{p^n}(b_i) = \sum_{j=0}^{2^{m-1}-1} q\beta_{ij}\zeta_{2^m}^j.$$

Since the left side was shown to be in $\mathbb{Z}[\zeta_{2^m}]$ and since, for $j = 0, \ldots, 2^{m-1}-1$, the numbers $\zeta_{2^m}^j$ form an integral basis for $\mathbb{Z}[\zeta_{2^m}]$, it follows that the coefficients $q\beta_{ij}$ are in $\mathbb{Z}$. Therefore, each b_i is in $\frac{1}{2q}\mathbb{Z}[H']$, and hence $\overline{\theta}_{\mathfrak{C}_{2^m p^n}}$ is contained in

$$\frac{1}{2p}\mathbb{Z}[G] \cap \frac{1}{pq}\mathbb{Z}[G] = \frac{1}{q}\mathbb{Z}[G].$$

□

To conclude this section, we provide an instance where $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ can be shown to have an affirmative answer. In the next section, we will present another instance.

Proposition 4.6.4. *If Brumer's Conjecture is true for the extension K_n/k_0 and the set S_0, and if Ker is a cyclic $\mathcal{O}$-module, then equation (4.32) is valid up to prime ideals dividing 2 and p. If, additionally, either $|G| = 2p^n$ or p is inert in $\mathbb{Q}(\zeta_{2^m})$, then the p-primary part of equation (4.32) is valid. If 2 is inert in $\mathbb{Q}(\zeta_{p^n})$, then the 2-primary part of equation (4.32) is valid.*

Proof. For simplicity, let $\theta = \theta_{K_n/k_0,S_0}$. Since (B) holds for the extension K_n/k_0 and the set S_0, we know that

$$\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)\,\theta \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{Cl}_{K_n}) \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{Ker}).$$

Let ψ be a generator of $\widehat{G}$. Ker is endowed with an $\mathcal{O}$-module structure through ψ, and

$$\mathrm{Ann}_{\mathcal{O}}\left(\mathrm{Ker}\right) = \psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}\left(\mathrm{Ker}\right)\right).$$

Thus,

$$\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)\,\theta\right) \subseteq \mathrm{Ann}_{\mathcal{O}}\left(\mathrm{Ker}\right).$$

Since Ker is cyclic,

$$\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)\theta\right) \subseteq \mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right).$$

Therefore, there exists an integral ideal $\mathfrak{a}$ in $\mathcal{O}$ such that

$$\psi\left(\mathrm{Ann}_{\mathbb{Z}[G]}(\mu_n)\theta\right) = \mathfrak{a}\,\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right).$$

Equation (4.34) then shows that

$$\mathfrak{P}^e\,\mathrm{Fit}_{\mathcal{O}}\left(\tilde{\mu}\right)\psi\left(\theta\right) = \mathfrak{a}\,\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right).$$

By equation (4.25),

$$\psi\left(\theta\right) = \psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right).$$

Taking absolute norms and using equation (4.31), we find that $\mathfrak{a}$ is supported at primes dividing 2 and p. This proves the first statement of the proposition. The other statements all follow from the fact that the p'-primary part of $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ has an affirmative answer whenever there is only one prime ideal of $\mathcal{O}$ dividing p'. □

4.7 L-values for degree $2^m p^n$ extensions

Proving formula (4.32) in general seems to be beyond the capabilities of the above methods, because the analytic class number formula only gives information about a product of values of L-functions, in other words, about norms of L-values. However, we can mimic the methods in Section 4.4 to prove formula (4.32) in special cases. We will use the same notation as in Section 4.6. In addition, assume that there exists a field k' such that $k' \subset k_0 \subset K_n$, with K_n/k' and k_0/k' Galois. Assume further that S_0 is stable under the action of $\mathrm{Gal}\left(K_n/k'\right)$ on the ideal group

of k_0. Let $F = \mathrm{Gal}\,(k_0/k')$. Then F acts on $\mathbb{Z}[G]$ as described in Section 2.7. The action of F fixes the unique element τ of G of order 2 and also N_p. We thus have an induced homomorphism

$$\phi\colon F \to \mathrm{Aut}\,(\mathbb{Z}\,[G]\,/\,(1+\tau, N_p)) \cong \mathrm{Aut}\,(\mathcal{O}) \cong \mathrm{Gal}\,(\mathbb{Q}\,(\zeta_{2^m p^n})\,/\mathbb{Q})\,.$$

We need a preliminary lemma.

Lemma 4.7.1. *If F acts nontrivially either on H' or on $\sigma^{p^{n-1}}$, then $q = 1$.*

Proof. If F acts nontrivially on H', then Lemma 4.4.1 applies with the objects K, k, k', H, G, and W in that lemma set equal to K_n, k_n, k', $\mathrm{Gal}\,(k_n/k')$, H', and W_n respectively (note that k_n/k' is normal since H' is a characteristic subgroup of G, and that S_n is stable under the action of $\mathrm{Gal}\,(K_n/k')$ since S_0 is.) Thus, $W_n = 2$, and so $q = 1$.

Otherwise, suppose that ρ is an element of F that acts nontrivially on $\sigma^{p^{n-1}}$. Choose an element $\tilde{\rho}$ in $\mathrm{Gal}\,(K_n/k')$ that restricts to ρ. Set $\rho \cdot \sigma^{p^{n-1}} = \sigma^{cp^{n-1}}$, where $2 \le c \le p-1$. If ζ is a primitive W_nth root of unity, assume that $\tilde{\rho}(\zeta) = \zeta^r$ and $\sigma^{p^{n-1}}(\zeta) = \zeta^s$ where $(rs, W_n) = 1$. Then

$$\sigma^{cp^{n-1}}\,(\zeta) = \tilde{\rho}\sigma^{p^{n-1}}\tilde{\rho}^{-1}\,(\zeta) = \zeta^{rsr^{-1}} = \zeta^s. \tag{4.37}$$

Therefore,

$$\zeta^{s^c} = \zeta^s,$$

so that

$$s^c \equiv s \pmod{W_n}.$$

Since $(s, W_n) = 1$, it follows that

$$s^{c-1} \equiv 1 \pmod{W_n}.$$

On the other hand, since $|H| = p^n$, we have

$$\sigma^{p^n}(\zeta) = \zeta^{s^p} = \zeta,$$

so that

$$s^p \equiv 1 \pmod{W_n}.$$

Since $(c-1,p)=1$, there exist integers u and v such that $u(c-1)+vp=1$. Then

$$s = s^{u(c-1)+vp} \equiv 1 \pmod{W_n}.$$

Therefore,

$$\sigma^{p^{n-1}}(\zeta) = \zeta^s = \zeta,$$

so that $W_n = W_{n-1}$ and $q=1$. □

We have the following:

Proposition 4.7.2. *Let ψ generate $\widehat{G}$. Then $\psi(\theta)$ and $Fit_{\mathcal{O}}(Ker)$ are fixed by $\phi(F)$.*

Proof. Let g generate G, and let ζ be the primitive $2^m p^n$-th root of unity satisfying $\psi(g)=\zeta$. We write

$$\theta = \left(\sum_{i=0}^{2^m p^n - 1} a_i g^i \right).$$

Let ρ be in F and let c be an integer such that $\rho \cdot g = g^c$. Suppose that $\tilde{\rho}$ is an element of $\mathrm{Gal}(K_n/k')$ that restricts to ρ. For any i such that $0 \le i \le 2^m p^n - 1$, we have

$$\rho \cdot g^i = g^{ic}.$$

By Proposition 3.2.2, we have an equality of partial zeta functions

$$\zeta_{K_n/k_0,S_0}\left(s, g^i\right) = \zeta_{K_n/k_0,S_0}\left(s, g^{ic}\right)$$

for $i = 0, \ldots, 2^m p^n - 1$. Thus, $a_i = a_{ic}$ for all i (where it is understood that a_{ic} stands for the coefficient of σ^{ic} even if $ic \notin [0, 2^m p^n - 1]$). It follows that

$$\psi(\theta) = \sum_{i=0}^{2^m p^n - 1} a_i \zeta^i$$

is fixed by $\phi(\rho)$, which is the automorphism of $\mathbb{Q}(\zeta_{2^m p^n})$ that sends ζ to ζ^c. Since ρ was an arbitrary element of F, this proves the first part of the proposition.

Since S_0 was assumed to be stable under the action of $\mathrm{Gal}(K_n/k')$, Ker is a $\mathbb{Z}[\mathrm{Gal}(K_n/k')]$-module. This can be demonstrated with the argument used to prove that Ker is a $\mathbb{Z}[G]$-module preceding the statement of the question $\mathrm{Q}_{2^m p^n}(K_n/k_0)$.

One should note in this case that although H is not necessarily in the center of $\mathrm{Gal}\left(K_n/k'\right)$, the elements of $\mathrm{Gal}\left(K_n/k'\right)$ do commute with N_p. The second part of the proposition now follows from Proposition 2.7.1. □

Corollary 4.7.3. *If*

$$\mathbb{Q}\left(\zeta_{2^m p^n}\right)^{\phi(F)} = \mathbb{Q},$$

then equation (4.32) *is valid.*

Proof. Let ψ generate $\widehat{G}$. By the previous proposition, $\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)$ is in $\mathbb{Q}$. Also, ψ endows Ker with the structure of an $\mathcal{O}$-module, and $\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)$ is fixed by $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{2^m p^n}\right)/\mathbb{Q}\right)$. We can therefore write

$$\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right) = \left(1-\zeta_{2^m}\right)^{e_2}\left(1-\zeta_{p^n}\right)^{e_p} c\,\mathcal{O},$$

where c is a rational integer. By Lemma 4.7.1 and equation (4.33), we know that $\mathrm{Fit}_{\mathcal{O}}(\tilde{\mu})$ is equal to $\mathcal{O}$. Since $\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)$ and c are in $\mathbb{Q}$, we can rewrite equation (4.31) as

$$\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)^{2^{m-1}p^{n-1}(p-1)} = \pm\, 2^{p^{n-1}(p-1)\left(\left|\tilde{S}_1\right|+e_2\right)} p^{2^{m-1}\left(\left|\tilde{S}_2\right|+e_p\right)} c^{2^{m-1}p^{n-1}(p-1)}.$$

Therefore, $\left|\tilde{S}_1\right| + e_2$ is divisible by 2^{m-1} and $\left|\tilde{S}_2\right| + e_p$ is divisible by $p^{n-1}(p-1)$. Furthermore,

$$\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right) = \pm\, 2^{\frac{|\tilde{S}_1|+e_2}{2^{m-1}}} p^{\frac{|\tilde{S}_2|+e_p}{p^{n-1}(p-1)}} c.$$

□

Write

$$L = \mathbb{Q}\left(\zeta_{2^m p^n}\right)^{\phi(F)},$$

with $d = |\phi(F)| = [\mathbb{Q}\left(\zeta_{2^m p^n}\right) : L]$. Let ψ generate $\widehat{G}$. Proposition 4.7.2 shows that $\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)$ is in L. In addition, $\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)$ can be written as

$$\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right) = \mathfrak{a}_2\mathfrak{a}_p\mathfrak{a}.$$

where $\mathfrak{a}$ is an integral ideal of L and $\mathfrak{a}_2$ and $\mathfrak{a}_p$ are integral ideals of $\mathcal{O}$ with absolute norms 2^{e_2} and p^{e_p} respectively. Let S_n^{ns} be the set of places of K_n lying above places in $S_0^{\min}$ that do not split completely in K_0.

Corollary 4.7.4. *Let r_2 be the smallest nonnegative residue of*

$$-p^{n-1}(p-1)\left|\tilde{S}_1\right| \ \ mod\ d.$$

Let $\delta = 1$ if $p \mid q$ and let $\delta = 0$ otherwise. Let r_p be the smallest nonnegative residue of

$$\delta - 2^{m-1}\left|\tilde{S}_2\right| \ \ mod\ d.$$

If $h_S^{ns} = \left|\mathrm{Cl}_{K_n,S_n^{ns}}\right|$ is the S_n^{ns} class number of K_n, then

$$2^{r_2}p^{r_p} \mid h_S^{ns},$$

Proof. Let $\mathfrak{N}$ denote the absolute norm on ideals of L. We can rewrite equation (4.31) as

$$q\,\mathfrak{N}\left(\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right)\right)^d = 2^{p^{n-1}(p-1)\left|\tilde{S}_1\right|+e_2}p^{2^{m-1}\left|\tilde{S}_2\right|+e_p}\,\mathfrak{N}\left(\mathfrak{a}\right)^d.$$

Since $(2,q)=1$ and the exact power of p dividing q is either 1 or p, the integers $p^{n-1}(p-1)\left|\tilde{S}_1\right| + e_2$ and $2^{m-1}\left|\tilde{S}_2\right| + e_p - \delta$ are divisible by d. By property 6 of Fitting ideals from Section 2.4 and the definition of e_2 and e_p, $|\mathrm{Ker}|$ is divisible by 2^{e_2} and by p^{e_p}. □

Example. Set $k_0 = \mathbb{Q}\left(\sqrt{105}\right)$, and set $K_0 = k\left(\zeta_3\right)$. According to calculations performed with PARI/GP, the polynomial $x^{12} - 51x^6 + 729$ defines a non-Abelian Galois extension field K_1 of $\mathbb{Q}$ which is also an Abelian cubic extension of K_0. The extension K_1/K_0 is ramified only at the two primes of K_0 dividing 3. Set $S_0 = S_0^{\min}$, which in this case consists of the two Archimedean places of k and the lone prime ideal of k dividing 3. Then the set $\tilde{S}_1$ consists of the two Archimedean places of K_0, and the set $\tilde{S}_2$ is empty.

Let $k' = \mathbb{Q}$. Since $\mathrm{Gal}\left(K_1/k'\right)$ is non-Abelian, $\mathrm{Gal}\left(k/k'\right)$ acts nontrivially on G. Lemma 4.7.1 then shows that $q = 1$, so that $W_1 = 6$. Corollary 4.7.3 also applies, showing that the answer to $\mathrm{Q}_{2^m p^n}\left(K_1/k_0\right)$ is affirmative. Finally, the numbers r_2 and r_p in Corollary 4.7.4 are 0 and 1. PARI/GP says that the class numbers of k_0, K_0, k_1, and K_1 are 2, 2, 2, and 18 respectively. Since K_1/k_1 is ramified at the Archimedean places, the norm map on the the ideal class groups is surjective, so that ideals representing the class of order 2 in k_1 lift to principal ideals in K_1.

Since the prime ideal of k_0 lying above 3 splits in K_0/k_0, the set S_0^{ns} contains only the Archimedean places of k_0. Therefore, $|\text{Coker}_1| = 9$, and similarly, $|\text{Coker}_0| = 1$. Thus, $|\text{Ker}| = 9$, which is divisible by 3 as is predicted by the corollary.

Finally, we note that this corollary has the same feature as Corollary 4.4.4 – one can let the sets $\tilde{S}_1$ and $\tilde{S}_2$ vary, producing seemingly different results. One can show using similar methods as in the example following Corollary 4.4.4 that in the present example, at least, $|S_2|$ is always even when S_0 is stable under the action of $\text{Gal}\,(K_1/k')$.

4.8 A generalization of a theorem of Kummer

One of the first results relating the special values of L-functions to the arithmetic of number fields was discovered by Kummer. We denote the Riemann zeta function by $\zeta(s)$. The numbers $\zeta(-n)$ for $n = 1, 3, \ldots, p-4$ are p-integral rational numbers.

Kummer's Criterion. *An odd prime number divides at least one of the numbers $\zeta(-n)$ for $n = 1, 3, \ldots, p-4$ if and only if the following equivalent assertions hold:*

1. *p divides the class number h of $\mathbb{Q}\,(\zeta_p)$.*
2. *p divides the relative class number h^- of $\mathbb{Q}\,(\zeta_p)$.*
3. *There exists a cyclic extension of $\mathbb{Q}\,(\zeta_p)^+$, distinct from $\mathbb{Q}\,(\zeta_{p^2})^+$ and unramified away from primes dividing p.*

The equivalence $1 \Leftrightarrow 2$ is one of the inspirations for Leopoldt's Spiegelungssatz, or reflection theorem ([34]). The equivalence $1 \Leftrightarrow 3$ can be found, for instance, in [60, Proposition 10.13].

In this section, we will first provide a generalization of the implication $3 \Rightarrow 2$. We will then prove a result on class numbers in the case where K is a number field *not* containing the pth roots of unity. Both proofs use similar methods; it is perhaps surprising that neither proof makes explicit use of Kummer theory.

Before we state the first theorem, we must fix some notation. Let K/k be a cyclic extension of number fields of degree 2^m. Assume that k is totally real and K

is totally complex. Let $S^{\min}$ be the set of places of k consisting of the Archimedean places and the prime ideals that ramify in K/k. We abuse notation by also writing $S^{\min}$ for the set of places in K^+ and for the set of places in K lying above the places of $S^{\min}$ in k. Let Coker be the cokernel of the canonical map $\mathrm{Cl}_{K^+,S^{\min}} \to \mathrm{Cl}_{K,S^{\min}}$. Set $\mathcal{O} = \mathbb{Z}[\zeta_{2^m}]$. Let χ be a character on $\mathrm{Gal}(K/k)$ of order 2^m. We write τ for the element in $\mathrm{Gal}(K/k)$ of order 2. As in Section 4.3, Coker is annihilated by $1+\tau$, and χ provides Coker with an $\mathcal{O}$-module structure. Furthermore, χ provides the group μ of roots of unity in K with an $\mathcal{O}$-module structure. Let p be an odd prime number and assume that p^t is the exact power of p dividing $|\mu|$. If F_p is the factor of the ideal $\mathrm{Fit}_{\mathcal{O}}(\mu)$ supported at primes dividing p, then Lemma 2.4.1 shows that there is a prime ideal $\mathfrak{P}$ in $\mathcal{O}$ dividing p and of residual degree 1 such that

$$F_p = \mathfrak{P}^t.$$

We can now state the generalization of Kummer's criterion.

Theorem 4.8.1. *Let n be an integer with $0 \leq n \leq t$. Suppose that the p-primary part of $\mathrm{Q}_{2^m}(k_m/k_0)$ has an affirmative answer. Assume that there exists a cyclic extension L of k of degree p^n satisfying:*

1. *The number of p-power roots of unity in LK is p^t.*
2. *No place in k splits completely in K/k and ramifies in L/k.*

Then $\mathfrak{P}^n$ divides $\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})$.

Proof. We change the notation to that of Section 4.6, providing K, k, and $S^{\min}$ with the subscript 0. We set $L = k_n$. Then these fields satisfy the assumptions from Section 4.5, and we will resume using the rest of the notation from that section. Set

$$N_H = \sum_{i=0}^{p^n-1} \sigma^i,$$

the norm element in $\mathbb{Q}[G]$ corresponding to the extension K_n/K_0. For $1 \leq r \leq n$, let $\mathfrak{C}_{2^m p^r}$ be the equivalence class of characters in $\widehat{G}$ of order $2^m p^r$. Let $\mathfrak{C}$ be the equivalence class of characters in $\widehat{G}$ of order 2^m. We write θ for $\theta_{K_0/k_0,S_0}$ and $\tilde{\theta}$ for

the lift of $\theta_{K_0/k_0,S_0}$ to $\mathbb{Q}[H']$. Property 2 of components of L-function evaluators from Section 3.3 shows that

$$\theta_{K_n/k_0,S_0,\mathfrak{E}} = \frac{1}{p^n}\tilde{\theta}N_H.$$

For $1 \leq r \leq n$, set

$$q_r = \frac{W_r}{W_{r-1}}.$$

Property 2 of components of L-function evaluators and Proposition 4.6.3 show that, for $1 \leq r \leq n$,

$$\theta_{K_n/k_0,S_0,\mathfrak{E}_{2^{m}p^r}} \in \frac{1}{p^{n-r+1}q_r}\mathbb{Z}[G].$$

Assumption 1 on L in the theorem implies that $(p, q_r) = 1$ for all r. Since $n-r+1 \leq t$ for all such r, it follows that

$$W_n\theta_{K_n/k_0,S_0,\mathfrak{E}_{2^{m}p^r}} \in \mathbb{Z}[G].$$

Then the relation

$$\theta_{K_n/k_0,S_0} = \sum_{r=0}^{n} \theta_{K_n/k_0,S_0,\mathfrak{E}_{2^{m}p^r}}$$

and Theorem 3.2.4 imply that

$$W_n\theta_{K_n/k_0,S_0,\mathfrak{E}} = \frac{W_n}{p^n}\tilde{\theta}N_H \in \mathbb{Z}[G].$$

As $\tilde{\theta}$ is in $\mathbb{Q}[H']$ and N_H is in $\mathbb{Q}[G]$, it follows that

$$\frac{W_n}{p^n}\theta \in \mathbb{Z}[\mathrm{Gal}(K_0/k_0)].$$

We will have no further need for the group H', so we now let $H' = \mathrm{Gal}(K_0/k_0)$. Since the p-primary part of $\mathrm{Q}_{2^m}(k_m/k_0, S_0)$ has an affirmative answer, the above inclusion implies that

$$W_n \,\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})\left(p^n \,\mathrm{Fit}_{\mathcal{O}}(\mu)\right)^{-1}$$

is a $\mathfrak{P}$-integral fractional ideal of $\mathcal{O}$. Using assumption 1 on L in the theorem, it follows that

$$p^t \,\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})\left(p^n F_p\right)^{-1} = p^t \,\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})\left(p^n\mathfrak{P}^t\right)^{-1}$$

is a $\mathfrak{P}$-integral fractional ideal of $\mathcal{O}$. Consideration of $\mathfrak{P}$-valuations then shows that

$$\mathfrak{P}^n \mid \mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right).$$

□

Corollary 4.8.2. *Let K be a CM field containing the p^nth roots of unity. Assume that there exists a cyclic extension L of K^+ of degree p^n satisfying*

1. *The number of p-power roots of unity in LK is the same as the number of p-power roots of unity in K.*

2. *No place in K^+ splits completely in K/K^+ and ramifies in L/K^+.*

Then p^n divides $|\mathrm{Coker}|$.

Proof. This follows immediately from the above theorem and the fact that $\mathrm{Q}_{2^m}\left(k_m/k_0\right)$ has an affirmative answer for quadratic extensions. □

Remarks.

1. When $k = \mathbb{Q}\left(\zeta_p\right)^+$ and $K = \mathbb{Q}\left(\zeta_p\right)$, this is exactly implication $3 \Rightarrow 2$ of Kummer's Criterion.

2. Condition 2 above is essential, as is illustrated by the following example. Set $k = \mathbb{Q}\left(\sqrt{105}\right)$, and set $K = k\left(\zeta_3\right)$. According to calculations performed with PARI/GP, the polynomial $x^{12} - 51x^6 + 729$ defines a cubic extension field L of K, Abelian over k, unramified outside of primes dividing 3, and not containing the 9th roots of unity. The prime ideal of k lying above 3 splits in K/k and ramifies in L. Thus, all of the conditions in the corollary are satisfied except for condition 2. However, the class number of K is 2.

Results related to the case $n = 1$ in the corollary above were derived in [13] and [31]. Condition 2 was also a necessary assumption in those papers. For another similar result when k is imaginary quadratic, see [7].

For the second theorem, suppose that K_n/k_0 is a cyclic extension of number fields of degree $2^m p^n$. Assume that k_0 is totally real and K_n is totally complex. For

$0 \leq r \leq n$, let k_r and K_r be as defined in Section 4.6. Let G, H, H', σ, σ', $S_0^{\min}$ and S_r^{ns}, Coker_{n-1}, Coker_n, and Ker be as defined in Section 4.6. Let $\mathcal{O} = \mathbb{Z}[\zeta_{2^m p^n}]$. Let χ be a generator of $\widehat{G}$. Let $\tilde{\mu} = \mu_n/\mu_{n-1}$ as in Section 4.6. Then χ provides Ker and $\tilde{\mu}$ with $\mathcal{O}$-module structures.

Theorem 4.8.3. *Assume that K_n does not contain the pth roots of unity, and that there exists a prime ideal of k_0 that splits completely in K_0/k_0 and k_{n-1}/k_0, but ramifies in k_n/k_{n-1}. Suppose that the question $\text{Q}_{2^m p^n}(K_n/k_0, S_0)$ has an affirmative answer. Then*

$$(1-\zeta_p) \mid \text{Fit}_{\mathcal{O}}(Ker).$$

Proof. Let $\mathfrak{C}$ denote the equivalence class of characters in $\widehat{G}$ of order $2^m p^n$. Assume that $S_0 = S_0^{\min}$, so that $\tilde{S}_2$ is empty. Set

$$\theta_{\mathfrak{C}} = \theta_{K_n/k_0, S_0, \mathfrak{C}}.$$

Since k_0 contains a prime ideal that splits completely in K_r/k_0 for $0 \leq r \leq n-1$, it follows that

$$\theta_{K_r/k_0, S_0} = 0$$

for these values of r. Repeated application of property 2 of components of L-function evaluators then shows that

$$\theta_{K_n/k_0, S_0} = \theta_{\mathfrak{C}}.$$

Let $\theta_{\mathfrak{C}} = \left(1 - \sigma^{p^{n-1}}\right) \tilde{\theta}_{\mathfrak{C}}$ as in equations (4.35) and (4.36). By Proposition 4.6.3,

$$\tilde{\theta}_{\mathfrak{C}} \in \frac{1}{pq}\mathbb{Z}[G].$$

Theorem 3.2.4 and the assumption that $(W_n, p) = 1$ then imply that

$$\tilde{\theta}_{\mathfrak{C}} \in \frac{1}{q}\mathbb{Z}[G].$$

Since the p-primary part of $\text{Q}_{2^m p^n}(K_n/k_0, S_0)$ has an affirmative answer,

$$\frac{q(1-\zeta_{2^m})^{|\tilde{S}_1|}\,\text{Fit}_{\mathcal{O}}(\text{Ker})}{(1-\zeta_p)\,\text{Fit}_{\mathcal{O}}(\tilde{\mu})}$$

is p-integral. Therefore, $(1-\zeta_p)$ divides $\text{Fit}_{\mathcal{O}}(\text{Ker})$. □

Corollary 4.8.4. *Under the assumptions of the theorem,*

$$p^{2^{m-1}p^{n-1}} \mid |\mathrm{Ker}|\,.$$

Also, the p-rank of Ker is at least 2^{m-1}.

Proof. The first statement is a consequence of property 6 of Fitting ideals from Section 2.4. For the second part, we begin by using the primary decomposition theorem for finitely generated torsion modules. It says that the p-primary part of Ker is isomorphic to a module of the form

$$\bigoplus_{i=1}^{g} \left(\mathcal{O}/\mathfrak{P}_{\mathfrak{i}}{}^{e_{i,1}} \oplus \cdots \oplus \mathcal{O}/\mathfrak{P}_{\mathfrak{i}}{}^{e_{i,l(i)}}\right),$$

where the ideals $\mathfrak{P}_i$ are the prime ideals in $\mathcal{O}$ dividing p. By the theorem and properties 3 and 4 of Fitting ideals,

$$(1-\zeta_p) \mid \prod_{i=1}^{g}\prod_{j=1}^{l(i)} \mathfrak{P}_i^{e_{i,j}}.$$

Thus, the sums

$$\sum_{j=0}^{l(i)} e_{i,j}$$

are each at least p^{n-1}. In particular, every prime ideal of $\mathcal{O}$ dividing p appears at least once in the above double product. Each factor in the direct sum decomposition of the p-primary part of Ker is an Abelian p-group of rank f, the residual degree of p in $\mathbb{Q}\left[\zeta_{2^m}\right]$. The p-rank of Ker is therefore at least fg, which equals 2^{m-1}. □

Corollary 4.8.5. *If assumptions are as in the theorem, then*

$$p \mid \left|Ker^H\right|,$$

where Ker^H *is the subgroup of Ker fixed by* H.

Proof. The subgroup of elements of Ker annihilated by p is a nonzero vector space over the finite field F_p. The element σ acts as a nonsingular linear transformation on this vector space, hence has an eigenvector v with associated eigenvalue c in $F_p^{\times}$. As σ^{p^n} is the identity transformation, it follows that $c^{p^n} = 1$, so that $c = 1$. Thus, v is fixed by σ, and hence, by H. □

Corollary 4.8.6. *With assumptions as in the Theorem,*

$$p \mid |Ker/(1-\sigma)Ker|$$

Proof. Let $N_H = \sum_{i=0}^{p^n-1} \sigma^i$. Since Ker is a finite module over the cyclic group H, we have

$$\left[\mathrm{Ker}^H \colon N_H \mathrm{Ker}\right] = \left[\mathrm{Ker}_{N_H} \colon (1-\sigma)\mathrm{Ker}\right],$$

where Ker_{N_H} is the part of Ker annihilated by the action of N_H. Since $\mathrm{Ker} = \mathrm{Ker}_{N_H}$ and $N_H \mathrm{Ker} = 0$, the result follows from the previous corollary. □

It should be noted that when $m = n = 1$, this result is somewhat weaker than Lemma 2.5 in [18], which is proved using Lemma 4.1 on p. 307 of [32].

Example. Let $k_0 = \mathbb{Q}$, and let K_0 be the quartic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{13})$. Let k_1 be the cubic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{61})$. Let $K_1 = K_0 k_1$. Then K_1 is a totally complex cyclic extension of $\mathbb{Q}$ of degree 12. The cube roots of unity are not contained in K_1. Finally, the prime ideal (61) in $\mathbb{Q}$ splits completely in K_0/k_0 and ramifies in k_1/k_0. Therefore, Corollary 4.8.4 applies to this example, and says that the 3-rank of the class group of K_1 is at least 2. According to calculations performed with PARI/GP, the primary decomposition of the class group of K_1 is

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/13\mathbb{Z}.$$

Now let $k_0 = \mathbb{Q}\left(\sqrt{321}\right)$. Let k_2 be the splitting field of the polynomial

$$\begin{aligned} x^{18} - 6x^{17} - 24x^{16} + 157x^{15} + 231x^{14} - 1482x^{13} \\ - 1225x^{12} + 6789x^{11} + 3981x^{10} - 16463x^9 - 7857x^8 + 21195x^7 \\ + 8378x^6 - 13656x^5 - 3681x^4 + 4027x^3 + 270x^2 - 441x + 49. \end{aligned}$$

PARI/GP determined that k_2 is a non-Abelian Galois extension of $\mathbb{Q}$ of degree 18, and hence an Abelian extension of k_0 of degree 9. The prime ideals of k_0 dividing 5 are inert in k_2/k_0. Since decomposition groups are cyclic, k_2/k_0 is a cyclic extension of degree 9 (and incidentally, $\mathrm{Gal}(k_2/\mathbb{Q})$ must be the dihedral group of order 18).

The prime ideal of k_0 dividing 3 splits completely in the extensions $K_0 = k_0\left(\sqrt{-5}\right)$ and $K_0' = k_0\left(\sqrt{-11}\right)$. Set $K_2 = K_0 k_2$ and $K_2' = K_0' k_2$. Both of K_2 and

K_2' are totally complex cyclic extensions of k_0 of degree 18, and neither contains the cube roots of unity. Therefore, Corollary 4.8.4 applies to these examples, and says that the class numbers of K_2 and K_2' are divisible by 27. According to calculations done with PARI/GP, the class group of K_2 is isomorphic to

$$(\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^6 \oplus (\mathbb{Z}/17\mathbb{Z})^2 \oplus (\mathbb{Z}/971\mathbb{Z})^2 .$$

The class group of K_2' is isomorphic to

$$(\mathbb{Z}/2\mathbb{Z})^8 \oplus \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^4 \oplus (\mathbb{Z}/5\mathbb{Z})^2 \oplus (\mathbb{Z}/53\mathbb{Z})^2 .$$

4.9 L-values in cyclotomic towers

Since the set S_0 will not have a significant role in this section, we will suppress it from the notation. Let k_0 be a totally real field, and let p be an odd prime number such that $K_0 = k_0(\zeta_p)$ is a degree 2^m extension for some positive integer m. Let p^v be the cardinality of the p-power roots of unity in K_0. We then set $K_n = k_0(\zeta_{p^{v+n}})$ for all positive integers n, so that the fields K_n form the p-cyclotomic tower of extensions of $k_0(\zeta_p)$. For $n \geq 0$, set $G_n = \mathrm{Gal}(K_n/k_0)$. Each extension K_n/k_0 has degree $2^m p^n$, so we may apply the results of Section 4.6 to these extensions. Let W_n denote the number of roots of unity in K_n. In this section, we will show that the coefficients of the integralized L-function evaluators $W_n\theta_{K_n/k_0}$ align into p-adic integers.

A crucial fact in the proof is the following lemma

Lemma 4.9.1. *There exists an integer M such that for $n > M$,*

$$\frac{W_n}{W_{n-1}} = p.$$

Proof. To begin, assume that $\tilde{p}$ is a prime number different from p that divides $\frac{W_n}{W_{n-1}}$ for some n. As $\tilde{p} \neq p$, there is one level n where this occurs. Since K_n contains the $\tilde{p}$th roots of unity and K_n/K_0 has odd order, K_0 must contain the quadratic subfield of $\mathbb{Q}(\zeta_{\tilde{p}})$. Therefore, there can exist only finitely many such prime numbers $\tilde{p}$. □

Proposition 4.9.2. *Let $\{\sigma_n\}_{n>1}$ be a sequence of elements in the Galois groups G_n, compatible under the projection maps. Let c_n be the coefficient of σ_n in $W_n\theta_{K_n/k_0}$. Then the limit*

$$\lim_{n\to\infty} c_n$$

exists in $\mathbb{Z}_p$.

Proof. The odd characters on G_n fall into $n+1$ equivalence classes under the equivalence relation from Section 3.3. Each equivalence class consists of the characters of order $2^m p^r$ for some r such that $0 \le r \le n$; we will denote the equivalence class for a given r by $\mathfrak{C}_{n,2^m p^r}$.

If $n \ge 1$, the L-function evaluator for the extension K_n/k_0 decomposes into components as

$$\theta_{K_n/k_0} = \sum_{r=0}^{n} \theta_{\mathfrak{C}_{n,2^m p^r}}.$$

For $1 \le r \le n$, let N_{p^r} be the norm element in $\mathbb{Q}[G]$ corresponding to the extension K_n/K_{n-r}. Using a tilde to denote a lift to $\mathbb{Z}[G_n]$, property 2 of components of L-function evaluators shows that

$$\begin{aligned}\theta_{K_n/k_0} &= \theta_{\mathfrak{C}_{n,2^m p^n}} + \sum_{r=0}^{n-1} \frac{1}{p^{n-r}} \tilde{\theta}_{\mathfrak{C}_{r,2^m p^r}} \mathrm{N}_{p^{n-r}} \\ &= \theta_{\mathfrak{C}_{n,2^m p^n}} + \frac{1}{p}\tilde{\theta}_{K_{n-1}/k_0} \mathrm{N}_p\,. \end{aligned} \tag{4.38}$$

Write

$$\theta_{K_{n-1}/k_0} = \sum_{\sigma\in G_{n-1}} a_\sigma \sigma.$$

For each σ in G_{n-1}, choose an arbitrary lift $\tilde{\sigma}$ of σ to G_n. We then choose to lift θ_{K_{n-1}/k_0} as

$$\tilde{\theta}_{K_{n-1}/k_0} = \sum_{\sigma\in G_{n-1}} a_\sigma \tilde{\sigma}.$$

Let M be an integer as defined in Lemma 4.9.1. For $n > M$,

$$W_n \frac{1}{p}\tilde{\theta}_{K_{n-1}/k_0} \mathrm{N}_p = W_{n-1}\tilde{\theta}_{K_{n-1}/k_0} \mathrm{N}_p\,.$$

This shows that the coefficient of σ_n in $W_n \frac{1}{p}\tilde{\theta}_{K_{n-1}/k_0} N_p$ is c_{n-1}. Furthermore, since p^{v+n-1} divides W_{n-1}, Proposition 4.6.3 shows that

$$W_n \theta_{\mathfrak{C}_{n,2^m p^n}} \in p^{v+n-1}\mathbb{Z}[G]\,.$$

It then follows from equation (4.38) that

$$c_n \equiv c_{n-1} \pmod{p^{v+n-1}}. \qquad \square$$

Remark. It is known that the values of the equivariant L-functions in the p-cyclotomic tower of a totally real field align p-adically. This was the construction of p-adic L-functions given in [6]. However, this does not immediately imply the above proposition.

Chapter 5

The Brumer-Stark Conjecture

In this chapter, we will use the formulae for L-values determined in Chapter 4 to prove cases of the Brumer-Stark conjecture.

5.1 The Brumer-Stark conjecture for extensions of degree 2^m

In this section, we will prove some of the local parts of the Brumer-Stark conjecture for cyclic extensions of number fields of degree 2^m. To begin, we need a preliminary lemma.

Lemma 5.1.1. *Let K/k be a cyclic extension of number fields of degree 2^m with $m \geq 2$. Assume that k is totally real. Then the 2-power roots of unity in K are 1 and -1.*

Proof. If K is not totally complex, then the conclusion is immediate. If K is totally complex, then the unique element τ of order 2 in $G = \mathrm{Gal}(K/k)$ is the complex conjugation corresponding to each embedding of K into $\mathbb{C}$. Therefore, K is a CM field. We denote the group of 2-power roots of unity in K by $\mu_K^{(2)}$.

Assume that $\left|\mu_K^{(2)}\right| = 2^c > 2$. Then there are non-real roots of unity in $\mu_K^{(2)}$, so that

$$K = k\left(\mu_K^{(2)}\right).$$

Thus, G is isomorphic to a subgroup of $\mathfrak{G} = \mathrm{Gal}\left(\mathbb{Q}\left(\mu_K^{(2)}\right)/\mathbb{Q}\right)$. Moreover, the complex conjugation τ restricts to complex conjugation in $\mathfrak{G}$. Under the isomorphism

$$\mathfrak{G} \to (\mathbb{Z}/2^c\mathbb{Z})^\times,$$

complex conjugation is mapped to -1. Since $c \geq 2$, -1 is not a square in this group. It follows that τ is not a square in G, a contradiction. Hence $\left|\mu_K^{(2)}\right| = 2$. $\square$

We resume the notation of Section 4.3.

Theorem 5.1.2. *Let k_m/k_0 be a cyclic extension of number fields of degree $2^m \geq 4$ with Galois group G. Let $\delta = 1$ if no prime ideal ramifies in k_m/k_0 or the 2-primary part of Coker is trivial. Otherwise, let $\delta = 0$. Then*

$$W\theta_{k_m/k_0} \in 2^{[k_0\colon \mathbb{Q}]-\delta}\,\mathbb{Z}[G],$$

and the 2-primary part of the Brumer-Stark conjecture is true with θ_{k_m/k_0} replaced by

$$\frac{1}{2^{[k_0\colon \mathbb{Q}]-\delta-1}}\theta_{k_m/k_0}.$$

In particular, (BS_2) is true for k_m/k_0.

Remark. This result was obtained independently by Greither, Roblot, and Tangedal in an unpublished manuscript ([17]). Their methods are similar, especially the proof of the Abelian condition of (BS_2). This is not surprising, as this proof is based on methods used by Tate and Sands in early work on the subject. In the same manuscript, Greither, Roblot, and Tangedal also proved (BS_2) for extensions K/k with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and such that K^+/k is not cyclic.

Proof. To avoid triviality, we assume that k_0 is totally real and k_m is totally complex. Let $W = |\mu|$ be the cardinality of the group of roots of unity in k_m. Let $S_0^{\min}$ be the set of places of k_0 comprising the Archimedean places and the prime ideals that ramify in k_m/k_0. We will denote the L-function evaluator $\theta_{k_m/k_0,S_0^{\min}}$ simply by θ. Let σ generate G, let $\tau = \sigma^{2^{m-1}}$, let χ generate $\widehat{G}$, and let ζ_{2^m} be the primitive 2^mth root of unity such that $\chi(\sigma) = \zeta_{2^m}$. Let k_m^+ be the maximal totally

real subfield of k_m. We will denote the sets of places in k_m^+ and k_m lying above the places in $S_0^{\min}$ by S^+ and S. Let Coker be the cokernel of the canonical map $\mathrm{Cl}_{k_m^+,S^+} \to \mathrm{Cl}_{k_m,S}$. Set $\mathcal{O} = \mathbb{Z}[\zeta_{2^m}]$ and $\lambda = 1 - \zeta_{2^m}$. Let v_λ denote the normalized valuation on $\mathcal{O}$ corresponding to the prime ideal (λ).

Property 2 of L-function evaluators in Section 3.1 shows that we can write

$$W\theta = \sum_{i=0}^{2^{m-1}-1} a_i \sigma^i (1-\tau).$$

When this product is expanded, the coefficient of σ^i for $0 \le i \le 2^{m-1}-1$ is a_i. Theorem 3.2.4 then shows that each a_i is an integer. Set

$$\alpha = \sum_{i=0}^{2^{m-1}-1} a_i \sigma^i.$$

The 2-primary part of the question $\mathrm{Q}_{2^m}(k_m/k_0)$ has an affirmative answer (see the comment before Proposition 4.3.2). It states that

$$v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}(\mu)\,\chi(\theta)\right) = \left|S^+\right| - 1 + v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})\right),$$

where μ and Coker have the $\mathcal{O}$-module structures provided by χ. By equation (4.6) and Lemma 5.1.1,

$$v_\lambda(\chi(\alpha)) = v_\lambda(\chi(\theta)) = \left|S^+\right| - 2 + v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}(\mathrm{Coker})\right). \tag{5.1}$$

The set S^+ contains the Archimedean places of the totally real field k_m^+, which has degree $2^{m-1}[k_0\colon \mathbb{Q}]$ over $\mathbb{Q}$. It follows that

$$v_\lambda\left(\sum_{i=0}^{2^{m-1}-1} a_i \zeta_{2^m}^i\right) \ge 2^{m-1}[k_0\colon \mathbb{Q}] - 2\delta \ge 2^{m-1}\left([k_0\colon \mathbb{Q}] - \delta\right).$$

Therefore, the algebraic integer $\sum_{i=0}^{2^{m-1}-1} a_i \zeta_{2^m}^i$ is divisible by $2^{[k_0\colon \mathbb{Q}]-\delta}$ in $\mathcal{O}$. Since the numbers $\zeta_{2^m}^i$ for $0 \le i \le 2^{m-1}-1$ form an integral basis for $\mathcal{O}$, it follows that the integers a_i are divisible by $2^{[k_0\colon \mathbb{Q}]-\delta}$. This proves the first statement of the theorem.

Next, set

$$\alpha' = \frac{1}{2^{[k_0\colon \mathbb{Q}]-\delta-1}}\,\alpha \qquad \text{and} \qquad \theta' = \frac{1}{2^{[k_0\colon \mathbb{Q}]-\delta-1}}\,\theta.$$

Equation (5.1) shows that

$$\begin{aligned} v_\lambda\left(\chi(\alpha')\right) &\geq 2^{m-1}\left(\delta+1\right)-\delta-1+v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right)\right) \\ &\geq v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right)\right). \end{aligned} \tag{5.2}$$

Thus, the algebraic integer $\chi\left(\alpha'\right)$ is divisible by the $\mathcal{O}$-Fitting ideal of the 2-primary part of Coker. As α' acts on this $\mathcal{O}$-module as $\chi\left(\alpha'\right)$, property 2 of Fitting ideals shows that α' annihilates the 2-primary part of Coker.

Now let $\mathfrak{a}$ be an ideal representing a class in the 2-primary part of Cl_{k_m}. Since α' annihilates the class of $\mathfrak{a}$ in Coker, we have

$$\mathfrak{a}^{\alpha'}=\mathfrak{b}\mathfrak{c}\left(\gamma\right),$$

where $\mathfrak{b}$ is an ideal of k_m with support above the prime ideals in S, $\mathfrak{c}$ is the lift of an ideal from k_m^+, and γ is an element of $k_m^\times$. Since no prime of S^+ splits in k_m, it follows that $\mathfrak{b}^\tau=\mathfrak{b}$. Thus,

$$\mathfrak{a}^{W\theta'}=\left(\mathfrak{b}\mathfrak{c}\left(\gamma\right)\right)^{1-\tau}=\left(\gamma^{1-\tau}\right).$$

We have found that $W\theta'$ annihilates the 2-primary part of Cl_{k_m}, and in fact, the principal ideals produced thereby are generated by anti-units. It remains to be shown that these anti-units can be chosen to be 2-Abelian.

Let P_{anti} denote the group of nonzero principal ideals of k_m generated by anti-units. We will first prove the claim that $(1-\sigma)\frac{W}{2}\theta'$ is in $\mathbb{Z}[G]$ and for any ideal $\mathfrak{a}$ in the 2-primary part of Cl_{k_m},

$$\mathfrak{a}^{(1-\sigma)\frac{W}{2}\theta'}\in P_{\mathrm{anti}}.$$

Using the inequality (5.2), we find that

$$\begin{aligned} v_\lambda\left(\chi\left((1-\sigma)\theta'\right)\right)=v_\lambda\left(\chi\left((1-\sigma)\alpha'\right)\right) &\geq 2^{m-1}\left(\delta+1\right)-\delta+v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right)\right) \\ &\geq 2^{m-1}+v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right)\right). \end{aligned}$$

Arguments similar to those after the inequalities (5.1) and (5.2) then show that 2 divides the coefficients of $(1-\sigma)W\theta'$ and $(1-\sigma)\frac{W}{2}\theta'$ annihilates the 2-primary part of Cl_{k_m}, producing principal ideals of the form $(\gamma^{1-\tau})$. The claim follows.

Let $\mathfrak{a}$ be a representative of a class in the 2-primary part of Cl_{k_m}. We will now see that there exists a generator γ of the principal ideal $\mathfrak{a}^{W\theta'}$ for which $\gamma^{1-\sigma^n}$ is a square in $k_m^\times$ for all n. Since $(1-\tau)$ is a factor of θ' in $\mathbb{Q}[G]$, we have

$$W\theta' = \frac{W}{2}(1-\tau)\theta' = \left(\sum_{i=0}^{2^{m-1}-1} \sigma^i\right)(1-\sigma)\frac{W}{2}\theta'.$$

Therefore, if $\tilde{\gamma}$ is an element of $k_m^\times$ such that

$$\mathfrak{a}^{(1-\sigma)\frac{W}{2}\theta'} = \left(\tilde{\gamma}^{1-\tau}\right),$$

then

$$\mathfrak{a}^{W\theta'} = \left(\tilde{\gamma}^{\left(\sum_{i=0}^{2^{m-1}-1}\sigma^i\right)(1-\tau)}\right).$$

Set

$$\gamma = \tilde{\gamma}^{\left(\sum_{i=0}^{2^{m-1}-1}\sigma^i\right)(1-\tau)}.$$

Then

$$\gamma^{1-\sigma} = \tilde{\gamma}^{2(1-\tau)}.$$

Since for $1 \leq n \leq m-1$,

$$1-\sigma^n = (1-\sigma)\sum_{i=0}^{n-1}\sigma^i,$$

it follows that

$$\gamma^{1-\sigma^n} \in k_m^{\times 2}. \tag{5.3}$$

Now $k_m\left(\sqrt{\gamma}\right)/k_m$ is a Kummer extension. From Section 2.5, the subgroup Δ of $k_m^\times$ generated by γ and $k_m^{\times 2}$ corresponds to this extension through Kummer theory. The inclusion (5.3) shows that γ^σ is also in Δ. Hence, $k_m\left(\sqrt{\gamma}\right)/k_0$ is a Galois extension by Proposition 2.7.2.

Next, let $\tilde{G} = \mathrm{Gal}\left(k_m\left(\sqrt{\gamma}\right)/k_0\right)$ and $H = \mathrm{Gal}\left(k_m\left(\sqrt{\gamma}\right)/k_m\right)$. We will show that $\tilde{G}$ is a central extension of H by G. The argument is that of the second half of Lemma A.1.4 in the appendix of [10]. Let η be a square root of γ. Let n be an integer such that $1 \leq n \leq m-1$, and let $\tilde{\sigma}$ be an element of $\tilde{G}$ that restricts to the element σ in G. The inclusion (5.3) shows that there exists ξ in $k_m^\times$ such that

$$\eta^{1-\tilde{\sigma}^n} = \xi.$$

If h is in H, then

$$\begin{aligned}\eta^{h\tilde{\sigma}^n-\tilde{\sigma}^n h} &= \eta^{(1-\tilde{\sigma}^n)h}\eta^{h(\tilde{\sigma}^n-1)} \\ &= \xi^h\left(\pm\eta\right)^{-(1-\tilde{\sigma}^n)} \\ &= \xi\xi^{-1} \\ &= 1.\end{aligned}$$

Since the elements $\tilde{\sigma}^n$ for $0 \leq n \leq m-1$ form a complete set of coset representatives for $\tilde{G}/H$, it follows that $\tilde{G}$ is a central extension of H by G. Finally, $\tilde{G}$ is generated by H and the lifts $\tilde{\sigma}^n$. Since these lifts all commute with each other, $\tilde{G}$ is Abelian. □

Remark. As stated, the theorem applies to the minimal set $S^{\min}$. If there are very many prime ideals that ramify in k_m/k_0 or if unramified prime ideals are included in S_0, the theorem can be refined. However, a precise statement of this refinement would be somewhat inelegant.

Corollary 5.1.3. *The Brumer-Stark conjecture is true for* 2*-power degree cyclic extensions of real quadratic fields.*

Proof. This follows immediately from the above theorem and the following result (Corollary 1.4 in [18]):

Proposition 5.1.4 (Greither-Roblot-Tangedal)**.** *Let p be an odd prime number. Let K/F be an Abelian extension of number fields with K CM and F totally real. Assume that the degree $[K\colon F]$ is relatively prime to p. Then (BS_p) is true if $F/\mathbb{Q}$ is Abelian and the p-part of $\mathrm{Gal}(F/\mathbb{Q})$ is cyclic.* □

Remark. Combining Stickelberger's theorem [59, §3(b)] with the results in [59, §3(c)], [48], and the above corollary, the Brumer-Stark conjecture has now been completely proved for all Abelian number field extensions K/k with $[K:\mathbb{Q}] < 12$.

Theorem 5.1.5. *Let k_m/k_0 be a cyclic extension of number fields of degree 2^m with Galois group G. If p is an odd prime number and the p-primary part of $\mathrm{Q}_{2^m}(k_m/k_0)$ has an affirmative answer, then the p-primary part of the Brumer-Stark conjecture holds for k_m/k_0.*

Remark. Under the assumptions of this theorem, the p-primary part of μ is G-cohomologically trivial because its order is relatively prime to the order of G. Thus, Proposition 3.4.3 shows that the p-primary part of the Brumer-Stark conjecture in this case follows from the p-primary part of Brumer's conjecture. This, in turn, often follows from the work of Wiles (see [64, Theorem 3] and [18, Proposition 1.3]). It is possible that the question $\mathrm{Q}_{2^m}(k_m/k_0)$ could be resolved with these techniques (although the any "trivial zeroes" involved with the descent to the finite level would present a major problem). If it could instead be resolved working only at the finite level, this would have the advantage that the proofs would remain global, and hopefully could be accomplished without resort to machinery like the main conjecture of Iwasawa theory.

Proof. (BS) was proved for quadratic extensions by Tate ([59, §3, case (c)]). We therefore assume that k_0 is totally real, k_m is totally complex, and $m \geq 2$. Let $W = |\mu|$ be the cardinality of the group of roots of unity in k_m, and write $W = p^e W'$, where $(p, W') = 1$. Let $S_0^{\min}$ be the set of places of k_0 comprising the Archimedean places and the prime ideals that ramify in k_m/k_0. We will denote the L-function evaluator $\theta_{k_m/k_0, S_0^{\min}}$ simply by θ. According to the statement of (BS_p) in Subsection 3.4.1 and the above lemma, we must show that $W\theta$ annihilates the p-primary part of Cl_{k_m}, and that each principal ideal created in this manner is generated by a p^e-Abelian anti-unit.

Let notation be as in Theorem 5.1.2. Property 2 of L-function evaluators in Section 3.1 shows that we can write

$$W\theta = \sum_{i=0}^{2^{m-1}-1} a_i \sigma^i (1 - \tau).$$

When this product is expanded, the coefficient of σ^i for $0 \leq i \leq 2^{m-1} - 1$ is a_i. Theorem 3.2.4 then shows that each a_i is an integer. Set $\alpha = \sum_{i=0}^{2^{m-1}-1} a_i \sigma^i$. We will now see that α annihilates the p-primary part of Cl_{k_m}.

Lemma 2.4.1 shows that the factor of $\mathrm{Fit}_{\mathcal{O}} \mu$ supported above primes dividing p has the form $\tilde{\mathfrak{P}}^e$ for some prime ideal $\tilde{\mathfrak{P}}$ of $\mathcal{O}$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}$ dividing p, and set $\delta = 0$ if $\mathfrak{P} = \tilde{\mathfrak{P}}$ and $\delta = e$ otherwise. Let $v_{\mathfrak{P}}$ denote the normalized

valuation on $\mathcal{O}$ induced by $\mathfrak{P}$. By assumption, the p-primary part of the question $\mathrm{Q}_{2^m}\left(k_m/k_0\right)$ has an affirmative answer. It implies that

$$v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mu\right)\chi\left(\theta\right)\right) = v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right)\right),$$

where μ and Coker have the $\mathcal{O}$-module structures provided by χ. Hence,

$$v_{\mathfrak{P}}\left(\chi\left(\alpha\right)\right) = v_{\mathfrak{P}}\left(\chi\left(\theta\right)\right) + e = v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right)\right) + \delta. \tag{5.4}$$

The algebraic integer $\chi\left(\alpha\right)$ is thus divisible by the $\mathcal{O}$-Fitting ideal of the p-primary part of Coker. As α acts on this $\mathcal{O}$-module as $\chi\left(\alpha\right)$, property 2 of Fitting ideals shows that α annihilates the p-primary part of Coker.

Now let $\mathfrak{a}$ be an ideal in the p-primary part of Cl_{k_m}. Since α annihilates the class of $\mathfrak{a}$ in Coker, we have

$$\mathfrak{a}^{\alpha} = \mathfrak{b}\mathfrak{c}\left(\gamma\right),$$

where $\mathfrak{b}$ is an ideal of k_m with support above the prime ideals in S, $\mathfrak{c}$ is the lift of a nonzero ideal from k_m^+, and γ is an element of $k_m^{\times}$. Since no prime of S^+ splits in k_n, it follows that $\mathfrak{b}^{\tau} = \mathfrak{b}$. Thus,

$$\mathfrak{a}^{W\theta} = \left(\mathfrak{b}\mathfrak{c}\left(\gamma\right)\right)^{1-\tau} = \left(\gamma^{1-\tau}\right).$$

We have found that $W\theta$ annihilates the p-primary part of Cl_{k_m}, and in fact, the principal ideals produced thereby are generated by anti-units. It remains to be shown that these anti-units can be chosen to be p-Abelian. Since this is trivial if $(p, W) = 1$, we assume that p divides W.

Let $N\sigma$ be an integer such that

$$\sigma(\zeta) = \zeta^{N\sigma}$$

for all p-power roots of unity in k_m. Since p divides W and k_0 is totally real, $N\sigma \not\equiv 1 \bmod p$. In addition, since $\sigma^{2^m} = 1$, we have

$$\left(N\sigma\right)^{2^m} \equiv 1 \pmod{p^e}.$$

If necessary, we adjust $N\sigma$ by p^e to ensure that p^e is the exact power of p dividing $\left(N\sigma\right)^{2^m} - 1$. Let P_{anti} denote the group of nonzero principal ideals of k_m generated by anti-units. We will now prove the claim that $(N\sigma - \sigma)\frac{W}{p^e}\theta$ is in $\mathbb{Z}[G]$ and

$$\mathfrak{a}^{(N\sigma-\sigma)\frac{W}{p^e}\theta} \in P_{\mathrm{anti}},$$

for any ideal $\mathfrak{a}$ in the p-primary part of Cl_{k_m}.

First, let $\mu^{(p)}$ be the p-primary part of μ. Then $N\sigma - \zeta_{2^m}$ is contained in

$$\mathrm{Fit}_{\mathcal{O}}\, \mu^{(p)} = \tilde{\mathfrak{P}}^e.$$

Using (5.4), we find that

$$v_{\mathfrak{P}}\left(\chi\left((N\sigma - \sigma)W\theta\right)\right) \geq v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}\right)\right) + e \tag{5.5}$$

for all prime ideals $\mathfrak{P}$ of $\mathcal{O}$ dividing p. Thus, p^e divides $\chi\left((N\sigma - \sigma)W\theta\right)$ in $\mathcal{O}$. If we write

$$(N\sigma - \sigma)W\theta = \sum_{i=0}^{2^{m-1}-1} a_i'\sigma^i(1-\tau),$$

then p^e divides $2\sum_{i=0}^{2^{m-1}-1} a_i'\zeta_{2^m}$. The numbers ζ_{2^m} form an integral basis for $\mathcal{O}$, so the integers a_i' are divisible by p^e. It follows that

$$(N\sigma - \sigma)\frac{W}{p^e}\theta \in \mathbb{Z}[G], \tag{5.6}$$

which is the first part of the claim.

Next, let $\mathfrak{a}$ be an ideal representing a class in the p-primary part of Cl_{k_m}. Let

$$c = \frac{(N\sigma)^{2^m} - 1}{p^e}.$$

Because c is relatively prime to p, we can find an ideal $\mathfrak{a}'$ in the p-primary part of Cl_{k_m} and an element γ' in $k_m^\times$ such that $\mathfrak{a}(\gamma') = \mathfrak{a}'^c$. The inequality (5.5) shows that $\sum_{i=0}^{2^{m-1}-1} \frac{a_i'}{p^e}\sigma^i$ annihilates the p-primary part of Coker. The argument in the paragraph following equation (5.4) then shows that there is an element $\tilde{\gamma}$ in $k_m^\times$ such that

$$\mathfrak{a}'^{(N\sigma-\sigma)\frac{W}{p^e}\theta} = \left(\tilde{\gamma}^{1-\tau}\right).$$

Applying $\beta = \sum_{i=0}^{2^m-1} (N\sigma)^i\, \sigma^{2^m-1-i}$ to both sides, we find that

$$\mathfrak{a}'^{\left((N\sigma)^{2^m}-1\right)\frac{W}{p^e}\theta} = \mathfrak{a}^{W\theta}\left(\gamma'^{W\theta}\right) = \left(\tilde{\gamma}^{\beta(1-\tau)}\right).$$

We will now see that the generator $\gamma = \tilde{\gamma}^{\beta(1-\tau)}\gamma'^{-W\theta}$ for the principal ideal $\mathfrak{a}^{W\theta}$ is p^e-Abelian (we can once again use property 2 of L-function evaluators to verify

that it is an anti-unit). First, for any n such that $1 \leq n \leq 2^m - 1$, $(N\sigma)^n - \sigma^n$ annihilates $\mu^{(p)}$ and

$$\begin{aligned}\gamma^{(N\sigma)^n-\sigma^n} &= \tilde{\gamma}^{\beta(1-\tau)(N\sigma-\sigma)\sum_{i=0}^{n-1}(N\sigma)^i\sigma^{n-1-i}}\gamma'^{-W\theta(N\sigma-\sigma)\sum_{i=0}^{n-1}(N\sigma)^i\sigma^{n-1-i}} \\ &= \tilde{\gamma}^{\left((N\sigma)^{2^m}-1\right)(1-\tau)\sum_{i=0}^{n-1}(N\sigma)^i\sigma^{n-1-i}}\gamma'^{-W\theta(N\sigma-\sigma)\sum_{i=0}^{n-1}(N\sigma)^i\sigma^{n-1-i}}.\end{aligned}$$

The first factor is in $k_m^{\times p^e}$ since p^e divides $(N\sigma)^{2^m} - 1$, and equation (5.6) shows that the second factor is in $k_m^{\times p^e}$. Therefore,

$$\gamma^{(N\sigma)^n-\sigma^n} \in k_m^{\times p^e} \tag{5.7}$$

for $1 \leq n \leq 2^m - 1$.

Now $k_m\left(\sqrt[p^e]{\gamma}\right)/k_m$ isa Kummer extension. From Section 2.5, the subgroup Δ of $k_m^\times$ generated by γ and $k_m^{\times p^e}$ corresponds to this extension through Kummer theory. The inclusion (5.7) shows that γ^{σ^n} is also in Δ for $1 \leq n \leq 2^m - 1$. Hence, $k_m\left(\sqrt[p^e]{\gamma}\right)/k_0$ is a Galois extension by Proposition 2.7.2.

Next, let $\tilde{G} = \mathrm{Gal}\left(k_m\left(\sqrt[p^e]{\gamma}\right)/k_0\right)$ and $H = \mathrm{Gal}\left(k_m\left(\sqrt[p^e]{\gamma}\right)/k_m\right)$. We will show that $\tilde{G}$ is a central extension of H by G. The argument is that of the second half of Lemma A.1.4 in the appendix of [10]. Let η be a p^eth root of γ. Let n be an integer such that $1 \leq n \leq 2m - 1$, and let $\tilde{\sigma}$ be an element of $\tilde{G}$ that restricts to the element σ in G. The inclusion (5.7) shows that there exists ξ in $k_m^\times$ such that

$$\eta^{(N\sigma)^n-\tilde{\sigma}^n} = \xi.$$

Let h be in H, and let ζ be the p^eth root of unity such that $h\eta = \zeta\eta$. Then

$$\begin{aligned}\eta^{h\tilde{\sigma}^n-\tilde{\sigma}^nh} &= \eta^{((N\sigma)^n-\tilde{\sigma}^n)h}\eta^{h(\tilde{\sigma}^n-(N\sigma)^n)} \\ &= \xi^h\left(\zeta\eta\right)^{-((N\sigma)^n-\tilde{\sigma}^n)} \\ &= \xi\xi^{-1} \\ &= 1.\end{aligned}$$

Since the elements $\tilde{\sigma}^n$ for $0 \leq n \leq 2^m - 1$ form a complete set of coset representatives for $\tilde{G}/H$, it follows that $\tilde{G}$ is a central extension of H by G. Finally, $\tilde{G}$ is generated by H and the lifts $\tilde{\sigma}^n$. Since these lifts all commute with each other, $\tilde{G}$ is Abelian. □

Corollary 5.1.6. *Let $k' \subset k_0 \subset k_m$ be a tower of fields such that k_m/k_0 is cyclic of degree 2^m and k_m/k' and k_0/k' are Galois. Assume that the map*

$$\phi\colon \operatorname{Gal}(k_0/k') \to \operatorname{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q})$$

from Section 4.4 is surjective. Then the Brumer-Stark conjecture holds for the extension k_m/k_0.

This follows directly from the above theorem and Corollary 4.4.3. (Note that the minimal set $S^{\min}$ of places of k_0 is stable under the action of $\operatorname{Gal}(k_0/k')$ on the ideal group of k_0, which is a necessary condition to apply Corollary 4.4.3). This corollary generalizes a result of Tate ([59, §3, case (e)]).

5.2 The component Brumer-Stark conjecture for extensions of degree $2^m p^n$

In this section, we will prove results similar to the local parts of the Brumer-Stark conjecture, but for the individual components of the L-function evaluator. We resume the notation of Section 4.6. In particular, p is an odd prime number, m and n are positive integers, and K_n/k_0 is a cyclic extension of number fields of degree $2^m p^n$ with Galois group G. We assume that k_0 is totally real and K_n is totally complex; the Brumer-Stark conjecture is trivial otherwise. For $0 \leq r \leq n$, let k_r and K_r be the unique extensions fields of k_0 contained in K_n with $[k_r\colon k_0] = p^r$ and $[K_r\colon k_0] = 2^m p^r$. The fields k_r are all totally real and the fields K_r are all CM fields. Let K_r^+ denote the maximal totally real subfield of K_r. Let S_0 be the set of places in k_0 consisting of the Archimedean places and the prime ideals that ramify in K_n/k_0. We will abuse notation as follows: for $0 \leq r \leq n$, if k is a field between k_r and K_r, we will denote the set of places in k lying above the places in S_0 by S_r. We will also denote the set of places in k_r lying above places in S_0 that do not split completely in K_0/k_0 by S_r^{ns}. We will denote the L-function evaluator $\theta_{K_n/k_0,S_0}$ simply by θ. We let $W_r = |\mu_r|$ denote the cardinality of the group of roots of unity in K_r, and set $q = \frac{W_n}{W_{n-1}}$. We let $\mathfrak{C}$ be the equivalence class in $\widehat{G}$ consisting of the characters of order $2^m p^n$. We set $\mathcal{O} = \mathbb{Z}[\zeta_{2^m p^n}]$.

5.2.1 Local results at primes other than 2 and p

This subsection is devoted to proving the following proposition:

Proposition 5.2.1. *Let p' be a prime number, different from 2 and p, and such that the p'-primary part of $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer. Let $\mathrm{Cl}_{p'}$ be the p'-primary part of the class group of K_n. Then*

$$pq\theta_{\mathfrak{C}} \in \mathrm{Ann}_{\mathbb{Z}[G]} \mathrm{Cl}_{p'}.$$

Let p'^t be the exact power of p' dividing W_n. Then the principal ideals produced by applying $pW_n\theta_{\mathfrak{C}}$ to ideals representing classes in $\mathrm{Cl}_{p'}$ are generated by p'^t-Abelian anti-units. Furthemore, when $W_n\theta_{\mathfrak{C}}$ is integral,

$$W_n\theta_{\mathfrak{C}} \in \mathrm{Ann}_{\mathbb{Z}[G]} \mathrm{Cl}_{p'},$$

and the principal ideals produced by applying $W_n\theta_{\mathfrak{C}}$ to ideals representing classes in $\mathrm{Cl}_{p'}$ are generated by p'^t-Abelian anti-units.

Proof. Let σ generate $H = \mathrm{Gal}(K_n/K_0)$, let σ' generate $H' = \mathrm{Gal}(K_n/k_n)$, and let $\tau = \sigma'^{2^{m-1}}$ denote complex conjugation. Let χ generate $\widehat{G}$. For $1 \leq r \leq n$, let ζ_{p^r} be the primitive p^rth root of unity such that

$$\chi^{2^m}\left(\sigma^{p^{n-r}}\right) = \zeta_{p^r}.$$

Let ζ_{2^m} be the primitive 2^mth root of unity such that

$$\chi^{p^n}(\sigma') = \zeta_{2^m}.$$

Let $\tilde{\mu}$ be the quotient of the group of roots of unity in K_n by the group of roots of unity in K_{n-1}. For $0 \leq r \leq n$, let K_n^+ be the maximal totally real subfield of K_n. Let Coker_{n-1} be the cokernel of the map

$$\mathrm{Cl}_{K_{n-1}^+, S_{n-1}^{\mathrm{ns}}} \to \mathrm{Cl}_{K_{n-1}, S_{n-1}^{\mathrm{ns}}},$$

and let Coker_n be the cokernel of the map

$$\mathrm{Cl}_{K_n^+, S_n^{\mathrm{ns}}} \to \mathrm{Cl}_{K_n, S_n^{\mathrm{ns}}}.$$

Finally, let Ker denote the kernel of the norm map $\mathrm{N}\colon \mathrm{Coker}_n \to \mathrm{Coker}_{n-1}$.

We write

$$\theta_{\mathfrak{C}} = \left(1 - \sigma^{p^{n-1}}\right) \overline{\theta}_{\mathfrak{C}},$$

with $\overline{\theta}_{\mathfrak{C}}$ defined by equations (4.35) and (4.36). These equations and Proposition 4.6.3 show that

$$pq\overline{\theta}_{\mathfrak{C}} \in \mathbb{Z}\left[G\right].$$

Property 4 of components of L-function evaluators shows that

$$(1+\tau)\overline{\theta}_{\mathfrak{C}} = 0.$$

Hence, considering this as an equality between elements of the group algebra $\mathbb{Q}\left[H\right]\left[H'\right]$, we can write

$$pq\overline{\theta}_{\mathfrak{C}} = \sum_{i=0}^{2^{m-1}-1} a_i \sigma'^i (1-\tau) \tag{5.8}$$

for some coefficients a_i in $\mathbb{Z}[H]$. Set

$$\alpha = \sum_{i=0}^{2^{m-1}-1} a_i \sigma'^i.$$

We will now see that α annihilates the p'-primary part of Ker.

Lemma 2.4.1 shows that the factor of $\mathrm{Fit}_{\mathcal{O}} \tilde{\mu}$ supported above primes dividing p' has the form $\tilde{\mathfrak{P}}^e$, where $\tilde{\mathfrak{P}}$ is a prime ideal of $\mathcal{O}$ and p'^e is the exact power of p' dividing q. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}$ dividing p', and let $\delta_{\tilde{\mathfrak{P}}} = 0$ if $\mathfrak{P} = \tilde{\mathfrak{P}}$ and $\delta_{\tilde{\mathfrak{P}}} = e$ otherwise. Let $v_{\mathfrak{P}}$ denote the normalized valuation on $\mathcal{O}$ induced by $\mathfrak{P}$. By assumption, the p'-primary part of the question $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ has an affirmative answer. It implies that

$$v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\tilde{\mu}\right)\chi\left(\theta_{\mathfrak{C}}\right)\right) = v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right), \tag{5.9}$$

where $\tilde{\mu}$ and Ker have the $\mathcal{O}$-module structures provided by χ (recall that p' is not 2 or p). Hence,

$$\begin{aligned} v_{\mathfrak{P}}\left(\chi\left(\alpha\right)\right) &= v_{\mathfrak{P}}\left(\chi\left(\theta_{\mathfrak{C}}\right)\right) + v_{\mathfrak{P}}(q) \\ &= v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right) + \delta_{\tilde{\mathfrak{P}}}. \end{aligned}$$

The algebraic integer $\chi(\alpha)$ is thus divisible by the $\mathcal{O}$-Fitting ideal of the p'-primary part of Ker. As α acts on this $\mathcal{O}$-module as $\chi(\alpha)$, property 2 of Fitting ideals shows that α annihilates the p'-primary part of Ker.

Next, let $\mathfrak{a}$ be an ideal representing a class in $\mathrm{Cl}_{p'}$. Then

$$\mathfrak{a}^{pq\theta_{\mathfrak{C}}} = \mathfrak{a}^{\left(1-\sigma^{p^{n-1}}\right)\alpha(1-\tau)}.$$

The ideal $\mathfrak{a}^{\left(1-\sigma^{p^{n-1}}\right)}$ represents a class in Ker. Therefore, our previous work shows that $\mathfrak{a}^{\left(1-\sigma^{p^{n-1}}\right)\alpha}$ represents the trivial class in Ker, a submodule of Coker_n. By the definition of Coker_n, we have

$$\mathfrak{a}^{\left(1-\sigma^{p^{n-1}}\right)\alpha} = \mathfrak{b}\mathfrak{c}(\gamma),$$

where $\mathfrak{b}$ is an ideal of k_m with support above the prime ideals in S_n^{ns}, $\mathfrak{c}$ is the lift of a nonzero ideal from K_n^+, and γ is an element of $K_n^\times$. Since the prime ideals in S_n^{ns} do not split completely in K_n/k_n, they do not split in K_n/K_n^+. It follows that $\mathfrak{b}^\tau = \mathfrak{b}$. Thus,

$$\mathfrak{a}^{pq\theta_{\mathfrak{C}}} = (\mathfrak{b}\mathfrak{c}(\gamma))^{1-\tau} = \left(\gamma^{1-\tau}\right). \tag{5.10}$$

We have found that $pq\theta_{\mathfrak{C}}$ annihilates $\mathrm{Cl}_{p'}$, and in fact, the principal ideals produced thereby are generated by anti-units. It remains to be shown that when $pW_n\theta_{\mathfrak{C}}$ is applied to $\mathfrak{a}$ instead, the anti-units can be chosen to be p'^t-Abelian. We assume that p' divides W_n, the p'^t-Abelian condition being trivial otherwise.

Choose a generator g of G. Let $\mu_{p'}$ be the group of p'-power roots of unity in K_n, and let Ng be an integer such that

$$\zeta^g = \zeta^{Ng}$$

for all ζ in $\mu_{p'}$. Since $g^{2^m p^n} = 1$, we have

$$(Ng)^{2^m p^n} \equiv 1 \pmod{p'^t}.$$

If necessary, we adjust Ng by p'^t to ensure that p'^t is the exact power of p' dividing $(Ng)^{2^m p^n} - 1$. Let P_{anti} denote the group of nonzero principal ideals of K_n generated by anti-units. We will first prove the claim that $(Ng-g)\frac{pW_n}{p'^t}\theta_{\mathfrak{C}}$ is in $\mathbb{Z}[G]$ and

$$\mathfrak{a}^{(Ng-g)\frac{pW_n}{p'^t}\theta_{\mathfrak{C}}} \in P_{\mathrm{anti}}$$

for any ideal $\mathfrak{a}$ representing a class in $\mathrm{Cl}_{p'}$.

As $Ng - g$ annihilates $\tilde{\mu}$, $\chi(Ng - g)$ is contained in

$$\mathrm{Fit}_{\mathcal{O}} \tilde{\mu}_{p'} = \tilde{\mathfrak{P}}^e.$$

Using property 4 of components of L-function evaluators, we can write

$$(Ng - g)\, pW_n\theta_{\mathfrak{C}} = \left(1 - \sigma^{p^{n-1}}\right) \sum_{i=0}^{(p-1)p^{n-1}-1} a_i\sigma^i,$$

where the coefficients a_i are elements of $\mathbb{Z}[H']$ (see equations (4.35) and (4.36) for the general idea). Since $1 + \tau$ annihilates $\theta_{\mathfrak{C}}$, we can further write

$$a_i = \sum_{j=0}^{2^{m-1}-1} b_{ij}\sigma'^j(1 - \tau),$$

for $0 \le i \le (p-1)p^{n-1} - 1$ (begin by observing that this is true for the coefficients a_i for $(p-1)p^{n-1} < i < p^{n-1} - 1$; then work backward through the smaller values of i). The coefficients b_{ij} are integers, since the a_i s are in $\mathbb{Z}[H]$. Then (5.9) shows that

$$\begin{aligned} v_{\mathfrak{P}}\left(\sum_{i=0}^{(p-1)p^{n-1}-1} \sum_{j=0}^{2^{m-1}-1} b_{ij}\zeta_{2^m}^j\zeta_{p^n}^i\right) &= v_{\mathfrak{P}}\left((Ng - g)\, W_n\theta_{\mathfrak{C}}\right) \\ &\ge v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right) + v_{\mathfrak{P}}\left(W_n\right) \\ &= v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right) + v_{\mathfrak{P}}\left(p'^t\right) \end{aligned} \tag{5.11}$$

for all prime ideals $\mathfrak{P}$ of $\mathcal{O}$ dividing p'. Thus, p'^t divides the algebraic integer

$$\sum_{i=0}^{(p-1)p^{n-1}-1} \sum_{j=0}^{2^{m-1}-1} b_{ij}\zeta_{2^m}^j\zeta_{p^n}^i$$

in $\mathcal{O}$. The numbers $\zeta_{2^m}^j\zeta_{p^n}^i$ for $0 \le j \le 2^{m-1} - 1$ and $0 \le i \le (p-1)p^{n-1} - 1$ form an integral basis for $\mathcal{O}$, so the integers b_{ij} are divisible by p'^t. It follows that

$$(Ng - g)\frac{pW_n}{p'^t}\theta_{\mathfrak{C}} \in \mathbb{Z}[G], \tag{5.12}$$

which is the first part of the claim.

Next, let $\mathfrak{a}$ be an ideal representing a class in $\mathrm{Cl}_{p'}$. Let

$$c = \frac{(Ng)^{2^m p^n} - 1}{p'^t}.$$

Because c is relatively prime to p', we can find an ideal $\mathfrak{a}'$ in $\mathrm{Cl}_{p'}$ and an element γ' in $K_n^\times$ such that $\mathfrak{a}(\gamma') = \mathfrak{a}'^c$. The inequality (5.11) shows that

$$\sum_{i=0}^{(p-1)p^{n-1}-1} \sum_{j=0}^{2^{m-1}-1} \frac{b_{ij}}{p'^t} \sigma^i \sigma'^j$$

annihilates the p'-primary part of Ker. The argument used to prove (5.10) then shows that there is an element $\tilde{\gamma}$ in $K_n^\times$ such that

$$\mathfrak{a}'^{(Ng-g)\frac{pW_n}{p'^t}\theta_{\mathfrak{C}}} = \left(\tilde{\gamma}^{1-\tau}\right).$$

Applying $\beta = \sum_{i=0}^{2^m p^n - 1} (Ng)^i g^{2^m p^n - 1 - i}$ to both sides, we find that

$$\mathfrak{a}'^{\left((Ng)^{2^m p^n}-1\right)\frac{pW_n}{p'^t}\theta_{\mathfrak{C}}} = \mathfrak{a}^{pW_n\theta_{\mathfrak{C}}} \left(\gamma'^{pW_n\theta_{\mathfrak{C}}}\right) = \left(\tilde{\gamma}^{\beta(1-\tau)}\right).$$

We will now see that the generator $\gamma = \tilde{\gamma}^{\beta(1-\tau)}\gamma'^{-pW_n\theta_{\mathfrak{C}}}$ for the principal ideal $\mathfrak{a}^{pW_n\theta_{\mathfrak{C}}}$ is p'^t-Abelian (property 4 of components of L-function evaluators shows that it is an anti-unit). First, for any r such that $1 \le r \le 2^m p^n - 1$, $(Ng)^r - g^r$ annihilates $\mu_{p'}$ and

$$\begin{aligned}
\gamma^{(Ng)^r - g^r} &= \tilde{\gamma}^{\beta(1-\tau)(Ng-g)\sum_{i=0}^{r-1}(Ng)^i g^{r-1-i}} \gamma'^{-pW_n\theta_{\mathfrak{C}}(Ng-g)\sum_{i=0}^{r-1}(Ng)^i g^{r-1-i}} \\
&= \tilde{\gamma}^{\left((Ng)^{2^m p^n}-1\right)(1-\tau)\sum_{i=0}^{r-1}(Ng)^i g^{r-1-i}} \gamma'^{-pW_n\theta_{\mathfrak{C}}(Ng-g)\sum_{i=0}^{r-1}(Ng)^i g^{r-1-i}}.
\end{aligned}$$

The first factor is in $K_n^{\times p'^t}$ since p'^t divides $(Ng)^{2^m p^n} - 1$, and equation (5.12) shows that the second factor is in $K_n^{\times p'^t}$. Therefore,

$$\gamma^{(Ng)^r - g^r} \in K_n^{\times p'^t} \tag{5.13}$$

for $1 \le r \le 2^m p^n - 1$.

Now $K_n\left(\sqrt[p'^t]{\gamma}\right)/K_n$ is a Kummer extension. From Section 2.5, the subgroup Δ of $K_n^\times$ generated by γ and $K_n^{\times p'^t}$ corresponds to this extension through Kummer theory. The inclusion (5.13) shows that γ^{g^r} is also in Δ for $1 \le r \le 2^m p^n - 1$. Hence, $K_n\left(\sqrt[p'^t]{\gamma}\right)/k_0$ is a Galois extension by Proposition 2.7.2.

Next, let $\tilde{G} = \mathrm{Gal}\left(K_n\left(\sqrt[p'^t]{\gamma}\right)/k_0\right)$ and $H = \mathrm{Gal}\left(K_n\left(\sqrt[p'^t]{\gamma}\right)/K_n\right)$. We will show that $\tilde{G}$ is a central extension of H by G. The argument is that of the second half of Lemma A.1.4 in the appendix of [10]. Let η be a p'^tth root of γ. Let r be an integer such that $1 \leq r \leq 2^m p^n - 1$, and let $\tilde{g}$ be an element of $\tilde{G}$ that restricts to the element g in G. The inclusion (5.13) shows that there exists ξ in $K_n^\times$ such that

$$\eta^{(Ng)^r - \tilde{g}^r} = \xi.$$

Let h be in H, and let ζ be the p'^tth root of unity such that $h\eta = \zeta\eta$. Then

$$\begin{aligned}
\eta^{h\tilde{g}^r - \tilde{g}^r h} &= \eta^{((Ng)^r - \tilde{g}^r)h} \eta^{h(\tilde{g}^r - (Ng)^r)} \\
&= \xi^h \left(\zeta\eta\right)^{-((Ng)^r - \tilde{g}^r)} \\
&= \xi\xi^{-1} \\
&= 1.
\end{aligned}$$

Since the elements $\tilde{g}^r$ for $0 \leq r \leq 2^m p^n - 1$ form a complete set of coset representatives for $\tilde{G}/H$, it follows that $\tilde{G}$ is a central extension of H by G. Finally, $\tilde{G}$ is generated by H and the lifts $\tilde{g}^n$. Since these lifts all commute with each other, $\tilde{G}$ is Abelian.

Now assume that $W_n\theta_{\mathfrak{C}}$ is integral. If $\mathfrak{a}$ is in $\mathrm{Cl}_{p'}$, then we can find an ideal $\mathfrak{a}'$ such that $\mathfrak{a}'^p$ is in the same ideal class as $\mathfrak{a}$. Since $\mathfrak{a}'^{pW_n\theta_{\mathfrak{C}}}$ is principal, generated by a p'^t-Abelian anti-unit, $\mathfrak{a}^{W_n\theta_{\mathfrak{C}}}$ is as well (use the argument in the paragraph containing equation (5.13) to handle the quotient of $\mathfrak{a}'^p$ and $\mathfrak{a}$, a principal ideal). □

5.2.2 The 2-primary part

We will now prove a similar result for the prime 2, but with a strengthened annihilation statement.

Proposition 5.2.2. *Let* Cl_2 *be the* 2*-primary part of the class group of* K_n*. If the* 2*-primary part of* $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ *has an affirmative answer, then*

$$pq\theta_{\mathfrak{C}} \in 2^{[k_0:\,\mathbb{Q}]-1}\mathbb{Z}\left[G\right].$$

Furthermore,

$$\frac{pq}{2^{[k_0\colon \mathbb{Q}]-1}}\theta_{\mathfrak{C}} \in \operatorname{Ann}_{\mathbb{Z}[G]} \operatorname{Cl}_2.$$

Proof. We continue with the same notation. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}$ dividing 2. Let $\tilde{S}_1$ be the set of places in K_0 lying above places in S_0 that split completely in k_n/k_0. By assumption, the 2-primary part of the question $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer. It implies that

$$v_{\mathfrak{P}}(\chi(\theta_{\mathfrak{C}})) = v_{\mathfrak{P}}(\operatorname{Fit}_{\mathcal{O}}(\mathrm{Ker})) + \left|\tilde{S}_1\right|,$$

where Ker has the $\mathcal{O}$-module structure provided by χ (note that $|\tilde{\mu}| = q$ is odd). We again write

$$pq\theta_{\mathfrak{C}} = pq\left(1-\sigma^{p^{n-1}}\right)\overline{\theta}_{\mathfrak{C}},$$

where $\overline{\theta}$ is defined by equations (4.35) and (4.36). We then factor further to obtain

$$pq\theta_{\mathfrak{C}} = \left(1-\sigma^{p^{n-1}}\right)\alpha(1-\tau),$$

with

$$\alpha = \sum_{i=0}^{(p-1)p^{n-1}-1}\ \sum_{j=0}^{2^{m-1}-1} a_i \sigma'^j \sigma^i,$$

where the coefficients a_i are integers. Then since $\tilde{S}_1$ contains $2^{m-1}[k_0\colon \mathbb{Q}]$ Archimedean places,

$$\begin{aligned} v_{\mathfrak{P}}(\chi(\alpha)) &= v_{\mathfrak{P}}(\chi(\theta_{\mathfrak{C}})) - v_{\mathfrak{P}}(2) \\ &= v_{\mathfrak{P}}(\operatorname{Fit}_{\mathcal{O}}(\mathrm{Ker})) + \left|\tilde{S}_1\right| - 2^{m-1} \\ &\geq 2^{m-1}([k_0\colon \mathbb{Q}]-1). \end{aligned} \tag{5.14}$$

The algebraic integer

$$\chi(\alpha) = \sum_{i=0}^{(p-1)p^{n-1}-1}\ \sum_{j=0}^{2^{m-1}-1} a_i \zeta_{2^m}^j \zeta_{p^n}^i$$

is thus divisible by $2^{[k_0\colon \mathbb{Q}]-1}$ in $\mathcal{O}$. Since the numbers $\zeta_{2^m}^j \zeta_{p^n}^i$ appearing in the above double sum form an integral basis for $\mathcal{O}$, each coefficient a_i is divisible by $2^{[k_0\colon \mathbb{Q}]-1}$. This proves the first statement of the proposition.

Returning to (5.14), we find that

$$v_{\mathfrak{P}}\left(\frac{\chi(\alpha)}{2^{[k_0\colon\mathbb{Q}]-1}}\right) \geq v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right).$$

It follows that the element

$$\frac{\alpha}{2^{[k_0\colon\mathbb{Q}]-1}} \in \mathbb{Z}\left[G\right]$$

annihilates Ker. The proof of (5.10) with α replaced by

$$\frac{\alpha}{2^{[k_0\colon\mathbb{Q}]-1}}$$

shows that

$$\frac{pq}{2^{[k_0\colon\mathbb{Q}]-1}}\theta_{\mathfrak{C}} \in \mathrm{Ann}_{\mathbb{Z}[G]}\,\mathrm{Cl}_2.$$

□

5.2.3 The p-primary part

In this subsection, we will prove three propositions with a similar flavor to, but weaker than, the propositions of the preceding subsections. Two of them concern annihilation of class groups, and the other concerns an Abelian condition like that in the Brumer-Stark conjecture. The method of proof of the Abelian condition is essentially that of Section 2 of [18], applied to our wider setting. We need two lemmas. The first is based on lemma 2.5 in [18], which was crucial for the authors' study of (BS_p) for degree $2p$ extensions.

Lemma 5.2.3. *Let K_n/k_0 be a cyclic extension of degree $2^m p^n$ as above, and let K_{n-1}/k_0 be the subextension of degree $2^m p^{n-1}$. Set $\mathcal{H} = \mathrm{Gal}\left(K_n/K_{n-1}\right)$. Let s be the number of prime ideals in k_n lying above places in S_0 (not necessarily the minimal possible set) that split completely in K_0/k_0 and ramify in k_n/k_0. Let A_{n-1} and A_n be the p-primary parts of Coker_{n-1} and Coker_n. Then*

$$\left|A_n^{\mathcal{H}}\right| = p^{2^{m-1}s}\left|A_{n-1}\right|,$$

where the superscript $\mathcal{H}$ indicates the submodule fixed by $\mathcal{H}$.

Proof. Lemma 2.5 in [18] shows that the above equation holds with $2^{m-1}s$ replaced by the number of prime ideals in K_{n-1}^{+} that split in K_{n-1} and ramify in K_n. (Recall that the p-primary parts of the cokernels are isomorphic to minus parts of the p-primary parts of the corresponding ideal class groups when p is odd.) Since K_{n-1}/k_{n-1} is cyclic, a prime ideal of K_{n-1}^{+} splits in K_{n-1} if and only if the prime ideal of k_{n-1} that it divides splits completely in K_{n-1}/k_{n-1}. Thus, the number of prime ideals in K_{n-1}^{+} that split in K_{n-1} and ramify in K_n is $2^{m-1}s$. □

Lemma 5.2.4. *Let notation be as in the previous lemma, and assume that $m = 1$. Let $\mathfrak{C}$ be the equivalence class of characters on $G = \mathrm{Gal}\,(K_n/k_0)$ of order $2p^n$. If $s \geq p^{n-1}$, then*

$$\theta_{\mathfrak{C}} \in \frac{1}{q}\mathbb{Z}[G].$$

Proof. If p divides q, then this result is part of Proposition 4.6.3. We thus assume that p does not divide q. Let Ker_p be the p-primary part of Ker. By the previous lemma and the assumption that $s \geq p^{n-1}$,

$$|\mathrm{Ker}_p| = \frac{\left|A_n^{\mathcal{H}}\right|}{|A_{n-1}|} \geq p^{p^{n-1}}. \tag{5.15}$$

We may assume that S_0 is the set of places of k_0 consisting of the Archimedean places and the prime ideals that ramify in K_n/k_0. It follows that the set $\tilde{S}_2$ appearing in the question $\mathrm{Q}_{2^m p^n}\,(K_n/k_0)$ is empty.

Set $\lambda = (1 - \zeta_{p^n})$. Since (λ) is the only prime ideal dividing p in $\mathbb{Q}\,(\zeta_{p^n})$, the p-primary part of $\mathrm{Q}_{2^m p^n}\,(K_n/k_0)$ has an affirmative answer. Thus, the (λ)-valuations of both sides of the equation

$$\mathrm{Fit}_{\mathcal{O}}\,(\tilde{\mu})\,\psi\,(\theta_{\mathfrak{C}}) = (1 - \zeta_{2^m})^{|\tilde{S}_1|}\,\mathrm{Fit}_{\mathcal{O}}\,(\mathrm{Ker})$$

are equal for any character ψ in $\mathfrak{C}$. We write $\theta_{\mathfrak{C}} = \left(1 - \sigma^{p^{n-1}}\right)\overline{\theta}_{\mathfrak{C}}$ as in equations (4.35) and (4.36). Proposition 4.6.3 shows that $\psi\left(q\overline{\theta}_{\mathfrak{C}}\right)$ is integral at prime ideals other than (λ). Also, the (λ)-valuations of both sides of

$$\psi\left(q\overline{\theta}_{\mathfrak{C}}\right) = \frac{q\,(1 - \zeta_{2^m})^{|\tilde{S}_1|}\,\mathrm{Fit}_{\mathcal{O}}\,(\mathrm{Ker})}{(1 - \zeta_p)\,\mathrm{Fit}_{\mathcal{O}}\,(\tilde{\mu})}$$

are equal. Equation (5.15) and the assumption that p does not divide $q = |\tilde{\mu}|$ show that the right side is (λ)-integral. Therefore, $q\psi\left(\overline{\theta}_{\mathfrak{C}}\right)$ is an algebraic integer. The end of the proof of Proposition 4.6.3 now shows that $q\theta_{\mathfrak{C}}$ is contained in $\mathbb{Z}[G]$. □

Remark. To conclude that $q\psi\left(\overline{\theta}_{\mathfrak{C}}\right)$ is an algebraic integer in the above proof, it is essential that there is only one prime of $\mathbb{Q}\left(\zeta_{p^n}\right)$ dividing p. Thus, it is necessary to restrict the lemma to the case where $m = 1$. If $m > 1$, then let $\mathcal{O} = \mathbb{Z}\left[\zeta_{2^m p^n}\right]$. To generalize the above proof, it is necessary to prove that $1 - \zeta_p$ divides $\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)$. Perhaps this could be accomplished as follows. The quotient $A_n/A_n^{\mathcal{H}}$ is annihilated both by $1 + \tau$ and $N_{\mathcal{H}}$. It is therefore an $\mathcal{O}$-module. We can then rewrite the equation in Lemma 5.2.3 as

$$p^{2^{m-1}s}\left|A_n/A_n^{\mathcal{H}}\right| = \left|A_n\right| / \left|A_{n-1}\right| = \left|\mathrm{Ker}_p\right|.$$

It is natural to conjecture the following equality, which implies the above equation by property 6 of Fitting ideals:

$$\left(1 - \zeta_{p^n}\right)^s \mathrm{Fit}_{\mathcal{O}}\left(A_n/A_n^{\mathcal{H}}\right) = \mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}_p\right). \tag{5.16}$$

Since the proof of Lemma 2.5 in [18] is based on Lemma 4.1 on p. 307 in [32], which is proved using purely algebraic methods, perhaps there is some hope for proving this conjecture. If $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ as an affirmative answer, then this conjecture is implied by the conjectural equality

$$\mathrm{Fit}_{\mathcal{O}}\left(\tilde{\mu}\right)\psi\left(\theta_{\mathfrak{C}_{2^m p^n}}\right) = \left(1 - \zeta_{2^m}\right)^{\left|\tilde{S}_1\right|}\left(1 - \zeta_{p^n}\right)^{\left|\tilde{S}_3\right|}\mathrm{Fit}_{\mathcal{O}}\left(A_n/A_n^{\mathcal{H}}\right),$$

where $\tilde{S}_3$ is the set of places in k_{n-1} lying over places in S_0 that split completely in K_{n-1}/k_{n-1}. In this formula, there is a beautiful symmetry between the sets $\tilde{S}_1$ and $\tilde{S}_3$. Let c be either 2 or p. Then the set in the exponent on the factor dividing c in the above formula is a set of places in the subfield of K_n of maximal c-power degree over k_0, and it consists of the places lying above those places in S_0 that split completely in the extension field of k_0 having maximal c-power index in K_n.

For the following propositions, K_n/k_0 will be an extension as in the previous lemmas, and s will be the integer defined in Lemma 5.2.3. We set $\tilde{q} = q$ if p divides q or $s \geq p^{n-1}$, and set $\tilde{q} = pq$ otherwise. Similarly, we set $\tilde{W} = W_n$ when $\tilde{q} = q$ and $\tilde{W} = pW_n$ when $\tilde{q} = pq$. Finally, we denote the p-primary part of Cl_{K_n} by Cl_p.

Proposition 5.2.5. *Let K_n/k_0 be an extension of degree $2^m p^n$ for which p divides $\tilde{q}$. If the p-primary part of $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer, then*

$$\tilde{q}\theta_{\mathfrak{C}} \in \mathrm{Ann}_{\mathbb{Z}[G]} \mathrm{Cl}_p,$$

and each principal ideal produced by applying $\tilde{q}\theta_{\mathfrak{C}}$ to an ideal representing a class in Cl_p is generated by an anti-unit.

Proof. We continue with the notation from the beginning of this section. Assume that S_0 is the minimal possible set of places in k_0. Then the set $\tilde{S}_2$ of places in k_n lying above places in S_0 that split completely in K_0/k_0 and are unramified in k_n/k_0 is empty. Let $\mathfrak{P}$ be a prime ideal divisor of p in $\mathcal{O}$. The p-primary part of $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ implies that

$$v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}(\tilde{\mu})\,\chi(\theta_{\mathfrak{C}})\right) = v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}(\mathrm{Ker})\right), \tag{5.17}$$

where $\tilde{\mu}$ and Ker have the $\mathcal{O}$-module structures provided by χ.

By Proposition 4.6.3, $\tilde{q}\theta_{\mathfrak{C}}$ has integer coefficients. The same argument used to derive equation (5.8) provides the factorization

$$\tilde{q}\theta_{\mathfrak{C}} = \left(1 - \sigma^{p^{n-1}}\right)\alpha(1-\tau),$$

where α has integral coefficients. Recall that in general, the exact power of p dividing $q = |\tilde{\mu}|$ is either 1 or p. With our current assumption, p is the exact power of p dividing $\tilde{q}$. Equation (5.17) implies that

$$\begin{aligned} v_{\mathfrak{P}}(\chi(\alpha)) &= v_{\mathfrak{P}}(\chi(\theta_{\mathfrak{C}})) + v_{\mathfrak{P}}(\tilde{q}) - v_{\mathfrak{P}}(1-\zeta_p) \\ &= v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}(\mathrm{Ker})\right) - v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}(\tilde{\mu})\right) + p^{n-1}(p-2) \\ &\geq v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}(\mathrm{Ker})\right) + p^{n-1}(p-2) - 1 \\ &\geq v_{\mathfrak{P}}\left(\mathrm{Fit}_{\mathcal{O}}(\mathrm{Ker})\right). \end{aligned} \tag{5.18}$$

The algebraic integer $\chi(\alpha)$ is thus divisible by the $\mathcal{O}$-Fitting ideal of the p-primary part of Ker. As α acts on this $\mathcal{O}$-module as $\chi(\alpha)$, property 2 of Fitting ideals shows that α annihilates the p-primary part of Ker. The argument used to derive equation (5.10) shows that $\tilde{q}\theta_{\mathfrak{C}}$ annihilates Cl_p, producing principal ideals generated by anti-units. □

Proposition 5.2.6. *Let K_n/k_0 be an extension of degree $2p^n$ (so we are setting $m = 1$). If p does not divide $\tilde{q}$, then*

$$\tilde{q}\theta_{\mathfrak{C}} \in \mathrm{Ann}_{\mathbb{Z}[G]} \mathrm{Cl}_p,$$

and each principal ideal produced by applying this element to an ideal representing a class in Cl_p is generated by an anti-unit.

Proof. Lemma 5.2.4 shows that $\tilde{q}\theta_{\mathfrak{C}}$ has integer coefficients. Let $\lambda = 1 - \zeta_{p^n}$, and let v_λ be the normalized valuation on $\mathcal{O} = \mathbb{Z}[\zeta_{p^n}]$ corresponding to the prime ideal (λ). Since (λ) is the only prime ideal divisor of p in $\mathcal{O}$, equation (4.31) implies that the p-primary part of the question $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer. As in the preceding proposition, we write

$$\tilde{q}\theta_{\mathfrak{C}} = \left(1 - \sigma^{p^{n-1}}\right) \alpha(1 - \tau).$$

The assumption that p does not divide $\tilde{q}$ implies that p does not divide $q = |\tilde{\mu}|$. Equation (5.17) then yields

$$v_\lambda\left(\chi(\alpha)\right) = v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right) - p^{n-1}, \tag{5.19}$$

which, at first glance, seems to be too small for what we need.

To rectify this situation, observe that the modules $\left(1 - \sigma^{p^{n-1}}\right)\mathrm{Coker}_n$ and $\mathrm{Coker}_n/\mathrm{Coker}_n^H$ are annihilated by the norm element in $\mathbb{Z}[G]$ associated with the extension K_n/K_{n-1}. Lemma 2.3.4 shows that they are $\mathcal{O}$-modules. Moreover, multiplication by $\left(1 - \sigma^{p^{n-1}}\right)$ gives an $\mathcal{O}$-module epimorphism

$$\mathrm{Coker}_n/\mathrm{Coker}_n^H \to \left(1 - \sigma^{p^{n-1}}\right)\mathrm{Coker}_n.$$

Letting A_n, A_{n-1}, and Ker_p denote the p-primary parts of Coker_n, Coker_{n-1}, and Ker respectively, Lemma 5.2.3 shows that

$$|\mathrm{Ker}_p| = \frac{|A_n|}{|A_{n-1}|} = p^s \left|A_n/A_n^H\right|.$$

Since (λ) is the only prime ideal divisor of p in $\mathcal{O}$, it follows that

$$\begin{aligned} v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right) &= s + v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Coker}_n/\mathrm{Coker}_n^H\right)\right) \\ &\geq s + v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\left(1 - \sigma^{p^{n-1}}\right)\mathrm{Coker}_n\right)\right), \end{aligned} \tag{5.20}$$

where the inequality follows from property 7 of Fitting ideals. The assumption that p does not divide $\tilde{q}$ implies that $s \geq p^{n-1}$. Equation (5.19) thus shows that

$$\begin{aligned} v_\lambda\left(\chi(\alpha)\right) &= v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\left(1-\sigma^{p^{n-1}}\right)\mathrm{Coker}_n\right)\right) + s - p^{n-1} \\ &\geq v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\left(1-\sigma^{p^{n-1}}\right)\mathrm{Coker}_n\right)\right). \end{aligned}$$

Property 2 of Fitting ideals then shows that α annihilates the p-primary part of the $\mathcal{O}$-module $\left(1-\sigma^{p^{n-1}}\right)\mathrm{Coker}_n$. We now observe that the derivation of equation (5.10) only requires that α has this property. It follows that $\tilde{q}\theta_{\mathfrak{C}}$ annihilates Cl_p, producing principal ideals generated by anti-units. □

Proposition 5.2.7. *Let K_n/k_0 be an extension of degree $2p^n$. Let p^t be the largest power of p dividing W_n. If $s \geq p^{n-1}$, then the principal ideals produced by applying $W_n\theta_{\mathfrak{C}}$ to ideals representing classes in Cl_p are generated by p^t-Abelian anti-units.*

Proof. Let $\mathcal{O}$ and λ be as defined in the previous proposition. We observe again that the p-primary part of $\mathrm{Q}_{2^m p^n}\left(K_n/k_0\right)$ has an affirmative answer. Let $\mathfrak{a}$ be an ideal representing a class in Cl_p. Propositions 5.2.5 and 5.2.6 show that

$$\mathfrak{a}^{\tilde{q}\theta_{\mathfrak{C}}} = (\gamma)$$

for some anti-unit γ in $K_n^\times$. If p does not divide $\tilde{q} = q$, then

$$\mathfrak{a}^{W_n\theta_{\mathfrak{C}}} = \left(\gamma^{\frac{W_n}{q}}\right).$$

This generator is then trivially p^t-Abelian, since p^t divides $\frac{W_n}{q}$.

Otherwise, we must consider the case when p divides q. Let $\mu^{(p)}$ be the group of p-power roots of unity in K_n. Let g be a generator of G, and let Ng be an integer such that

$$\zeta^g = \zeta^{Ng}$$

for all ζ in $\mu^{(p)}$. Let P_{anti} denote the group of nonzero principal ideals of K_n generated by anti-units. We will first prove the claim that $(Ng-g)\frac{W_n}{p^t}\theta_{\mathfrak{C}}$ is in $\mathbb{Z}[G]$ and

$$\mathfrak{a}^{(Ng-g)\frac{W_n}{p^t}\theta_{\mathfrak{C}}} \in P_{\mathrm{anti}}$$

for each ideal $\mathfrak{a}$ representing a class in Cl_p.

Since p divides $|\tilde{\mu}| = q$ and $Ng - g$ annihilates $\tilde{\mu}$, it follows that

$$\chi\left(Ng - g\right) \in \mathrm{Fit}_{\mathcal{O}}\,\tilde{\mu},$$

and so

$$v_\lambda\left(\chi\left(Ng - g\right)\right) \geq 1. \tag{5.21}$$

Proposition 4.6.3 shows that $W_n\theta_{\mathfrak{C}}$ is integral. The argument used to derive equation (5.8) shows that we can write

$$\left(Ng - g\right) W_n\theta_{\mathfrak{C}} = \left(1 - \sigma^{p^{n-1}}\right)\beta(1 - \tau),$$

where

$$\beta = \sum_{i=0}^{(p-1)p^{n-1}-1} b_{ij}\sigma^i$$

for some integer coefficients b_{ij}. Then equations (5.17), (5.20), and (5.21) show that

$$\begin{aligned} v_\lambda\left(\chi(\beta)\right) &= v_\lambda\left(\frac{\chi\left(Ng - g\right)W_n}{1 - \zeta_p}\right) + v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right) - v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\tilde{\mu}\right)\right) \\ &\geq 1 + tp^{n-1}(p-1) - p^{n-1} + v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\mathrm{Ker}\right)\right) - 1 \\ &\geq tp^{n-1}(p-1) + v_\lambda\left(\mathrm{Fit}_{\mathcal{O}}\left(\left(1 - \sigma^{p^{n-1}}\right)\mathrm{Coker}_n\right)\right), \end{aligned} \tag{5.22}$$

where we have used the assumption that $s \geq p^{n-1}$. Thus, p^t divides the algebraic integer

$$\sum_{i=0}^{(p-1)p^{n-1}-1} b_{ij}\zeta_{p^n}^i$$

in $\mathcal{O}$. The numbers $\zeta_{p^n}^i$ for $0 \leq j \leq 2^{m-1} - 1$ and $0 \leq i \leq (p-1)p^{n-1} - 1$ form an integral basis for $\mathcal{O}$, so the integers b_{ij} are divisible by p^t. It follows that

$$(Ng - g)\frac{W_n}{p^t}\theta_{\mathfrak{C}} \in \mathbb{Z}[G], \tag{5.23}$$

which is the first part of the claim.

We will next see that the extension K_n/K_0 is the nth layer of the cyclotomic $\mathbb{Z}_p$ extension of K_0. Let p^u be the number of pth power roots of unity in K_0. Then

$$\mathbb{Q}\left(\zeta_{p^u}\right) \subseteq K_0 \cap \mathbb{Q}\left(\zeta_{p^t}\right) \subseteq \mathbb{Q}\left(\zeta_{p^t}\right).$$

It follows that

$$K_0 \cap \mathbb{Q}\left(\zeta_{p^t}\right) = \mathbb{Q}\left(\zeta_{p^v}\right)$$

for some v such that $u \leq v \leq t$. Since K_0 does not contain the p^{u+1}th roots of unity, it follows that $v = u$. Therefore, the restriction map

$$\mathrm{Gal}\left(K_0\left(\zeta_{p^t}\right)/K_0\right) \to \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{p^t}\right)/\mathbb{Q}\left(\zeta_{p^u}\right)\right)$$

is an isomorphism. However, the assumption that p divides q implies that $K_0\left(\zeta_{p^t}\right)$ is a subfield of K_n not contained in K_{n-1}. It follows that $K_0\left(\zeta_{p^t}\right) = K_n$. Then $n = t - u$, so the assertion follows.

The assertion implies that g^2 fixes the p^uth roots of unity but not the p^{u+1}th roots of unity. It follows that $(Ng)^2 - 1$ is exactly divisible by p^u. Then

$$(Ng)^{2p^n} - 1 = \left(\left((Ng)^2 - 1\right) + 1\right)^{p^n} - 1 \equiv p^n\left((Ng)^2 - 1\right) \pmod{p^{t+1}},$$

so that $(Ng)^{2p^n} - 1$ is exactly divisible by p^t. Set

$$c = \frac{(Ng)^{2p^n} - 1}{p^t},$$

where $(c, p) = 1$. Let $\mathfrak{a}$ be an ideal representing a class in Cl_p. Because c is relatively prime to p, we can find an ideal $\mathfrak{a}'$ in Cl_p and an element γ' in $K_n^\times$ such that $\mathfrak{a}(\gamma') = \mathfrak{a}'^c$. The inequality (5.22) shows that

$$\sum_{i=0}^{(p-1)p^{n-1}-1} \frac{b_{ij}}{p^t}\sigma^i$$

annihilates the p-primary part of $\left(1 - \sigma^{p^{n-1}}\right)\mathrm{Coker}_n$. The argument used to derive equation (5.10) (with β in place of α) then shows that there is an element $\tilde{\gamma}$ in $K_n^\times$ such that

$$\mathfrak{a}'^{\,(Ng-g)\frac{W_n}{p^t}\theta_{\mathfrak{C}}} = \left(\tilde{\gamma}^{1-\tau}\right).$$

Applying $\beta = \sum_{i=0}^{2p^n-1}(Ng)^i\, g^{2p^n-1-i}$ to both sides, we find that

$$\mathfrak{a}'^{\left((Ng)^{2p^n}-1\right)\frac{W_n}{p^t}\theta_{\mathfrak{C}}} = \mathfrak{a}^{W_n\theta_{\mathfrak{C}}}\left(\gamma'^{W_n\theta_{\mathfrak{C}}}\right) = \left(\tilde{\gamma}^{\beta(1-\tau)}\right).$$

We will now see that the generator $\gamma = \tilde{\gamma}^{\beta(1-\tau)}\gamma'^{-W_n\theta_{\mathfrak{C}}}$ for the principal ideal $\mathfrak{a}^{W_n\theta_{\mathfrak{C}}}$ is p^t-Abelian (property 4 of components of L-function evaluators shows that

it is an anti-unit). First, for any r such that $1 \leq r \leq 2p^n - 1$, $(Ng)^r - g^r$ annihilates $\mu^{(p)}$, and

$$\begin{aligned}\gamma^{(Ng)^r - g^r} &= \tilde{\gamma}^{\beta(1-\tau)(Ng-g)\sum_{i=0}^{r-1}(Ng)^i g^{r-1-i}} \gamma'^{-W_n \theta_{\mathfrak{C}}(Ng-g)\sum_{i=0}^{r-1}(Ng)^i g^{r-1-i}} \\ &= \tilde{\gamma}^{\left((Ng)^{2p^n}-1\right)(1-\tau)\sum_{i=0}^{r-1}(Ng)^i g^{r-1-i}} \gamma'^{-W_n \theta_{\mathfrak{C}}(Ng-g)\sum_{i=0}^{r-1}(Ng)^i \sigma^{r-1-i}}.\end{aligned}$$

The first factor is in $K_n^{\times p^t}$ since p^t divides $(Ng)^{2p^n} - 1$, and equation (5.23) shows that the second factor is in $K_n^{\times p^t}$. Therefore,

$$\gamma^{(Ng)^r - g^r} \in K_n^{\times p^t} \tag{5.24}$$

for $1 \leq r \leq 2p^n - 1$.

Now $K_n\left(\sqrt[p^t]{\gamma}\right)/K_n$ is a Kummer extension. From Section 2.5, the subgroup Δ of $K_n^\times$ generated by γ and $K_n^{\times p^t}$ corresponds to this extension through Kummer theory. The inclusion (5.24) shows that γ^{g^r} is also in Δ for $1 \leq r \leq 2p^n - 1$. Hence, $K_n\left(\sqrt[p^t]{\gamma}\right)/k_0$ is a Galois extension by Proposition 2.7.2.

Next, let $\tilde{G} = \mathrm{Gal}\left(K_n\left(\sqrt[p^t]{\gamma}\right)/k_0\right)$ and $H = \mathrm{Gal}\left(K_n\left(\sqrt[p^t]{\gamma}\right)/K_n\right)$. We will show that $\tilde{G}$ is a central extension of H by G. The argument is that of the second half of Lemma A.1.4 in the appendix of [10]. Let η be a p^tth root of γ. Let r be an integer such that $0 \leq r \leq 2p^n - 1$, and let $\tilde{g}$ be an element of $\tilde{G}$ that restricts to the element g in G. The inclusion (5.24) shows that there exists ξ in $K_n^\times$ such that

$$\eta^{(Ng)^r - \tilde{g}^r} = \xi.$$

Let h be in H, and let ζ be the p^tth root of unity such that $h\eta = \zeta\eta$. Then

$$\begin{aligned}\eta^{h\tilde{g}^r - \tilde{g}^r h} &= \eta^{((Ng)^r - \tilde{g}^r)h} \eta^{h(\tilde{g}^r - (Ng)^r)} \\ &= \xi^h \left(\zeta\eta\right)^{-((Ng)^r - \tilde{g}^r)} \\ &= \xi\xi^{-1} \\ &= 1.\end{aligned}$$

Since the elements $\tilde{g}^r$ for $0 \leq r \leq 2p^n - 1$ form a complete set of coset representatives for $\tilde{G}/H$, it follows that $\tilde{G}$ is a central extension of H by G. Finally, $\tilde{G}$ is generated by H and the lifts $\tilde{g}^n$. Since these lifts all commute with each other, $\tilde{G}$ is Abelian. $\square$

Remark. The result of Proposition 5.2.7 in the case when $n = 1$ was essentially proved in [18]. The present proof is merely an adaptation of their methods, the only new addition being the use of the p-primary part of question $\mathrm{Q}_{2^m p^n}(K_n/k_0)$. Again, extending to the case of degree $2^m p^n$ extensions seems to be hindered only by the lack of a method to distinguish between the distinct prime ideals of $\mathbb{Z}[\zeta_{2^m p^n}]$ dividing p. This difficulty could be overcome if one could verify equation (5.16), the conjectured refinement of Lemma 5.2.3.

5.3 The Brumer-Stark conjecture for extensions of degree $2^m p^n$

In this section, we will use the results of the previous section to analyze the Brumer-Stark conjecture for a fixed cyclic extension of degree $2^m p^n$. If p' is a prime number not equal to p, we will see that if the p'-primary part of $\mathrm{Q}_{2^m p^n}(K_r/k_0)$ has an affirmative answer for $1 \leq r \leq n$ and the p'-primary part of $\mathrm{Q}_{2^m}(K_0/k_0)$ has an affirmative answer, then the p'-primary part of the Brumer-Stark conjecture holds for K_n/k_0. The p-primary part turns out to be much less tractable. Assuming that the p-primary part of $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer, we will prove (BS_p) only when θ has only one nonzero component. Proving even the annihilation statement of (BS_p) becomes much more difficult when θ comprises more than one nonzero component. We will provide proofs of the annihilation statement for certain extensions for which θ has two nonzero components and also for the finite layers of the cyclotomic $\mathbb{Z}_p$ extension of k_0 in the case where $[k_0(\zeta_p) : k_0] = 2^m$.

Theorem 5.3.1. *Let K_n/k_0 be a cyclic extension of degree $2^m p^n$ with Galois group G. Let p' be a prime number different from p. If the p'-primary part of $\mathrm{Q}_{2^m p^n}(K_r/k_0)$ has an affirmative answer for $1 \leq r \leq n$ and the p'-primary part of $\mathrm{Q}_{2^m}(K_n/k_0)$ has an affirmative answer, then the p'-primary part of the Brumer-Stark conjecture holds for K_n/k_0.*

Proof. We use the notation of Section 4.6. Let H and H' be the subgroups of G of orders p^n and 2^m respectively. For $0 \leq r \leq n$, let N_r be the norm element in $\mathbb{Z}[G]$

corresponding to the subgroup of G of order p^{n-r}. Let S_0 be the set of places of k_0 consisting of the Archimedean places and the prime ideals that ramify in K_n/k_0. For $0 \leq r \leq n$, let $\mathfrak{C}_r$ be the equivalence class of characters in $\widehat{G}$ of order $2^m p^r$. For simplicity, we set $\theta = \theta_{K_n/k_0,S_0}$ and $\theta_{\mathfrak{C}_n} = \theta_{K_n/k_0,S_0,\mathfrak{C}_n}$. If $0 \leq r \leq n$, let $\tilde{\theta}_{\mathfrak{C}_r}$ be a lift of $\theta_{K_r/k_0,S_0,\mathfrak{C}_{2^m p^r}}$ to $\mathbb{C}[G]$ chosen by extending each automorphism of K_r to an element in G (so that $\theta_{\mathfrak{C}_n} = \tilde{\theta}_{\mathfrak{C}_n}$). Then property 2 of components of L-function evaluators shows that

$$\theta = \sum_{r=0}^{n} \frac{\mathrm{N}_r}{p^{n-r}} \tilde{\theta}_{\mathfrak{C}_r}.$$

Let $\mathfrak{a}$ be an ideal representing a class in $\mathrm{Cl}_{p'}$, the p'-primary part of the ideal class group of K_n. Then since p' is relatively prime to p, there exists an ideal $\mathfrak{b}$ and an element γ in $K_n^{\times}$ such that

$$\mathfrak{a} = \mathfrak{b}^{p^{n+1}} (\tilde{\gamma}).$$

Write ι_r for the canonical map of class groups $\mathrm{Cl}_{K_r} \to \mathrm{Cl}_{K_n}$. We have

$$\mathfrak{b}^{\mathrm{N}_r} = \iota_r (\mathfrak{b}_r),$$

where $\mathfrak{b}_r$ is the image of $\mathfrak{B}$ under the norm map $\mathrm{N}\colon \mathrm{Cl}_{K_n} \to \mathrm{Cl}_{K_r}$. Then

$$\mathfrak{b}^{p^{r+1} W_n \mathrm{N}_r \tilde{\theta}_{\mathfrak{C}_r}} = \iota_r \left(\mathfrak{b}_r^{p^{r+1} W_n \theta_{\mathfrak{C}_r}} \right).$$

If p'^t is the exact power of p' dividing W_n, then Propositions 5.2.1 and 5.2.2 show that

$$\mathfrak{b}_r^{p^{r+1} W_n \theta_{\mathfrak{C}_r}} = (\varepsilon_r)$$

for some p'^t-Abelian anti-unit ε_r in $K_r^{\times}$ (when $p' = 2$, recall that $(2, pq) = 1$). Then

$$\begin{aligned} \mathfrak{a}^{W_n \theta} &= \mathfrak{b}^{p^{n+1} W_n \theta} (\tilde{\gamma})^{W_n \theta} \\ &= \mathfrak{b}^{\sum_{r=0}^{n} p^{r+1} W_n \mathrm{N}_r \tilde{\theta}_{\mathfrak{C}_r}} (\tilde{\gamma})^{W_n \theta} \\ &= \left(\prod_{r=0}^{n} \varepsilon_r \right) (\tilde{\gamma})^{W_n \theta}. \end{aligned}$$

In [59, §2], Tate showed that the statement of the Brumer-Stark conjecture is true when the ideal in the conjecture is principal. Therefore, there exists an p'^t-Abelian anti-unit γ in $K_n^\times$ such that

$$(\tilde{\gamma})^{W_n\theta} = (\gamma)\,.$$

We find that the element

$$\left(\gamma \prod_{r=0}^{n} \varepsilon_r\right)$$

is a p'^t-Abelian anti-unit generator for $\mathfrak{a}^{W_n\theta}$. Hence, $(\mathrm{BS}_{p'})$ holds for the extension K_n/k_0. □

Remark. When $p' = 2$, we did not use the full annihilation result of Proposition 5.2.2, which shows that we may remove the factor of $2^{[k_0\colon \mathbb{Q}]-1}$. The above proof can be adapted to show that an affirmative answer for the 2-primary part of $\mathrm{Q}_{2^m p^n}(K_r/k_0)$ for $1 \le r \le n$ implies that (BS_2) holds for the extension K_n/k_0 with θ replaced by

$$\frac{1}{2^{[k_0\colon \mathbb{Q}]-1}}\theta.$$

The following result generalizes Propositions 2.1 and 2.2 in [18] (excepting the part of Proposition 2.1 which treats "case I(b)", which is essentially a special case of Greither's work on "nice" extensions).

Theorem 5.3.2. *Let K_n/k_0 be a cyclic extension of degree $2p^n$ with Galois group G. Assume that only one component of θ_{K_n/k_0} is nonzero. Then the p-primary part of the Brumer-Stark conjecture holds for the extension K_n/k_0.*

Proof. Let S_0 be the set of places of k_0 consisting of the Archimedean places and the prime ideals that ramify in K_n/k_0. For $0 \le r \le n$, let $\mathfrak{C}_r$ be the equivalence class of characters in $\widehat{G}$ of order $2^m p^r$. Property 2 of components of L-function evaluators shows that the component $\theta_{\mathfrak{C}_r}$ of θ is 0 if and only if some prime in S_0 splits completely in K_r/k_0. Therefore, the assumption in the theorem is equivalent to the existence of a prime ideal in k_0 that splits completely in K_{n-1} and ramifies in K_n. The number s defined in Lemma 5.2.3 is thus greater than or equal to p^{n-1}, and also

$$W_n\theta = W_n\theta_{\mathfrak{C}}.$$

Proposition 5.2.7 thus proves the theorem. □

The next corollary follows immediately from theorems 5.3.1 and 5.3.2.

Corollary 5.3.3. *Let K_n/k_0 be a cyclic extension of degree $2p^n$. Assume that only one component of θ_{K_n/k_0} is nonzero. If the p' primary part of $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer for all prime numbers $p' \neq p$, then the Brumer -Stark conjecture holds for the extension K_n/k_0.*

Remark. Note that if 2 is inert in $\mathbb{Z}[\zeta_{p^n}]$, then the 2-primary part of $\mathrm{Q}_{2^m p^n}(K_n/k_0)$ has an affirmative answer. The other primary parts of the Brumer-Stark conjecture sometimes follow from the work of Wiles ([64]).

The following corollary follows from Corollaries 4.7.3 and 5.3.3.

Corollary 5.3.4. *Let $k' \subseteq k_0 \subseteq K_n$ be a tower of number fields with K_n/k_0 cyclic of degree $2p^n$ and K_n/k' and k_0/k' Galois. Assume that θ_{K_n/k_0} has only one nonzero component. Suppose that the map*

$$\phi\colon \mathrm{Gal}(k_0/k') \to \mathrm{Gal}(\mathbb{Q}(\zeta_{2p^n})/\mathbb{Q})$$

from Section 4.7 is surjective. Then the Brumer-Stark conjecture holds for the extension K_n/k_0.

We now turn to extensions where θ comprises more than one nonzero component. Obtaining even the annihilation statement of the p-primary part of the Brumer-Stark conjecture is more difficult in this setting. We resume the notation from Section 5.2. In particular, K_n/k_0 is a cyclic extension of degree $2^m p^n$ with Galois group G. For $0 \leq r \leq n$, K_r is the subfield of degree $2^m p^r$ over k_0, $W_r = |\mu_r|$ is the cardinality of the group of roots of unity in K_r, and

$$q = \frac{W_n}{W_{n-1}}$$

is the cardinality of the $\mathcal{O}$-module $\tilde{\mu} = \mu_n/\mu_{n-1}$. The set S_0 of places of k_0 consists of the Archimedean places and the prime ideals that ramify in K_n/k_0. We denote the p-primary part of Cl_{K_n} by Cl_p. For simplicity, we write θ instead of $\theta_{K_n/k_0,S_0}$ and θ_{n-1} instead of $\theta_{K_{n-1}/k_0,S_0}$.

To begin we will consider the case where K_n/K_0 is the nth layer of the cyclotomic $\mathbb{Z}_p$ extension of K_0.

Theorem 5.3.5. *Let K_n/k_0 be a cyclic extension of degree $2^m p^n$. Assume that K_0 contains the pth roots of unity, and that K_n/K_0 is the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of K_0. If the p-primary part of $(\mathrm{Q}_{2^m p^r})$ has an affirmative answer for each extension K_r/k_0 with $1 \leq r \leq n$ and (B_p) holds for the degree 2^m extension K_0/k_0, then*

$$W_n\theta \in \mathrm{Ann}_{\mathbb{Z}[G]} \mathrm{Cl}_p.$$

Remark. Both assumptions in the theorem are true when $m = 1$: the p-primary part of $\mathrm{Q}_{2^m p^n}$ (K_n/k_0) follows from equation (4.31), and (B_p) follows from Tate's proof of the Brumer-Stark conjecture for quadratic extensions ([59, §3, case (c)]).

Proof. Let S_0 be the set of places of k_0 consisting of the Archimedean places and the prime ideals that ramify in K_n/k_0. For $0 \leq r \leq n$, let $\mathfrak{C}_r$ be the equivalence class of characters in $\widehat{G}$ of order $2^m p^r$. Also, set $\theta_r = \theta_{K_r/k_0,S_0}$. Choose a lift $\tilde{\theta}_{n-1}$ of θ_{n-1} to $\mathbb{Q}[G]$ by choosing an extension of each automorphism in $\mathrm{Gal}\,(K_{n-1}/k_0)$ to G. Let N_p be the norm element in $\mathbb{Z}[G]$ corresponding to the extension K_n/K_{n-1}. Property 2 of components of L-function evaluators shows that

$$\theta = \theta_{\mathfrak{C}_n} + \frac{N_p}{p}\tilde{\theta}_{n-1}.$$

Then

$$W_n\theta = W_n\theta_{\mathfrak{C}_n} + \frac{q}{p}W_{n-1}\tilde{\theta}_{n-1}N_p, \tag{5.25}$$

and $\frac{q}{p}$ is an integer since K_n/K_0 is a layer of the cyclotomic $\mathbb{Z}_p$-extension of K_0.

Let $\mathfrak{a}$ be an ideal representing a classs in Cl_p. Denote the canonical homomorphism $\mathrm{Cl}_{K_{n-1}} \to \mathrm{Cl}_{K_n}$ by ι. We will prove the theorem by induction on n. Assume first that $n = 1$. Then

$$\mathfrak{a}^{N_p} = \iota\left(\mathrm{N}_{K_1/K_0}\,\mathfrak{a}\right).$$

It follows that

$$\mathfrak{a}^{\frac{q}{p}W_0\tilde{\theta}_0N_p} = \iota\left(\mathrm{N}_{K_1/K_0}\,\mathfrak{a}^{W_0\theta_0}\right)^{\frac{q}{p}}.$$

By assumption, (B_p) holds for the extension K_0/k_0, so the above ideal is principal. In addition, $\mathfrak{a}^{W_1\theta_{\mathfrak{C}_1}}$ is principal by Proposition 5.2.5. Therefore, equation (5.25) shows that the theorem is true for $n = 1$.

Next, assume that the theorem is true when the extension has degree $2^m p^{n-1}$. We have

$$\mathfrak{a}^{\frac{q}{p}W_{n-1}\tilde{\theta}_{n-1}N_p} = \iota\left(\mathrm{N}_{K_n/K_{n-1}}\,\mathfrak{a}^{W_{n-1}\theta_{n-1}}\right)^{\frac{q}{p}}.$$

The inductive hypothesis shows that this ideal is principal. Again, it follows from Proposition 5.2.5 and equation (5.25) that $W_n\theta$ annihilates Cl_p. □

Next, we consider a generalization of the case II(b) in [18] (as mentioned in Subsection 3.4.2, this was erroneously conflated with what the authors label case ♯; II(b) is actually a special case of ♯). Case II(b) was one of two relatively rare types of extensions which proved intractable using the methods in that paper.

Theorem 5.3.6. *Let K_n/k_0 be cyclic extension of degree $2p^n$. Suppose that K_n contains the pth roots of unity and that θ consists of precisely two nonzero components. Then*

$$W_n\theta \in \mathrm{Ann}_{\mathbb{Z}[G]}\,\mathrm{Cl}_p$$

under either of the following conditions:

1. *$n \geq 2$.*
2. *The maximal elementary p-extension of k_0 unramified outside of p has degree p or p^2 over k_0.*

Proof. In the paragraph following equation (5.23), it was shown that when p divides q, the extension K_n/K_0 is the nth layer of the cyclotomic $\mathbb{Z}_p$ extension of K_0. In this case, the theorem follows from Theorem 5.3.5. We therefore assume that $(p, q) = 1$.

We first consider the case where $n \geq 2$. For $0 \leq r \leq n$, let $\mathfrak{C}_r$ be the equivalence class of characters in $\widehat{G}$ of order $2p^r$. Property 2 of components of L-function evaluators shows that the component $\theta_{\mathfrak{C}_r}$ of θ is 0 if and only if some prime in S_0 splits completely in K_r/k_0. Therefore, the assumption in the theorem is equivalent

to the existence of a prime ideal in S_0 that splits completely in K_{n-2}, but none that splits completely in K_{n-1}. We may thus write

$$W_n\theta = W_n\theta_{\mathfrak{C}_n} + W_n\theta_{\mathfrak{C}_{n-1}}.$$

We will see that each of these terms annihilates Cl_p.

We begin with $W_n\theta_{\mathfrak{C}_{n-1}}$. Let N_p be the norm element in $\mathbb{Z}[G]$ corresponding to the extension K_n/K_{n-1}. Let $\tilde{\theta}_{n-1}$ be a lift of θ_{n-1} to $\mathbb{Q}[G]$ chosen by lifting the automorphisms in $\mathrm{Gal}\,(K_{n-1}/k_0)$ to G. Let $q' = \frac{W_{n-1}}{W_{n-2}}$. Property 2 of components of L-function evaluators shows that

$$\theta_{\mathfrak{C}_{n-1}} = \frac{N_p}{p}\tilde{\theta}_{n-1}.$$

Since there is a prime ideal in S_0 that splits completely in K_{n-2}/k_0, the integer s in Lemma 5.2.3 is greater than or equal to p^{n-2}. Lemma 5.2.4 then shows that

$$q'\tilde{\theta}_{n-1} \in \mathbb{Z}[G].$$

Let $\mathfrak{a}$ be an ideal representing a class in Cl_p. Denote the canonical homomorphism $\mathrm{Cl}_{K_{n-1}} \to \mathrm{Cl}_{K_n}$ by ι. Then

$$\mathfrak{a}^{N_p} = \iota\left(\mathrm{N}_{K_n/K_{n-1}}\,\mathfrak{a}\right).$$

It follows that

$$\begin{aligned}\mathfrak{a}^{W_n\theta_{\mathfrak{C}_{n-1}}} &= \mathfrak{a}^{\frac{W_{n-2}}{p}qq'\tilde{\theta}_{n-1}N_p} \\ &= \iota\left(\mathrm{N}_{K_n/K_{n-1}}\,\mathfrak{a}^{q'\theta_{n-1}}\right)^{\frac{qW_{n-2}}{p}}\end{aligned}$$

(note that p divides W_0, and hence, it divides W_{n-2}). Proposition 5.2.6 shows that this ideal is principal, generated by an anti-unit.

Next, Proposition 4.6.3 shows that

$$pq\theta_{\mathfrak{C}_n} \in \mathbb{Z}[G].$$

Since $(p, q) = 1$ and p divides W_n, Propositions 5.2.5 and 5.2.6 then show that $W_n\theta_{\mathfrak{C}_n}$ annihilates Cl_p. This proves the theorem in the case where $n \geq 2$.

We now prove the theorem for extensions of degree $2p$. For this, we need the following proposition:

Proposition 5.3.7. *Let K_1/k_0 be a cyclic extension of degree $2p$. Suppose that K_1 contains the pth roots of unity, but that p does not divide q. Assume that two components of θ are nonzero. For each ideal $\mathfrak{a}$ in K_1, let $\varepsilon(N_{K_1/K_0}(\mathfrak{a}))$ denote an anti-unit generator for the principal ideal $N_{K_1/K_0}(\mathfrak{a})^{W_0\theta_0}$. Then $W_1\theta$ annihilates Cl_p yielding principal ideals generated by anti-units if and only if*

$$\varepsilon(N_{K_1/K_0}(\mathfrak{a})) \in K_1^{\times p}\mu_1 \tag{5.26}$$

for every ideal $\mathfrak{a}$ representing a class in Cl_p.

Remark. The above condition implies that the Abelian extension of k_0 obtained by adjoining a pth root of $\varepsilon(N_{K_1/K_0}(\mathfrak{a}))$ to K_0 is contained in $K_1\left(\zeta_{pW_1}\right)$. We note that $\varepsilon\left(N_{K_1/K_0}(\mathfrak{a})\right)$ is only defined up to a root of unity in K_0, but this is irrelevant for our result.

Before we prove this proposition, let us first see how it allows us to finish the proof of Theorem 5.3.6. Observe that since θ has two nonzero components, there is no prime ideal in k_0 that splits completely in K_0 and ramifies in k_1/k_0. This places the extension K_1/K_0^+ in case II(b) in the paper [18]. Immediately prior to Proposition 2.2 in that paper, the authors observe that only primes dividing p can ramify in K_1/K_0. If the maximal elementary p-extension of k_0 unramified outside of p has degree p over k_0, then K_1 must be the extension of K_0 obtained by adjoining higher p-power roots of unity to K_0. In this case, the theorem follows from Theorem 5.3.5 (see the remark following the statement of that theorem).

Otherwise, assume that the maximal elementary p-extension of k_0 unramified outside of p has order p^2, and call this field L. We may assume that K_1 is not the extension of K_0 obtained by adjoining higher p-power roots of unity to K_0. But then the extension $K_1\left(\zeta_{pW_1}\right)/K_0$ is a degree p^2 elementary p-extension of K_0 unramified outside of p. Since $K_1\left(\zeta_{pW_1}\right)$ is Abelian over k_0, L is the unique subfield of $K_1\left(\zeta_{pW_1}\right)$ of degree p^2 over k_0.

Now let $\mathfrak{a}$ be an ideal representing a class of p-power order in Cl_{K_1}, and fix an anti-unit generator ε for the principal ideal $N_{K_1/K_0}(\mathfrak{a})^{W_0\theta_0}$ as in Proposition 5.3.7. We will show that ε satisfies the condition (5.26). Property 2 of components of

L-function evaluators shows that

$$\theta_{\mathfrak{C}_0} = \frac{N_p}{p}\tilde{\theta}_0,$$

where $\tilde{\theta}_0$ is the lift of θ_{K_0/k_0} to $\mathbb{Z}[H']$. Since the p-valuations of W_0 and W_1 are the same, Theorem 3.2.4 shows that

$$W_0\theta = W_0\theta_{\mathfrak{C}_1} + W_0\frac{N_p}{p}\tilde{\theta}_0$$

is p-integral. Proposition 4.6.3 shows that the first term on the right side is p-integral. Therefore, the second is as well. As N_p is in $\mathbb{Q}[H]$ and $\tilde{\theta}_0$ is in $\mathbb{Q}[H']$,

$$W_0\theta_0 \in p\mathbb{Z}[H']. \tag{5.27}$$

(We have abused the notation somewhat). The valuations of ε at all primes are thus divisible by p. Proposition 2.5.2 shows that the extension of $K_0(\sqrt[p]{\varepsilon})/K_0$ is unramified outside of p. Tate proved (BS) for quadratic extensions [59, §3, case (c)]. Therefore, $K_0(\sqrt[p]{\varepsilon})$ is Abelian over k_0. The unique subfield of $K_0(\sqrt[p]{\varepsilon})$ of degree p over k_0 is a degree p Abelian extension of k_0 unramified outside of p. It is thus contained in L. We consider separately two possibilities for the field $K_0(\sqrt[p]{\varepsilon})$.

Assume first that

$$K_0\left(\sqrt[p]{\varepsilon}\right) = K_0(\zeta_{pW_0}).$$

By Kummer theory,

$$\varepsilon = \zeta_{W_0}^r\gamma^p$$

for some integer r and number γ in K_0. Therefore, ε satisfies the condition (5.26).

Otherwise, let η be a fixed pth root of ε, and assume that

$$K_0(\eta) \neq K_0(\zeta_{pW_0}).$$

Again by Kummer theory, the fields $K_0(\zeta_{pW_0})$ and $K_0\left(\zeta_{pW_0}^c\eta\right)$ for $0 \leq c \leq p-1$ are distinct. Thus, the subfields of $K_0(\zeta_{pW_0})$ and $K_0\left(\zeta_{pW_0}^c\eta\right)$ for $0 \leq c \leq p-1$ having degree p over k_0 are all distinct. Furthermore, they include all of the elementary p-extensions of k that are unramified outside of p. It follows that one of these latter fields is contained in K_1, and so $K_1 = K_0\left(\zeta_{pW_0}^c\eta\right)$ for some c. In other words, $\zeta_{W_0}^c\varepsilon$ is a pth power in K_1. As claimed, we see that ε satisfies the condition (5.26). The theorem now follows from the proposition. □

Remark. Almost all of the several hundred degree 6 case II(b) extensions for which it was computationally verified in [18] that $W_1\theta$ annihilates the 3-primary part of Cl_{K_1} are covered by the above theorem. Of course, the authors computed much more, showing that (BS_3) holds in each example.

Finally, we must prove Proposition 5.3.7.

Proof of Proposition 5.3.7. Let $\mathfrak{C}_0$ and $\mathfrak{C}_1$ be the equivalence classes of characters in $\widehat{G}$ of order 2 and $2p$ respectively. We have

$$\theta = \theta_{\mathfrak{C}_1} + \theta_{\mathfrak{C}_0}.$$

First, assume that $W_1\theta$ annihilates Cl_p yielding principal ideals generated by anti-units. Let $\mathfrak{a}$ be an ideal representing a class in Cl_p. Since $(p,q)=1$, we can find an ideal $\mathfrak{b}$ representing a class in Cl_p such that $\mathfrak{b}^q = (\gamma)\mathfrak{a}$ for some element γ in $K_1^\times$. By assumption, applying $pW_1\theta$ to $\mathfrak{b}$ gives an ideal generated by the pth power of an anti-unit. By Proposition 5.2.5 (note that $s=0$ and $\tilde{q}=pq$),

$$\mathfrak{b}^{pW_1\theta_{\mathfrak{C}_1}} = \mathfrak{b}^{W_0pq\theta_{\mathfrak{C}_1}} = \left(\tilde{\gamma}^{W_0}\right)$$

for some anti-unit $\tilde{\gamma}$ in $K_1^\times$. The generator $\tilde{\gamma}^{W_0}$ is a pth power. Therefore,

$$\mathfrak{b}^{pW_1\theta_{\mathfrak{C}_0}}$$

is also generated by the pth power of an anti-unit.

Next,

$$\begin{aligned}
\mathfrak{b}^{pW_1\theta_{\mathfrak{C}_0}} &= \mathfrak{b}^{qW_0\tilde{\theta}_0N_p} \\
&= \gamma^{W_0\tilde{\theta}_0N_p}\mathfrak{a}^{W_0\tilde{\theta}_0N_p} \\
&= \iota\left(\mathrm{N}_{K_1/K_0}\left(\gamma^{W_0\theta_0}\mathfrak{a}^{W_0\theta_0}\right)\right) \\
&= \iota\left(\mathrm{N}_{K_1/K_0}\left(\gamma\right)^{W_0\theta_0}\varepsilon\left(\mathrm{N}_{K_1/K_0}(\mathfrak{a})\right)\right).
\end{aligned}$$

Equation (5.27) shows that the coefficients of $W_0\theta_0$ are divisible by p. Therefore, $\mathrm{N}_{K_1/K_0}\left(\gamma\right)^{W_0\theta_0}$ is the pth power of an anti-unit. As we determined earlier that $\mathfrak{b}^{pW_1\theta_{\mathfrak{C}_0}}$ is generated by the pth power of an anti-unit, it follows that $\left(\varepsilon\left(N_{K_1/K_0}(\mathfrak{a})\right)\right)$ is generated by the pth power of an anti-unit. Since an anti-unit generator for a given ideal is specified up to a root of unity, it follows that

$\varepsilon(N_{K_1/K_0}(\mathfrak{a}))$ differs from the pth power of an element of K_1 by a root of unity of K_1. This proves one implication.

For the reverse implication, assume that $\mathfrak{a}$ is an ideal whose class in Cl_{K_1} has p-power order. If

$$\varepsilon(N_{K_1/K_0}(\mathfrak{a})) = \gamma^p \zeta \in K_1^{\times p} \mu_{K_1},$$

then γ is an anti-unit. Furthermore,

$$\mathfrak{a}^{pW_1\theta_{\mathfrak{C}_0}} = \mathfrak{a}^{qW_0\tilde{\theta}_0 N_p} = (\gamma^{pq}),$$

and hence,

$$\mathfrak{a}^{W_1\theta_{\mathfrak{C}_0}} = (\gamma^q).$$

Thus, $W_1\theta_{\mathfrak{C}_0}$ annihilates Cl_p, yielding principal ideals generated by anti-units. Proposition 5.2.5 shows that $W_1\theta_{\mathfrak{C}_1}$ does as well. The proposition thus follows from the decomposition

$$W_1\theta = W_1\theta_{\mathfrak{C}_1} + W_1\theta_{\mathfrak{C}_0}.$$

□

Chapter 6

Hayes's Conjecture

We will begin this chapter by using the results of Chapter 4 to prove the modified strong local version of Hayes conjecture ((H_p)) from Section 3.5 for cyclic extensions of degree 2^m for which the p-primary part of $\mathrm{Q}_{2^m}(k_m/k_0)$ has an affirmative answer. We will then prove a "non-equivariant" reformulation of (H_p) for cyclic extensions of degree $2^m p$ that implies the equivariant version. Next, we will examine the functoriality properties of (H_p), proving "top change" completely and "base change" under certain hypotheses. These results will be sufficient to prove Hayes's conjecture for extensions K/k with K Abelian over $\mathbb{Q}$ of prime conductor (with certain restrictions on S). Finally, we will provide a counterexample to the annihilation part of the strong version of Hayes's conjecture.

6.1 Hayes's conjecture for degree 2^m extensions

Let p be an odd prime number. In this section, we will prove (H_p) for cyclic extensions of degree 2^m for which the p-primary part of $\mathrm{Q}_{2^m}(k_m/k_0)$ has an affirmative answer. Let k_m/k_0 be a degree 2^m cyclic extension of number fields with Galois group G, and for $1 \leq i \leq m-1$, let k_i be the extension of k_0 of degree 2^i contained in k_m. Let S_0 be a set of places of k containing the Archimedean places and the prime ideals that ramify in k_m. For $1 \leq i \leq m$, let S_i be the set of places of k_i lying above the places in S_0. Let $W = |\mu|$ be the cardinality of the group of roots of unity in k_m. We restate (H_p) here for convenience:

Conjecture (H_p)**.** *Let p^r be a prime power divisor of W, and assume that there exists a totally positive element ε in k_0 whose p^rth root generates an unramified extension L of k_m of degree p^r. Then $W\theta_{k_m/k_0,S_0}$ is in $p^r\mathbb{Z}[G]$.*

To prove this, we will prove a stronger "non-equivariant" version of (H_p) for such extensions. Let notation be as in the previous proposition. Let χ be a generator of $\widehat{G}$, and let $\mathcal{O} = \mathbb{Z}[\zeta_{2^m}]$. In Section 4.3, we saw that μ is an $\mathcal{O}$-module. The non-equivariant reformulation of (H_p) is as follows:

Proposition 6.1.1. *Let p^r be a prime power divisor of W, and assume that there exists a totally positive element ε in k_0 whose p^rth root generates an unramified extension L of k_m of degree p^r. Let $H = \mathrm{Gal}(L/k_m)$. Then H is an $\mathcal{O}$-module and $\mathrm{Fit}_{\mathcal{O}} H$ divides $\mathrm{Fit}_{\mathcal{O}} \mu$ as ideals in $\mathcal{O}$.*

Proof. Since both H and μ are cyclic groups, their Fitting ideals as $\mathcal{O}$-modules are the same as their annihilators. Proposition 2.7.2 shows that L/k_0 is Galois, so that $\mathrm{Gal}(L/k_0)$ is an extension of $H = \mathrm{Gal}(L/k_m)$ by G. This provides H with the structure of a $\mathbb{Z}[G]$-module, and Lemma 2.7.4 shows that

$$\mathrm{Ann}_{\mathcal{O}} \mu = \chi\left(\mathrm{Ann}_{\mathbb{Z}[G]} \mu\right) \subseteq \chi\left(\mathrm{Ann}_{\mathbb{Z}[G]} H\right).$$

The first statement of the proposition then follows from the fact that $1 + \tau$ is in $\mathrm{Ann}_{\mathbb{Z}[G]} \mu$. The second statement follows from the above inclusion and the equality

$$\chi\left(\mathrm{Ann}_{\mathbb{Z}[G]} H\right) = \mathrm{Ann}_{\mathcal{O}} H. \qquad \square$$

We now use this proposition to prove (H_p).

Proposition 6.1.2. *Let p be an odd prime number. Let k_m/k_0 be a cyclic extension of number fields of degree 2^m. Let S_0 be a set of places of k_0 containing the Archimedean places and the prime ideals that ramify in k_m/k_0. Assume that the p-primary part of $\mathrm{Q}_{2^m}(k_m/k_0)$ has an affirmative answer. Then (H_p) holds for the extension k_m/k_0 and the set S_0.*

Proof. The proposition is trivial if $\theta_{k_m/k_0,S_0} = 0$. Therefore, we assume that no place in S_0 splits completely in k_m/k_0. In particular, k_0 is totally real and k_m is totally complex.

Let p^r be a prime power divisor of W, and assume that there exists a totally positive element ε in k_0 whose p^rth root generates an unramified extension L of k_m of degree p^r. Let $H = \mathrm{Gal}\,(L/k_m)$. By Proposition 6.1.1, H is an $\mathcal{O}$-module and $\mathrm{Fit}_{\mathcal{O}} H$ divides $\mathrm{Fit}_{\mathcal{O}} \mu$. If p^t is the exact power of p dividing μ, then Lemma 2.4.1 shows that the p-primary part of $\mathrm{Fit}_{\mathcal{O}} \mu$ has the form $\mathfrak{P}^t$ for some prime ideal of $\mathcal{O}$ dividing p and of residual degree 1 over $\mathbb{Q}$. Therefore,

$$\mathrm{Fit}_{\mathcal{O}} H = \mathfrak{P}^r. \tag{6.1}$$

Let τ be complex conjugation. Since p is odd, the p-primary parts of H and Cl_{k_m} decompose into isotypic components correponding to the idempotents $\frac{1+\tau}{2}$ and $\frac{1-\tau}{2}$. Then H, being annihilated by τ, is a quotient of the minus part of the p-primary part Cl_p^- of the ideal class group of k_m. Since no place in S_0 splits completely in k_m/k_0, Coker and the minus class number h^- of k_m differ by a factor of 2. Therefore, the p-primary parts of $\mathrm{Cl}_{k_m}^-$ and Coker are isomorphic. It follows that H is a quotient of Coker. Since H is cyclic, properties 2 and 3 of Fitting ideals in Section 2.4 show that

$$\mathrm{Fit}_{\mathcal{O}}\,(\mathrm{Coker}) \subseteq \mathrm{Ann}_{\mathcal{O}}\,(\mathrm{Coker}) \subseteq \mathrm{Ann}_{\mathcal{O}} H = \mathrm{Fit}_{\mathcal{O}} H.$$

Combining this with equation (6.1), we have found that

$$\mathfrak{P}^r \mid \mathrm{Fit}_{\mathcal{O}}\,(\mathrm{Coker})\,. \tag{6.2}$$

By Theorem 3.2.3,

$$WL_{k_m/k_0,S_0}\,(0,\overline{\chi}) \in \mathcal{O}.$$

Since the p-primary part of $\mathrm{Q}_{2^m}\,(k_m/k_0)$ has an affirmative answer, we have

$$WL_{k_m/k_0,S_0}\,(0,\overline{\chi}) = W\,(\lambda)^{|S_{m-1}|-1}\,\mathrm{Fit}_{\mathcal{O}}\,(\mathrm{Coker})\,(\mathrm{Fit}_{\mathcal{O}}\,(\mu))^{-1}\,.$$

Equation (4.6) shows that this is an integral ideal in $\mathcal{O}$. The exact power p^t of p dividing W factors in $\mathcal{O}$ as

$$p^t\mathcal{O} = \mathfrak{P}^t \prod_{i=1}^{2^{m-1}-1} \mathfrak{P}_i^t,$$

where the ideals $\{\mathfrak{P}, \mathfrak{P}_1, \ldots, \mathfrak{P}_{2^{m-1}-1}\}$ are the distinct prime ideals of $\mathcal{O}$ dividing p. Using (6.2), we find that

$$W(\lambda)^{|S_{m-1}|-1} \operatorname{Fit}_{\mathcal{O}}(\operatorname{Coker}) (\operatorname{Fit}_{\mathcal{O}}(\mu))^{-1} = \mathfrak{a}\mathfrak{P}^r \prod_{i=1}^{2^{m-1}-1} \mathfrak{P}_i^t \subseteq p^r\mathcal{O},$$

where $\mathfrak{a}$ is an ideal in $\mathcal{O}$. It follows that

$$\chi\left(W\theta_{k_m/k_0,S_0}\right) = WL_{k_m/k_0,S_0}(0,\overline{\chi}) \in p^r\mathcal{O}.$$

Let σ be a generator of $\operatorname{Gal}(k_m/k_0)$. Let χ be a generator of $\widehat{G}$, and let ζ_{2^m} be the primitive 2^mth root of unity such that $\chi(\sigma) = \zeta_{2^m}$. Property 2 of L-function evaluators in Section 3.1 and Theorem 3.2.3 show that we can write

$$\theta_{k_m/k_0,S_0} = \sum_{i=0}^{2^{m-1}-1} a_i\sigma^i\frac{1-\tau}{2}, \qquad a_i \in \mathbb{Q}.$$

Therefore,

$$W\sum_{i=0}^{2^{m-1}-1} a_i\zeta_{2^m}^i \in p^r\mathcal{O}.$$

Since the numbers $\zeta_{2^m}^i$ for $i = 0, \ldots, 2^{m-1}-1$ form an integral basis for $\mathbb{Q}(\zeta_{2^m})$ over $\mathbb{Q}$, it follows that the coefficients Wa_i are all divisible by p^r. Thus, $W\theta_{k_m/k_0,S_0}$ is contained in $p^r\mathbb{Z}[G]$, which is the statement (H_p). □

Corollary 6.1.3. *Let p be an odd prime number. Let k_m/k_0 be a cyclic extension of number fields of degree 2^m. Suppose that there exists a field k' with $k' \subseteq k_0 \subseteq k_m$, such that k_m/k' and k_0/k' are Galois extensions. Assume further that the map*

$$\operatorname{Gal}(k_0/k') \to \operatorname{Aut}(\operatorname{Gal}(k_m/k_0))$$

given by lifting an automorphism to $\operatorname{Gal}(k_m/k')$ and conjugating is surjective. Then (H_p) holds for the extension K/k.

Corollary 6.1.4. *Let p be an odd prime number. Let K/k be a quadratic extension of number fields. Then (H_p) holds for the extension K/k.*

The above corollaries and statements follow from Corollary 4.4.3 and Proposition 4.3.2 and the comments preceding it.

6.2 Change of the set S in Hayes's conjecture

In this section, we let K/k be an Abelian extension of number fields with Galois group G and let S be a set of places of k containing the Archimedean places and the prime ideals that ramify in K/k. Write

$$W\theta_{K/k,S} = \sum_{\sigma \in G} a_\sigma \sigma,$$

where W is the number of roots of unity in K and the coefficients a_σ are integers. Denote the coefficient of the identity map by a_1. Let p be an odd prime number. As with the Brumer-Stark conjecture, it is true that if (H_p) holds in the given setup, then it also holds when S is expanded to any larger set of places of k. In fact, we can say more:

Theorem 6.2.1. *Assume that* (H_p) *holds for the extension K/k and a set S of places of k. Then it holds for the extension K/k and any other allowable set S' of places of k containing the prime ideals in S that divide p or split completely in $k(\zeta_p)/k$.*

Proof. For each τ in G, let N_τ be an integer such that

$$\tau(\zeta) = \zeta^{N_\tau}$$

for all roots of unity ζ in K. Theorem 3.2.4 shows that for each τ in G,

$$(\tau - N_\tau) \sum_{\sigma \in G} a_\sigma \sigma \in W\mathbb{Z}[G]. \tag{6.3}$$

Therefore,

$$a_{\tau^{-1}\sigma} \equiv N_\tau a_\sigma \pmod{W}$$

for all pairs of automorphisms σ and τ in G.

If $\mathfrak{p}$ is a prime ideal of k not contained in S, then property 1 of L-function evaluators shows that

$$\theta_{S\cup\{\mathfrak{p}\},K/k} = \left(1 - \sigma_{\mathfrak{p}}^{-1}\right)\theta_{S,K/k}, \tag{6.4}$$

where $\sigma_{\mathfrak{p}}$ is the Frobenius automorphism in G corresponding to $\mathfrak{p}$. If p^r divides (a_1, W), then it follows from the above congruence that p^r divides a_n for all n.

Then from (6.4), one sees that p^r divides the coefficient of the identity map in $W\,\theta_{S',K/k}$ for any set S' containing S.

Let S and S' be a pair of sets as in the theorem. We must show the implication

$$W\theta_{K/k,S} \in p^r\mathbb{Z}[G] \Rightarrow W\theta_{K/k,S'} \in p^r\mathbb{Z}[G]$$

where p^r is a power of p dividing W. From above, it suffices to show this under the assumption that

$$S = S' \cup \mathfrak{p},$$

where $\mathfrak{p}$ is a prime ideal of k that does not divide p, ramify in K/k, or split completely in $k\left(\zeta_p\right)/k$. Let a_n and a'_n denote the coefficients of σ_n in $W\theta_{K/k,S}$ and $W\theta_{K/k,S'}$ respectively. Let $\mathfrak{N}\,\mathfrak{p}$ be the absolute norm of $\mathfrak{p}$. Then

$$\sigma_{\mathfrak{p}}(\zeta) = \zeta^{\mathfrak{N}\,\mathfrak{p}}$$

for all roots of unity ζ in K. From (6.3) and (6.4), we have

$$W\theta_{S,K/k} = W\left(1-\sigma_{\mathfrak{p}}^{-1}\right)\theta_{S',K/k} \equiv \left(1-\mathfrak{N}\,\mathfrak{p}^{-1}\right)W\theta_{S',K/k} \pmod{W\mathbb{Z}\left[G\right]}$$

and so

$$a_n \equiv \left(1-\mathfrak{N}\,\mathfrak{p}^{-1}\right)a'_n \pmod{W},$$

where the inverse $\mathfrak{N}\,\mathfrak{p}^{-1}$ is understood to be taken modulo W. As $\mathfrak{p}$ does not split completely in $k\left(\zeta_p\right)/k$,

$$\mathfrak{N}\,\mathfrak{p}^{-1} \not\equiv 1 \pmod{p}.$$

Thus, if p^r divides a_n, then p^r divides a'_n. □

6.3 Top change for Hayes's conjecture

In this section, we will show that "top change" holds for (H_p).

Theorem 6.3.1. *Let p be an odd prime number. Let $k \subseteq K \subseteq K'$ be a tower of number fields with K'/k Abelian. Let S be a set of places in k containing the Archimedean places and the prime ideals that ramify in K'. If (H_p) holds for the extension K'/k and the set S, then it also holds for the extension K/k and the set S.*

To prove the theorem, we need a preliminary lemma.

Lemma 6.3.2. *Let $k \subseteq K \subseteq K'$ be a tower of number fields with K'/k Abelian. Set $G' = \mathrm{Gal}\,(K'/k)$ and $G = \mathrm{Gal}\,(K/k)$. Let S be a set of places of k containing the Archimedean places and the prime ideals that ramify in K'/k. Let $W = |\mu|$ and $W' = |\mu'|$ be the cardinalities of the groups of roots of unity in K and K' respectively. If n is a divisor of W such that*

$$W'\theta_{K'/k,S} \in n\mathbb{Z}\,[G']\,,$$

then

$$W\theta_{K/k,S} \in n\mathbb{Z}\,[G]\,.$$

Proof. Set $\theta' = \theta_{K'/k,S}$ and $\theta = \theta_{K/k,S}$. Write

$$W'\theta' = \sum_{\sigma \in G'} a'_\sigma \sigma.$$

Let a'_1 be the coefficient of the identity map. For each σ in G', let N_σ be an integer satisfying

$$\sigma(\zeta) = \zeta^{N_\sigma}$$

for all roots of unity ζ in K'. Equation (6.3) implies that

$$a'_{\tau^{-1}} \equiv N_\tau a'_1 \pmod{W'}, \tag{6.5}$$

so we have

$$W'\theta' \equiv a'_1 \sum_{\sigma \in G'} N_\sigma \sigma^{-1} \pmod{W'\mathbb{Z}\,[G']}.$$

Since each integer N_σ is relatively prime to W', it follows that when the coefficients of θ' (or the L-function evaluator for any Abelian extension) are written in lowest terms, they all have the same denominator.

Now the inflation property of equivariant L-functions from Section 3.1 shows that the coefficient of the identity map in $W\theta$ is given by

$$a_1 = W \sum_{\substack{\sigma \in G' \\ \sigma|_K = \mathbf{1}}} \frac{a'_\sigma}{W'}.$$

The congruence (6.5) shows that

$$W \sum_{\substack{\sigma \in G' \\ \sigma|_K = \mathbf{1}}} \frac{a'_\sigma}{W'} \equiv \frac{W}{W'} a'_1 \sum_{\substack{\sigma \in G' \\ \sigma|_K = \mathbf{1}}} N_\sigma \pmod{W}. \tag{6.6}$$

Let

$$c = \sum_{\substack{\sigma \in G' \\ \sigma|_K = \mathbf{1}}} N_\sigma.$$

If ζ is a primitive W'th root of unity, then

$$\zeta^c = \left(\sum_{\substack{\sigma \in G' \\ \sigma_K = \mathbf{1}}} \sigma \right) \cdot \zeta = \mathrm{N}_{K'/K} \zeta.$$

It follows that c annihilates μ'/μ, so that $\frac{W'}{W}$ divides c. Equation (6.6) and the fact that n divides a'_1 then imply that n divides a_1. The lemma then follows from the fact that the denominators of the coefficients of θ when written in lowest terms are all identical. □

Proof of Theorem 6.3.1. Let $W = |\mu|$ and $W' = |\mu'|$ be the cardinalities of the groups of roots of unity in K and K' respectively. Let p^r be a prime power divisor of W, and assume that there exists a totally positive element ε in k whose p^rth root generates an unramified extension L of K of degree p^r. We must show that $W\theta_{K/k,S^{\min}}$ is in $p^r\mathbb{Z}[G]$. We assume that k is totally real and K is totally complex, since this is trivially true otherwise.

First, we will show that $L \cap K' = K$. Proposition 2.7.2 shows that L/k is a Galois extension. Set $\tilde{G} = \mathrm{Gal}\,(L/k)$, $G = \mathrm{Gal}\,(K/k)$, and $H = \mathrm{Gal}\,(L/K)$. Then $\tilde{G}$ is an extension of H by G, providing H with a $\mathbb{Z}[G]$-module structure. Since K'/k is Abelian, $L \cap K'/k$ is as well. Let

$$[L \cap K' \colon K] = p^s,$$

and let η be a fixed p^sth root of ε, and hence a generator of $L \cap K'$ over K. Let μ_{p^s} be the group of p^sth roots of unity in K. If α is in $\mathrm{Ann}_{\mathbb{Z}[G]}\, \mu_{p^s}$ and σ is in H, then there exists ζ in μ_{p^s} satisfying

$$\sigma\,(\eta) = \zeta\eta.$$

Using the fact that $L \cap K'$ is Abelian over k, we find that for any lift $\tilde{\alpha}$ of α to $\mathbb{Z}\left[\tilde{G}\right]$,

$$(\sigma - 1)\tilde{\alpha} \cdot \eta = \tilde{\alpha}(\sigma - 1) \cdot \eta = \tilde{\alpha} \cdot \zeta = 1.$$

Thus, $\tilde{\alpha} \cdot \eta$ is fixed by H, and hence, $\tilde{\alpha} \cdot \varepsilon$ is in $K^{\times p^s}$. We have found that

$$\mathrm{Ann}_{\mathbb{Z}[G]}\, \mu_{p^s} \cdot \varepsilon \in K^{\times p^s}. \tag{6.7}$$

(For a much more general result, see [10, Appendix, Lemma A.1.4]).

Let $\phi\colon K \hookrightarrow \mathbb{C}$ be an embedding of K into $\mathbb{C}$ with corresponding complex conjugation τ in G. Let ζ be a primitive p^rth root of unity in K. If $\tau(\zeta) = \zeta^a$, then $\zeta^{a^2} = \zeta$. Therefore,

$$a^2 \equiv 1 \pmod{p^r}.$$

It follows that $\tau(\zeta) = \zeta^{\pm 1}$. If $\tau(\zeta) = \zeta$, then

$$\phi^{-1}\left(\overline{\phi(\zeta)}\right) = \zeta,$$

so that $\phi(\zeta)$ is in $\mathbb{R}$. Since $p^r > 2$, this is a contradiction. Therefore, $\tau(\zeta) = \zeta^{-1}$. Equation (6.7) then shows that

$$(1 + \tau) \cdot \varepsilon \in \left(K^{\times}\right)^{p^s}$$

Since ε is in k, it follows that ε^2 is in $(K^{\times})^{p^s}$, and hence ε is in $K^{\times p^s}$. This says that $L \cap K' = K$ as claimed.

We have now determined that the composite field LK' is a cyclic extension of K' of degree p^r. It is generated over K' by the p^rth root of ε. Since L is an unramified extension of K, LK' is an unramified extension of K'. We now use the assumption that (H_p) holds for the extension K'/k. It follows that

$$W'\theta_{K'/k,S^{\min}} \in p^r\mathbb{Z}[G].$$

The theorem is now a consequence of Lemma 6.3.2. □

Remark. If there are prime ideals that ramify in K'/k but not in K/k, then the theorem does not imply that (H_p) for K'/k implies (H_p) for K/k, because the minimal allowed set of places of k for the extension K/k might be properly contained in the minimal set for K'/k.

6.4 Hayes's conjecture for Abelian extensions of prime conductor

This section is devoted to proving the following theorem.

Theorem 6.4.1. *Let K/k be an extension of number fields with $K/\mathbb{Q}$ Abelian of conductor p, where p is an odd prime number. If $\tilde{p}$ is an odd prime number, then $(\mathrm{H}_{\tilde{p}})$ holds for the extension K/k.*

The conjecture $(\mathrm{H}_{\tilde{p}})$ is trivial if K does not contain the $\tilde{p}$th roots of unity. We thus assume that $K = \mathbb{Q}(\zeta_p)$ and that $\tilde{p} = p$. We also assume that k is totally real, again since the conjecture is otherwise trivial. We set $d = [k\colon \mathbb{Q}]$. We set $G = \mathrm{Gal}(K/k)$. If k' is any subfield of K, then for each integer n prime to p, we let σ_n be the element of $\mathrm{Gal}(K/k')$ such that

$$\sigma_n(\zeta) = \zeta^n$$

for all pth roots of unity ζ. Finally, we assume that S is the set of places of $\mathbb{Q}$ consisting of the Archimedean place and the prime ideal (p). We abuse notation and use S also to denote the set of places in k lying above the places of S in $\mathbb{Q}$. For simplicity, we write θ in place of $\theta_{K/k,S}$.

In the first subsection, we will derive a congruence involving the coefficients of θ for such extensions and certain products of Bernoulli numbers. In the next subsection, we will prove the above theorem. Following that, we will provide a table of examples for which the conjecture is nontrivial. Finally, we will give a local result at the prime 2, which shows that any formulation of a local version Hayes's conjecture at the prime 2 will probably be trivially true for these extensions.

6.4.1 The key congruence

In this section, we will derive the following congruence for the cofficients of the L-function evaluator for the extension $\mathbb{Q}(\zeta_p)/k$:

Proposition 6.4.2. *Let n be an integer whose image in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a dth power.*

Let a_n be the coefficient of σ_n in $2p\theta$. Then

$$a_n \equiv (-1)^d 2dn^{-1} \prod_{l=1}^{d-1} \frac{B_{l\frac{p-1}{d}}}{\frac{p-1}{d}} \pmod{p}, \tag{6.8}$$

where the congruence is understood to be between elements of $\mathbb{Z}_p$.

Proof. Fix a primitive pth root of unity ζ_p. Let $G = \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_p\right)/k\right)$ and $\tilde{G} = \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_p\right)/\mathbb{Q}\right)$. Let g be a primitive root mod p, so that by identifying $\tilde{G}$ with $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$, G is generated by g^d. For $0 \leq i \leq p-2$, denote by $\tilde{\chi}_i$ the unique character on $\tilde{G}$ satisfying $\tilde{\chi}_i\left(\sigma_g\right) = \zeta_{p-1}^i$. Similarly, for $0 \leq i \leq \frac{p-1}{d} - 1$, let χ_i be the unique character on $\widehat{G}$ such that $\chi_i\left(\sigma_{g^d}\right) = \zeta_{p-1}^{id}$.

Now let $L = L_{\mathbb{Q}(\zeta_p)/\mathbb{Q},S}\left(s,\chi\right)$ be the S-incomplete Artin L-function associated with the extension $\mathbb{Q}\left(\zeta_p\right)/\mathbb{Q}$ and the character χ of a representation ρ of $\tilde{G}$ in a $\mathbb{C}$-vector space V. Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Q}\left(\zeta_p\right)$ lying above p. The inertia group $I_{\mathfrak{P}}$ is all of $\tilde{G}$, so that $V^{I_{\mathfrak{P}}} = V^{\tilde{G}}$. Let $\mathfrak{L}$ be the primitive Artin L-function associated with the extension $\mathbb{Q}\left(\zeta_p\right)/\mathbb{Q}$ and the representation ρ. The relationship between L and $\mathfrak{L}$ is given by equation (1.2):

$$L\left(s,\chi\right) = \det\left(1 - \rho\left(\sigma_{\mathfrak{P}}\right)\mathfrak{N}\left(\mathfrak{p}\right)^{-s}; V^{\tilde{G}}\right)\mathfrak{L}\left(s,\chi\right).$$

The dimension of $V^{\tilde{G}}$ is the number of times that the trivial representation appears in ρ. Choosing ρ to be an irreducible representation of G, so that $\chi = \tilde{\chi}_i$ for some i, we see that $V^{\tilde{G}} = 0$ unless ρ is the trivial representation. By convention, when $V^{\tilde{G}} = 0$ the above determinant is defined to be 1. If ρ is the trivial representation, then $\dim V^{\tilde{G}} = 1$ and the determinant is $1 - p^{-s}$.

By Proposition 2.2.1, for $0 \leq i \leq \frac{p-1}{d} - 1$, the character of the representation of $\tilde{G}$ induced by χ_i is

$$\mathrm{Ind}\,\chi_i = \sum_{\substack{\psi \in \tilde{G} \\ \mathrm{Res}\,\psi = \chi_i}} \psi = \sum_{l=0}^{d-1} \tilde{\chi}_{i+l\frac{p-1}{d}}.$$

The induction and additivity properties of Artin L-functions from Section 3.1 show that

$$L_{\mathbb{Q}(\zeta_p)/k,S}\left(0,\chi_i\right) = \prod_{i=0}^{d-1} L\left(0,\tilde{\chi}_{i+l\frac{p-1}{d}}\right).$$

Thus, if $1 \leq i \leq \frac{p-1}{d} - 1$, then

$$L_{\mathbb{Q}(\zeta_p)/k,S}(s, \chi_i) = \prod_{l=0}^{d-1} \mathfrak{L}\left(s, \tilde{\chi}_{i+l\frac{p-1}{d}}\right). \tag{6.9a}$$

In contrast, for the trivial character, we have

$$L_{\mathbb{Q}(\zeta_p)/k,S}(s, \chi_i) = \left(1 - p^{-s}\right) \prod_{l=0}^{d-1} \mathfrak{L}\left(s, \tilde{\chi}_{l\frac{p-1}{d}}\right). \tag{6.9b}$$

Let $\mathfrak{L}$ be the Dirichlet L-function corresponding to the Dirichlet character $\tilde{\chi}_j$ obtained by composing the $\tilde{\chi}_j$ with the Artin map. Since the conductor of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is $p\infty$ and $I_{\mathfrak{P}} = \tilde{G}$, Proposition 3.1.1 shows that for $1 \leq j \leq p-2$,

$$\mathfrak{L}(s, \tilde{\chi}_j) = \mathfrak{L}(s, \tilde{\chi}_j).$$

On the other hand, for the character of the trivial representation $\tilde{\chi}_0$, we have

$$\mathfrak{L}(s, \tilde{\chi}_0) = \zeta(s),$$

where ζ is the Riemann zeta function.

For $1 \leq i \leq \frac{p-1}{d} - 1$, setting $s = 0$ in (6.9a) and substituting in the well-known values of the Dirichlet L-functions [38, Chapter VII, Theorem 2.9] yields

$$L_{\mathbb{Q}(\zeta_p)/k,S}(0, \chi_i) = \prod_{l=0}^{d-1} -B_{1,\tilde{\chi}_{i+l\frac{p-1}{d}}} \tag{6.10a}$$

and from (6.9b), we find that

$$L_{\mathbb{Q}(\zeta_p)/k,S}(0, \chi_0) = 0. \tag{6.10b}$$

We can use these values to calculate $2p\theta$. By definition,

$$\begin{aligned} 2p\,\theta &= 2p \sum_{\chi \in \widehat{G}} L_{\mathbb{Q}(\zeta_p)/k,S}(0, \overline{\chi})\, e_{\chi} \\ &= 2p \sum_{i=1}^{\frac{p-1}{d}-1} \prod_{l=0}^{d-1} -B_{1,\tilde{\chi}_{i+l\frac{p-1}{d}}}\, e_{\overline{\chi_i}} \\ &= \frac{2p}{\frac{p-1}{d}} \sum_{\sigma \in G} \sum_{i=1}^{\frac{p-1}{d}-1} \chi_i(\sigma) \prod_{l=0}^{d-1} -B_{1,\tilde{\chi}_{i+l\frac{p-1}{d}}}\, \sigma. \end{aligned}$$

We now embed $\mathbb{Q}(\zeta_{p-1})$ into $\mathbb{Q}_p$ by mapping ζ_{p-1} to the unique $(p-1)$th root of unity congruent to $g \bmod p$, where g is our fixed primitive root mod p. For $0 \leq j \leq p-2$, composing $\tilde{\chi}_j$ with this embedding produces the character ω^j, where ω is the Teichmüller character. For $1 \leq i \leq \frac{p-1}{d} - 1$, composing χ_i with this embedding produces the restriction of ω^i to the subgroup $\left((\mathbb{Z}/p\mathbb{Z})^\times\right)^d$. The image of a_n under the embedding in $\mathbb{Q}_p$ is

$$a_n = \frac{2p}{\frac{p-1}{d}} \sum_{i=1}^{\frac{p-1}{d}-1} \omega^i(\sigma_n) \prod_{l=0}^{d-1} -B_{1,\omega^{i+l\frac{p-1}{d}}}. \tag{6.11}$$

It follows from the form of the power series expansion at $s = 1$ of the p-adic L-functions corresponding to powers of ω (see [60, Corollary 5.15]) that

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \pmod{p}, \qquad \text{for } n \not\equiv -1 \pmod{p-1},$$

and both sides of this congruence are p-integral. Also, if t is an integer such that $n \equiv g^{td} \mod p$, then

$$\omega^i(\sigma_n) \equiv g^{itd} \pmod{p}.$$

Finally,

$$pB_{1,\omega^{p-2}} \equiv p - 1 \pmod{p}.$$

Using these congruences, equation (6.11) becomes

$$\begin{aligned} a_n &\equiv (-1)^d \omega^{\frac{p-1}{d}-1}(\sigma_n) \frac{2p}{\frac{p-1}{d}} B_{1,\omega^{p-2}} \prod_{l=1}^{d-1} \frac{B_{l\frac{p-1}{d}}}{\frac{p-1}{d}} \pmod{p} \\ &\equiv (-1)^d 2 g^{td\left(\frac{p-1}{d}-1\right)} d \prod_{l=1}^{d-1} \frac{B_{l\frac{p-1}{d}}}{\frac{p-1}{d}} \pmod{p} \\ &\equiv (-1)^d 2 d n^{-1} \prod_{l=1}^{d-1} \frac{B_{l\frac{p-1}{d}}}{\frac{p-1}{d}} \pmod{p}. \end{aligned}$$

□

6.4.2 The p-primary part of Hayes's conjecture

In this subsection, we will prove Theorem 6.4.1. Then we will consider the converse.

Proof of Theorem 6.4.1. Let H_p be the p-Hilbert class field of K. Let

$$L = K\left(\sqrt[p]{U_k^+}\right) \text{ and } F = H_p \cap L.$$

Set $\mathcal{H} = \mathrm{Gal}\,(H_p/K)$, $\mathcal{L} = \mathrm{Gal}\,(L/K)$, and $\mathcal{F} = \mathrm{Gal}\,(F/K)$. By Propositions 2.7.2 and 2.7.5, L and H_p are normal over $\mathbb{Q}$, and hence, F is as well. We set $\tilde{\mathcal{L}} = \mathrm{Gal}\,(L/\mathbb{Q})$, $\tilde{\mathcal{H}} = \mathrm{Gal}\,(H_p/\mathbb{Q})$, $\tilde{\mathcal{F}} = \mathrm{Gal}\,(F/\mathbb{Q})$, and $\tilde{G} = \mathrm{Gal}(K/\mathbb{Q})$. The groups $\tilde{\mathcal{L}}$, $\tilde{\mathcal{H}}$, and $\tilde{\mathcal{F}}$ are extensions of the groups $\mathcal{L}$, $\mathcal{H}$, and $\mathcal{F}$ respectively by $\tilde{G}$. Each is therefore provided with the structure of a $\mathbb{Z}\left[\tilde{G}\right]$-module through the action defined in Section 2.7. We denote the p-primary part of the ideal class group of K by Cl_p. Proposition 2.7.5 shows that the Artin map gives an isomorphism of $\mathbb{Z}\left[\tilde{G}\right]$-modules

$$\mathrm{Cl}_p \cong \mathcal{H}.$$

Since $\mathcal{L}$ is Abelian of exponent p, $\mathcal{F}$ is also abelian of exponent p. By Kummer theory there is a unique subgroup $\Delta \subset U_k^+ K^{\times p}$ containing $K^{\times p}$ such that

$$F = K\left(\sqrt[p]{\Delta}\right).$$

Since F is normal over $\mathbb{Q}$, Proposition 2.7.2 shows that $\tilde{G}$ acts on Δ, and hence, on $\Delta/K^{\times p}$. Let μ_p be the group of pth roots of unity. As each of $\mathcal{F}$, $\Delta/K^{\times p}$, and μ_p has exponent p, they are $\mathbb{Z}_p\left[\tilde{G}\right]$-modules. Proposition 2.7.3 shows that the Kummer pairing

$$\mathcal{F} \times \Delta/K^{\times p} \to \mu_p$$

is $\tilde{G}$-equivariant. Furthermore, it induces a $\mathbb{Z}_p\left[\tilde{G}\right]$-module isomorphism

$$\mathcal{F} \cong \mathrm{Hom}\left(\Delta/K^{\times p}, \mu_p\right), \tag{6.12}$$

where $\tilde{G}$ acts on $\mathrm{Hom}\,(\Delta/K^{\times p}, \mu_p)$ by

$$(\tilde{g} \cdot f)\left(\overline{\delta}\right) = \tilde{g} f\left(\tilde{g}^{-1}\overline{\delta}\right).$$

As the order of $\tilde{G}$ is relatively prime to p, the $\mathbb{Z}_p\left[\tilde{G}\right]$-modules in the above isomorphism split into isotypic components as in Proposition 2.3.1. The above isomorphism induces isomorphisms between corresponding components. Also, $\Delta/K^{\times p}$

and μ_p split into the direct sums of their isotypic components, and in fact, if ω denotes the Teichmüller character of $\tilde{G}$, then $\mu_p = \mu_p^{\omega}$. We have

$$\begin{aligned}\bigoplus_{\chi} \left(\mathrm{Hom}\left(\Delta/K^{\times p}, \mu_p\right)\right)^{\chi} &\cong \mathrm{Hom}\left(\Delta/K^{\times p}, \mu_p\right) \\ &\cong \mathrm{Hom}\left(\bigoplus_{\chi} \left(\Delta/K^{\times p}\right)^{\chi}, \mu_p\right) \\ &\cong \bigoplus_{\chi} \mathrm{Hom}\left(\left(\Delta/K^{\times p}\right)^{\chi}, \mu_p\right). \qquad (6.13)\end{aligned}$$

Now choose

$$f \in \mathrm{Hom}\left(\left(\Delta/K^{\times p}\right)^{\chi} \mu_p\right),\ \sigma \in \tilde{G},\ \text{and } \overline{\delta} \in \left(\Delta/K^{\times p}\right)^{\chi}.$$

Note that since $(\Delta/K^{\times p})^{\chi}$ and μ_p both have exponent p, f is a homomorphism of $\mathbb{Z}_p$-modules. Then

$$(\sigma \cdot f)\left(\tilde{\delta}\right) = \sigma f\left(\sigma^{-1}\tilde{\delta}\right) = \sigma f\left(\chi^{-1}(\sigma)\,\tilde{\delta}\right) = \chi^{-1}(\sigma)\,\sigma f\left(\tilde{\delta}\right) = \chi^{-1}\omega(\sigma)\, f\left(\tilde{\delta}\right).$$

Thus, the component $\mathrm{Hom}\left(\left(\Delta/K^{\times p}\right)^{\chi}, \mu_p\right)$ on the right side of (6.13) corresponds under the isomorphism to a subgroup of the component $\left(\mathrm{Hom}\left(\Delta/K^{\times p}, \mu_p\right)\right)^{\chi^{-1}\omega}$ on the left side of (6.13). Since the groups involved are finite, it follows that

$$\mathrm{Hom}\left(\left(\Delta/K^{\times p}\right)^{\chi}, \mu_p\right) \cong \mathrm{Hom}\left(\Delta/K^{\times p}, \mu_p\right)^{\chi^{-1}\omega}. \qquad (6.14)$$

Assume that there exists an element ε in k whose pth root generates an unramified extension of $\mathbb{Q}(\zeta_p)$ of degree p. Then p divides $|\mathcal{F}|$, so p divides $|F^{\chi}|$ for some character χ of $\tilde{G}$. From the isomorphism (6.12), we find that

$$\left(\mathrm{Hom}\left(\Delta/K^{\times p}, \mu_p\right)\right)^{\chi} \neq 0.$$

Hence, by (6.14),

$$\left(\Delta/K^{\times p}\right)^{\chi^{-1}\omega} \neq 0.$$

Since $\Delta \subset U_k^{+} K^{\times p}$, the group $\Delta/K^{\times p}$ is fixed by G. Thus, in the decomposition of $\Delta/K^{\times p}$ as a direct sum of isotypic components, the components corresponding to characters which are nontrivial on G are zero. It follows that

$$\chi^{-1}\omega\,\big|_{G} = \mathrm{id}.$$

Therefore, $\chi^{-1}\omega = \omega^{l\frac{p-1}{d}}$ for some l with $0 \leq l \leq d-1$, and so

$$\chi = \omega^{p-l\frac{p-1}{d}}.$$

Now $\mathcal{F}$ is isomorphic to a quotient group $\mathcal{H}/\mathcal{H}'$. Furthermore, since F is normal over $\mathbb{Q}$, $\mathcal{H}'$ is stable under the action of $\tilde{G}$ on $\mathcal{H}$, and thus $\mathcal{H}/\mathcal{H}'$ is a quotient of $\tilde{G}$-modules. One can check that $\mathcal{H}/\mathcal{H}' \cong \mathcal{F}$ is an isomorphism of $\mathbb{Z}_p\left[\tilde{G}\right]$-modules. If χ is a character on $\tilde{G}$, we set e_χ to be the idempotent of $\mathbb{Z}_p\left[\tilde{G}\right]$ defined as in Section 2.3. Then one has

$$\mathcal{F}^\chi = e_\chi\mathcal{F} \cong e_\chi\mathcal{H}/e_\chi\mathcal{H} \cap \mathcal{H}' = \mathcal{H}^\chi/\mathcal{H}'^\chi.$$

Thus, $\mathcal{F}^\chi$ is isomorphic to a quotient of Cl_p^χ through the Artin map. Since p divides $|\mathcal{F}^\chi|$, p also divides $\left|\mathrm{Cl}_p^\chi\right|$. By Herbrand's theorem [60, Theorem 6.17], this implies that p divides $B_{l\frac{p-1}{d}}$. Finally, it follows from (6.8) that p divides each coefficient a_n of $2p\theta$. In other words,

$$W\theta \in p\mathbb{Z}\left[G\right],$$

which proves (H_p). □

The crucial element of the preceding proof was Herbrand's theorem. As the converse of Herbrand's theorem is true, one might ask if the converse of (H_p) holds as well.

Theorem 6.4.3. *Let k be a totally real subfield of $K = \mathbb{Q}(\zeta_p)$. Assume that p does not divide the class number of K^+. If p divides the coefficients of $2p\theta$, then there exists a unit ε in k such that $K(\sqrt[p]{\varepsilon})$ is unramified over K. In fact, this unit may be chosen to be the relative norm of a cyclotomic unit.*

Proof. By (6.8), there exists an integer l with $0 \leq l \leq d-1$ such that $p \mid B_{l\frac{p-1}{d}}$. This condition implies there is a unit $\varepsilon \in k$ which is the relative norm of a cyclotomic unit of K such that $K(\sqrt[p]{\varepsilon})$ is unramified over K (see [37, Theorem 1] or [60, Exercise 8.9]). Moreover, if Vandiver's conjecture is true for p, then this extension is nontrivial. □

Herbrand ([27]) proved the converse to his theorem under the assumption of Vandiver's conjecture. More recently, Ribet ([44]) proved it in full generality using modular forms and algebraic geometry. Finally, there is a purely arithmetic proof that uses Euler systems ([60, Theorem 15.8]). Thus, the converse to Herbrand's theorem has the potential to allow a proof of a refinement of Theorem 6.4.3 by removing the assumption that p does not divide the class number of K^+. However, if Vandiver's conjecture fails for the prime p, the Euler systems proof of the converse to Herbrand's theorem does not give information about specific generators of unramified Kummer extensions of $\mathbb{Q}(\zeta_p)$. Theorem 1.2 in [44] shows that regardless of whether Vandiver's conjecture holds, if $2n = r\frac{p-1}{d}$ and p divides B_{2n}, then there is an unramified degree p extension of the subfield k' of K of degree $\frac{p-1}{(p-1,n-1)}$ over $\mathbb{Q}$. Again, it does not seem that this gives enough information to determine that there are unramified extensions of K generated either by pth roots of elements of k or generated by pth roots of units.

However, we may "reverse" the first part of the proof of Theorem 6.4.1 using the converse to Herbrand's theorem to give some information in this direction. The notation is that of subsection 6.4.2. If p divides the coefficients a_n of $2p\theta$, then the congruence (6.8) shows that there exists an integer l with $0 \leq l \leq d-1$ for which p divides $B_{l\frac{p-1}{d}}$. Let $\chi = \omega^{p-l\frac{p-1}{d}}$. By the converse to Herbrand's theorem, it follows that p divides $\left|\mathrm{Cl}_p^{\chi}\right|$, and hence, p divides $|(\mathcal{H}/p\mathcal{H})^{\chi}|$. Let H' denote the subfield of H_p fixed by $p\mathcal{H}^{\chi}$, so H' is a nontrivial Kummer extension of K. Let Δ be the subgroup of $K^{\times}$ containing $K^{\times p}$ that corresponds to H' by Kummer theory. By Proposition 2.7.3, the Kummer pairing induces a duality:

$$\Delta/K^{\times p} \cong \mathrm{Hom}\left(\left(\mathcal{H}/p\mathcal{H}\right)^{\chi}, \mu_p\right).$$

Since $(\mathcal{H}/p\mathcal{H})^{\chi}$ is nontrivial, $\Delta \neq K^{\times p}$. Since $p\mathcal{H}^{\chi}$ is a $\tilde{G}$-submodule of $\mathcal{H}$, H' is normal over $\mathbb{Q}$. Thus, by Proposition 2.7.2, Δ is a $\tilde{G}$-submodule of $K^{\times}$. Furthermore, the above isomorphism is an isomorphism of $\tilde{G}$-modules. There is an isomorphism, similar to that of (6.13):

$$\bigoplus_{\chi} \left(\mathrm{Hom}\left(\left(\mathcal{H}/p\mathcal{H}\right), \mu_p\right)\right)^{\chi} \cong \bigoplus_{\chi} \mathrm{Hom}\left(\left(\mathcal{H}/p\mathcal{H}\right)^{\chi}, \mu_p\right).$$

Choose

$$f \in \mathrm{Hom}\left((\mathcal{H}/p\mathcal{H})^{\chi}, \mu_p\right), \ \sigma \in \tilde{G}, \text{ and } \overline{\tau} \in (\mathcal{H}/p\mathcal{H})^{\chi}.$$

We consider f to be a homomorphism of $\mathbb{Z}_p$-modules. Then

$$(\sigma \cdot f)(\overline{\tau}) = \sigma f\left(\sigma^{-1}\overline{\tau}\right) = \sigma f\left(\chi^{-1}(\sigma)\overline{\tau}\right) = \chi^{-1}(\sigma)\sigma f(\overline{\tau}) = \chi^{-1}\omega(\sigma) f(\overline{\tau}).$$

Thus, there is an isomorphism

$$\mathrm{Hom}\left((\mathcal{H}/p\mathcal{H})^{\chi}, \mu_p\right) \cong \mathrm{Hom}\left(\mathcal{H}/p\mathcal{H}, \mu_p\right)^{\chi^{-1}\omega}.$$

Since $\chi^{-1}\omega = \omega^{l\frac{p-1}{d}}$, we have

$$\chi^{-1}\omega \,\big|_G = \mathbf{1}.$$

Thus, G acts trivially on $\mathrm{Hom}\left((H/pH)^{\chi}, \mu_p\right)$, and hence, on $\Delta/K^{\times p}$.

Since $\Delta \neq K^{\times p}$, we may choose an element δ in $\Delta \setminus K^{\times p}$. If σ generates G, we have

$$\sigma\delta = \alpha^p\delta$$

for some α in K. Applying σ to both sides $\frac{p-1}{d} - 1$ more times, we find that

$$\delta = N_{K/k}(\alpha)^p\delta,$$

so that

$$N_{K/k}(\alpha) = 1.$$

By Hilbert's Theorem 90 ([24, Theorem 90, :-)]), there exists β in K such that

$$\alpha = \frac{\sigma\beta}{\beta},$$

and hence,

$$\sigma\frac{\delta}{\beta^p} = \frac{\delta}{\beta^p}.$$

Therefore,

$$\frac{\delta}{\beta^p} \in \left(\Delta \setminus K^{\times p}\right) \cap k,$$

and so $\frac{\delta^2}{\beta^{2p}}$ is a totally positive element of k whose pth root generates an unramified Kummer extension of K. Proposition 2.5.2 shows that the valuation of $\frac{\delta^2}{\beta^{2p}}$ at every finite prime of K relatively prime to p is divisible by p, but it does not seem to follow immediately that there is a totally positive *unit* in $(\Delta/K^{\times p}) \cap k$. To summarize, we have the following supplement to Theorem 6.4.1:

Theorem 6.4.4. *Without assuming Vandiver's conjecture, it is still true that if*

$$2p\theta \in p\mathbb{Z}\left[G\right],$$

then there is a totally positive element of k whose pth root generates a nontrivial Kummer extension of K. If Vandiver's conjecture holds, then this element can be chosen to be a unit.

6.4.3 Examples

Theorem 6.4.1 immediately provides many nontrivial examples of Hayes' conjecture. Given any irregular prime p such that Vandiver's conjecture holds, if p divides B_{2n} with $2 \leq 2n \leq p-3$, then there exists an extension $\mathbb{Q}\left(\zeta_p\right)/k$ with k totally real for which B_{2n} appears in the product (6.8). For instance, we may set $k = \mathbb{Q}\left(\zeta_p\right)^+$. Theorem 6.4.3 implies that there exists an element of k whose pth roots generate a nontrivial unramified extension of $\mathbb{Q}\left(\zeta_p\right)$. Theorem 6.4.1 then shows that p divides the coefficients of $2p\theta_{\mathbb{Q}(\zeta_p)/k}$, providing a nontrivial example of (H_p). However, computing examples reveals that for many irregular primes, $\mathbb{Q}\left(\zeta_p\right)^+$ is the minimal such k, and for most irregular primes, the smallest such k seems to have relatively large degree over $\mathbb{Q}$. Searching for examples of k with small degree over $\mathbb{Q}$ such that p divides the coefficients of $2p\theta_{\mathbb{Q}(\zeta_p)/k}$ provides some interesting results. If p is an irregular prime with p dividing B_{2n}, set

$$d_{p,n} = \frac{p-1}{(p-1, 2n)}.$$

Since p divides B_{2n}, the subfield k of $K = \mathbb{Q}\left(\zeta_p\right)$ of degree $d_{p,n}$ over $\mathbb{Q}$ is the smallest field for which the congruence (6.8) implies that p divides a_n. If the index of irregularity of p is 2 or greater, there can be many minimal subfields of K for which $p \mid e_S\left(K/k\right)$. The following table was computed using a script written by my brother Owen Smith to search through Joe Buhler's table of irregular primes up to 16777213 for primes for which $d_{p,n} \leq 25$:

Notice that for a prime p and Bernoulli number B_{2n} as above, $d_{p,n} = 2$ if and only if $n = \frac{p-1}{4}$. In this case, $p \equiv 1 \pmod 4$ and $p \mid B_{\frac{p-1}{2}}$. Kiselev ([29]) and Ankeny-Artin-Chowla ([1]) independently showed that p divides $B_{\frac{p-1}{2}}$ if and only

Table 6.1: Irregular prime numbers p with small $d_{p,n}$

$d_{p,n}$	p
3	5479, 15646243
5	130811
7	421, 44563
9	37, 13411
13	90247, 163307
14	633473
15	1446901
17	103, 3484729
19	43093, 3962603
20	2441, 9041
22	9901
23	4003, 52579, 376097
24	6801313
25	101, 166301, 345601

if p divides u, where $\frac{t+u\sqrt{p}}{2} > 1$ is the fundamental unit of $\mathbb{Q}\left(\sqrt{p}\right)$. Furthermore, the Ankeny-Artin-Chowla conjecture asserts that p never divides u. The previous discussion shows that this conjecture is equivalent to the statement that $d_{p,n} \neq 2$ for all irregular primes p and Bernoulli numbers B_{2n}. A glance at the above table reveals that, in fact, many small even numbers are absent as values of $d_{p,n}$ for $p \leq 16777213$. It would be interesting to know if there is some unknown factor which forces small even values of $d_{p,n}$ to occur only for very large values of p. On the other hand, perhaps the Ankeny-Artin-Chowla conjecture can be strengthened to say that some additional small even numbers are not possible values of $d_{p,n}$. Finally, it would be interesting to know if $d_{p,n}$ can ever take the odd values 11 or 21, which seem conspicuously absent from this list.

6.4.4 The 2-primary part of Hayes' Conjecture

Let k be a totally real subfield of $K = \mathbb{Q}(\zeta_p)$. Let S be the set consisting of the Archimedean places of $\mathbb{Q}$ and the prime ideal (p). We abuse notation by using S to denote the set of places of k lying above the places of S in $\mathbb{Q}$. In this section, we will prove the following theorem.

Theorem 6.4.5. *If $k \neq \mathbb{Q}$, then*

$$2p\theta_{K/k,S} \in 2\mathbb{Z}\left[G\right].$$

We will use the notation of Subsection 6.4.1.

Proof. The partial zeta functions for the extension $K/\mathbb{Q}$ are the Hurwitz zeta functions, whose special values at negative integers have long been known. Using these values, we find that

$$\theta_{K/\mathbb{Q},\tilde{S}} = \sum_{a=1}^{p-1} \left(\frac{1}{2} - \frac{a}{p}\right) \sigma_a^{-1}.$$

For each character χ on $\tilde{G}$, let t_χ be the twist by χ from Section 2.3. It is the endomorphism of $\mathbb{C}\left[\tilde{G}\right]$ defined by

$$t_\chi\left(\sum_{a=1}^{p-1} c_a\sigma_a\right) = \sum_{a=1}^{p-1} c_a\chi\left(\sigma_a\right)\sigma_a.$$

Property 3 of equivariant L-functions shows that

$$\theta_{K/k,S} = \prod_{\substack{\chi\in\widehat{\tilde{G}}\\ \chi(G)=\mathbf{1}}} t_\chi\left(\theta_{K/\mathbb{Q},\tilde{S}}\right).$$

Thus,

$$\theta = \prod_{i=0}^{d-1}\left(\sum_{a=1}^{p-1}\left(\frac{1}{2}-\frac{a}{p}\right)\tilde{\chi}_{i^{\frac{p-1}{d}}}\left(\sigma_a^{-1}\right)\sigma_a^{-1}\right),$$

and hence,

$$a_1 = 2p\sum_{\substack{1\leq c_0,\ldots,c_{d-1}\leq p-1\\ c_0c_1\cdots c_{d-1}\equiv 1 \bmod p}}\prod_{i=0}^{d-1}\left(\frac{1}{2}-\frac{c_i}{p}\right)\tilde{\chi}_{i^{\frac{p-1}{d}}}\left(\sigma_{c_i}^{-1}\right). \tag{6.15}$$

We will now need the following lemma.

Lemma 6.4.6. *Let $r \geq 2$ and let $\chi_0, \ldots, \chi_{r-1}$ be distinct even Dirichlet characters mod p. Let t be such that $0 \leq t \leq r$. If $1 \leq t \leq r$, let $\widehat{n} = (n_1, \ldots, n_t)$ be a t-tuple of integers with $0 \leq n_1 < \cdots < n_t \leq r-1$. If $t = 0$, let $\widehat{n}$ be the empty set. Set*

$$s_{\widehat{n}} = \sum_{\substack{1\leq c_0,\ldots,c_{r-1}\leq p-1\\ c_0c_1\cdots c_{r-1}\equiv 1 \bmod p}}\prod_{j=1}^{t} c_{n_j}\prod_{i=0}^{r-1}\chi_i\left(c_i\right),$$

where it is understood that the first product is 1 *if* $t = 0$. *Then* $t < r$ *implies* $s_{\widehat{n}} = 0$.

Proof. The proof will be by induction on t. Throughout this proof, given an integer a prime to p, a^{-1} will denote an integer inverse to a mod p. For $t = 0$,

$$\begin{aligned} s_{\widehat{n}} &= \sum_{\substack{1 \le c_0,\ldots,c_{r-1} \le p-1 \\ c_0 c_1 \cdots c_{r-1} \equiv 1 \bmod p}} \prod_{i=0}^{r-1} \chi_i(c_i) \\ &= \sum_{c_0=1}^{p-1} \cdots \sum_{c_{r-2}=1}^{p-1} \prod_{i=0}^{r-2} \chi_i(c_i)\, \chi_{r-1}\left(\prod_{i=0}^{r-2} c_i^{-1}\right) \\ &= \sum_{c_0=1}^{p-1} \cdots \sum_{c_{r-2}=1}^{p-1} \prod_{i=0}^{r-2} \chi_i \chi_{r-1}^{-1}(c_i) \\ &= \prod_{i=0}^{r-2} \left(\sum_{c_i=1}^{p-1} \chi_i \chi_{r-1}^{-1}(c_i) \right). \end{aligned}$$

None of the characters $\chi_i \chi_{r-1}^{-1}$ is the trivial character since the χ_i's were assumed to be distinct characters. Thus, by the orthogonality relations for characters, each of the above sums is 0. The lemma thus holds when $t = 0$. Now assume that it holds for some particular value $t - 1$ where $t < r$, so the statement of the proposition for t is nontrivial. Then at least one of the integers between 0 and $r - 1$ is not in the list of numbers $n_1, \ldots, n_t$, so assume without loss of generality that one such integer is $r - 1$. Then we have

$$\begin{aligned} s_{\widehat{n}} &= \sum_{\substack{1 \le c_0,\ldots,c_{r-1} \le p-1 \\ c_0 c_1 \cdots c_{r-1} \equiv 1 \bmod p}} \prod_{j=1}^{t} c_{n_j} \prod_{i=0}^{r-1} \chi_i(c_i) \\ &= \sum_{c_0=1}^{p-1} \cdots \sum_{c_{r-2}=1}^{p-1} \prod_{j=1}^{t} c_{n_j} \prod_{i=0}^{r-2} \chi_i \chi_{r-1}^{-1}(c_i), \end{aligned}$$

where rewriting the sum in this way is possible because c_{r-1} does not appear as one of the c_{n_j}'s. Now since all of the characters were assumed to be even, replacing c_{n_1} by $p - c_{n_1}$ in the above multiple sum gives us

$$\begin{aligned} s_{\widehat{n}} &= p \sum_{c_0=1}^{p-1} \cdots \sum_{c_{r-2}=1}^{p-1} \prod_{j=2}^{t} c_{n_j} \prod_{i=0}^{r-2} \chi_i \chi_{r-1}^{-1}(c_i) - s_{\widehat{n}} \\ &= p s_{\widehat{m}} - s_{\widehat{n}} \end{aligned}$$

where $\widehat{m}$ is the $(t-1)$-tuple formed by removing n_1 from the t-tuple $\widehat{n}$. By the induction hypothesis, $s_{\widehat{m}} = 0$, so we find that $s_{\widehat{n}} = 0$. □

We return now to our expression (6.15). The expansion of each product appearing there yields a sum of terms where for some of the integers i with $0 \leq i \leq d-1$, the $\frac{c_i}{p}$ term is chosen in the corresponding term in the product, while for the other integers i, the $\frac{1}{2}$ term is chosen. We may split the sum into subsums whereby one chooses a t-tuple $\widehat{n}$ with $0 \leq t \leq d$ and then forms the subsum consisting of those terms formed by choosing the $\frac{c_i}{p}$ from those terms where i is one of the numbers appearing in $\widehat{n}$ and choosing the $\frac{1}{2}$ from the rest. Then viewing the characters $\tilde{\chi}_{i^{\frac{p-1}{d}}}$ as distinct even Dirichlet characters mod p, we find that each of these subsums is a constant multiple of the sum $s_{\widehat{n}}$ appearing in the proposition. Thus, if $d \geq 2$, all of these subsums are zero except for the one formed by choosing $\widehat{n}$ to be the d-tuple $(0, \ldots, d-1)$. It follows that

$$a_1 = (-1)^d 2p \sum_{\substack{1 \leq c_0, \ldots, c_{d-1} \leq p-1 \\ c_0 c_1 \cdots c_{d-1} \equiv 1 \bmod p}} \prod_{i=0}^{d-1} \tilde{\chi}_{i^{\frac{p-1}{d}}}\left(\sigma_{c_i}^{-1}\right) \frac{c_i}{p}$$

Since a_1 is a rational integer, one sees immediately from this expression that it is an even integer. □

Remark. Sands mentions in [47, proof of Proposition 4.2] that for $d \geq 3$, the fact that a_1 is even follows from similar arguments to the ones he gives for proving integrality properties of θ.

6.5 A numerical counterexample

In this section, we will provide a counterexample to the strong version of Hayes's conjecture from section 3.5, which is the unpublished version given in [25]. Although no counterexample has been found to the first statement of the conjecture, the following example shows that the second statement claiming that (B) holds with $W\theta$ replaced by $\frac{W}{e}\theta$ is false. All of the computations in this section were performed with PARI/GP, and none of them were substantiated by theoretical work.

Let $k = \mathbb{Q}\left(\sqrt{113}\right)$ and $K = k\left(\zeta_3\right)$. Let S be the minimal allowed set, which in this case consists of the Archimedean places of k and the sole prime in k dividing 3. With these choices, $h_{k,S} = 1$ and $h_{K,S} = 3$. Tate's expression (4.2) for $W_K\theta$ in this case is

$$6\theta = 6(1 - \tau),$$

where τ denotes complex conjugation. The extension L of K obtained by adjoining the cube root of a fundamental unit of k has relative discriminant 1. Since both of L and K are totally complex, L is contained in the Hilbert class field H_K of K. Thus, the exponent of the Galois group of the intersection of L and H_K is 3. This divides the coefficients of 6θ, which is the statement of (H_3).

Next, if we remove the factor of 3 from 6θ, we are left with $2(1 - \tau)$. The second statement of the strong version of Hayes's conjecture predicts that this should annihilate the class group of K. However, the class group of K has order 3, and since the class group of k is trivial, the minus part of the class group of K has order 3. Thus, multiplying these classes by $2(1 - \tau)$ has the effect of multiplying by 4. Hence, $2(1 - \tau)$ does not annihilate the class group of K.

Two remarks are in order. First, as mentioned in Section 3.5, Hayes's initial statement of this conjecture included the assumption that K contains the narrow Hilbert class field of k. This condition is also satisfied by this example. To see this, observe that since 113 is prime and congruent to 1 mod 4, a fundamental unit u of k has norm negative 1. Thus, u and its conjugate have different signs. Assume that the signature of u under the two embeddings of k in $\mathbb{R}$ is $(1, -1)$. Choose a generator γ for a principal ideal of k. If γ has signature $(1, -1)$, $(-1, 1)$,

or $(-1,-1)$, then $u\gamma$, $-u\gamma$ or $-\gamma$ respectively will be a totally positive generator for (γ). Thus, the narrow ideal class group of k is the same as the ordinary ideal class group. Since $h_k = 1$, the narrow Hilbert class field of k is k itself.

The second remark is that the version of Hayes's conjecture presented in [26] includes the assumption that the prime p in (H_p) has a prime divisor in k that does not ramify in K/k. This condition is not satisfied by the prime 3 in this example.

References

[1] N. C. Ankeny, E. Artin, and S. Chowla, *The class-number of real quadratic fields*, Annals of Mathematics **56** (1952), 479–493.

[2] D. Barsky, *Fonctions zeta p-adiques d'une classe de rayon des corps de nombres totalement réels*, Groupe d'Étude d'Analyse Ultramétrique **5e année** (1977/1978), no. 16, 23 p. (French).

[3] A. J. Berrick and M. E. Keating, *An introduction to rings and modules with k-theory in view*, Cambridge Studies in Advanced Mathematics, vol. 65, Cambridge University Press, Cambridge-New York-Melbourne-Madrid, 2000.

[4] J. W. S. Cassels and A. Frölich (eds.), *Algebraic number theory: Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union*, Academic press Inc. (London) Ltd, 1967.

[5] P. Cassou-Noguès, *Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques*, Inventiones mathematicae **51** (1979), 29–59 (French).

[6] J. Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic Number Fields (L-Functions and Galois properties): Proceedings of a Symposium organised by the London Mathematical Society with the support of the Science Research Council and the Royal Society (A. Frölich, ed.), Academic Press Inc. (London) Ltd., 1977, held at the University of Durham, pp. 269–353.

[7] J. Coates and A. Wiles, *Kummer's criterion for Hurwitz numbers*, Algebraic number theory; papers contributed for the Kyoto international symposium (Tokyo) (S. Iyanaga, ed.), Japan Society for the Promotion of Science, 1977.

[8] P. Deligne and K. A. Ribet, *Values of L-functions at negative integers over totally real fields*, Inventiones mathematicae **59** (1980), 227–286.

[9] D. S. Dummit, J. W. Sands, and B. Tangedal, *Stark's Conjecture in multiquadratic extensions, revisited*, Journal de Théorie des Nombres de Bordeaux **15** (2003), no. 1, 83–97.

[10] C. Emmons, *Higher order integral Stark-type conjectures*, Ph.D. thesis, University of California, San Diego, 2006.

[11] A. Frölich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge-New York-Melbourne, 1991.

[12] G. Gras, *Class field theory: From theory to practice*, Springer-Verlag, Berlin-Heidelberg, 2003, translated from the original French manuscript by Henri Cohen.

[13] R. Greenberg, *A generalization of Kummer's criterion*, Inventiones mathematicae **21** (1973), 247–254.

[14] C. Greither, *Some cases of Brumer's conjecture for abelian CM extensions of totally real fields*, Mathematische Zeitschrift **233** (2000), 515–534.

[15] ———, *Arithmetic annihilators and Stark-type conjectures*, Stark's Conjectures: Recent Work and New Directions, Contemporary Mathematics, no. 358, American Mathematical Society, 2004, pp. 55–78.

[16] ———, *Computing Fitting ideals of Iwasawa modules*, Mathematische Zeitschrift **246** (2004), 733–767.

[17] C. Greither, X.-F. Roblot, and B. A. Tangedal, *The Brumer-Stark Conjecture in some families of extensions of specified degree*, manuscript, 12 pages.

[18] ———, *The Brumer-Stark Conjecture in some families of extensions of specified degree*, Mathematics of Computation **73** (2004), no. 245, 297–315.

[19] M. Hall, Jr., *The theory of groups*, The Macmillan Company, New York, 1959.

[20] D. R. Hayes, *Aligning Brumer-Stark elements into a Hecke character (working paper)*, preprint.

[21] ———, *Stickelberger elements in function fields*, Compositio Mathematica **55** (1985), 209–239.

[22] ———, *Hecke characters and Eisenstein reciprocity in function fields*, Journal of Number Theory **43** (1993), 251–292.

[23] ———, *The conductors of Eisenstein characters in cyclotomic number fields*, Finite Fields and their Applications **1** (1995), 278–296.

[24] ———, *Base change for the conjecture of Brumer-Stark*, Journal für die reine und angewandte Mathematik **497** (1998), 83–89.

[25] ———, *A conjectural property of the Brumer element*, manuscript, 4 pages, 2004.

[26] ———, *Stickelberger functions for non-abelian Galois extension of global fields*, Contemporary Mathematics **358** (2004), 193–205.

[27] J. Herbrand, *Sur les classes des corps circulaires*, J. Math. Pures et Appliqués, 9 série **11** (1932), 417–441 (French).

[28] G. J. Janusz, *Algebraic number fields*, Pure and Applied Mathematics, vol. 55, Academic Press [A Subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973.

[29] A. A. Kiselev, *An expression for the ideal class numbers of real quadratic fields using bernoulli numbers*, Dokl. Akad. Nauk. SSSR **61** (1948), 777–779 (Russian).

[30] H. Klingen, *Über die werte der dedekindsche zetafunktion*, Mathematische Annalen **145** (1962), 265–272.

[31] A. Kudo, *On a generalization of a theorem of Kummer*, Memoirs of the Faculty of Science, Kyushu University, Series A **29** (1975), no. 2, 255–261.

[32] S. Lang, *Cyclotomic fields I and II*, combined second edition ed., Springer-Verlag, New York, 1990, with an appendix by Karl Rubin.

[33] ———, *Algebraic number theory*, second ed., Springer-Verlag, New York, 1994.

[34] H.-W. Leopoldt, *Zur Struktur der l-Klassengruppe galoisscher Zahlkörper*, Journal für die reine und angewandte Mathematik **199** (1958), 165–174.

[35] S. Louboutin and R. Okazaki, *Determination of all non-normal quartic cm-fields and of all non-abelian normal octic cm-fields with class number one*, Acta Arithmetica **67** (1994), no. 1, 47–62.

[36] B. Mazur and A. Wiles, *Class fields of Abelian extensions of* $\mathbb{Q}$, Inventiones mathematicae **76** (1984), 179–330.

[37] N. Nakagoshi, *On the unramified extensions of the prime cyclotomic number field and its quadratic extensions*, Nagoya mathematical journal **115** (1989), 151–164.

[38] J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin-Heidelberg, 1999, Translated from the German by Norbert Schappacher.

[39] D. G. Northcott, *Finite free resolutions*, Cambridge Tracts in Mathematics, no. 71, Cambridge University Press, Cambridge-New York, 1976.

[40] _____, *Multilinear algebra*, Cambridge University Press, Cambridge-New York-Melbourne, 1984.

[41] C. D. Popescu, *On a refined Stark conjecture for function fields*, Compositio Math. **116** (1999), no. 3, 321–367.

[42] _____, *Base change for Stark-type conjectures over* $\mathbb{Z}$, Journal für die reine und angewandte Mathematik **542** (2002), 85–111.

[43] _____, *On the Rubin-Stark conjecture for a special class of CM extensions of totally real number fields*, Mathematische Zeitschrift **247** (2004), 529–547.

[44] K. A. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Inventiones mathematicae **34** (1976), 151–162.

[45] M. Rosen, *Number theory in function fields*, Springer-Verlag, New York, 2002.

[46] K. Rubin, *A Stark conjecture over* $\mathbb{Z}$ *for abelian L-functions with multiple zeros*, Annales de L'Institut Fourier **46** (1996), 33–62.

[47] J. W. Sands, *Abelian fields and the Brumer-Stark Conjecture*, Compositio Mathematica **53** (1984), 337–346.

[48] _____, *Galois groups of exponent two and the Brumer-Stark conjecture*, Journal für die reine und angewandte Mathematik **349** (1984), 129–135.

[49] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the French by Leonard L. Scott.

[50] _____, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[51] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. Univ. Tokyo, Sec. IA **23** (1976), 393–417.

[52] C. L. Siegel, *Über die Fourierschen Koeffizienten von Modulformen*, Göttingen Nach. **3** (1970), 15–56 (German).

[53] H. M. Stark, *Values of L-functions at* $s = 1$. *I. L-functions for quadratic forms*, Advances in Mathematics **7** (1971), 301–343.

[54] _____, *Values of L-functions at* $s = 1$. *II. Artin L-functions with rational characters*, Advances in Mathematics **17** (1975), no. 1, 60–92.

[55] ———, *Values of L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem*, Advances in Mathematics **22** (1976), no. 1, 64–84.

[56] ———, *Values of L-functions at $s = 1$. IV. First derivatives at $s = 0$*, Advances in Mathematics **35** (1980), no. 3, 197–235.

[57] P. Stevenhagen, *Class number parity for the pth cyclotomic field*, Mathematics of Computation **63** (1994), no. 208, 773–784.

[58] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$: notes d'un cours à Orsay*, Progress in Mathematics, vol. 47, Birkhäuser Boston Inc., Boston, MA, 1984 (French), lecture notes recorded by Dominique Bernardi and Norbert Schappacher.

[59] ———, *Brumer-Stark-Stickelberger*, Séminaire de Théorie des Nombres, Université de Bordeaux I, U. E. R. de mathèmatiques et d'information **exposé no. 24** (Année 1980-1981) (French).

[60] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Springer Verlag, New York, 1997.

[61] A. Weil, *Jacobi sums as "Grössencharaktere"*, Transactions of the American Mathematical Society **73** (1952), 487–495.

[62] ———, *Sommes de Jacobi et caractères de Hecke*, Nachrichten der Akademie der Wissenschaften in Göttingen II, Mathematisch-Physikalische Klasse (1974), 1–14.

[63] A. Wiles, *The Iwasawa conjecture for totally real fields*, Annals of Mathematics **131** (1990), 493–540.

[64] ———, *On a conjecture of Brumer*, Annals of Mathematics **131** (1990), 555–565.

[65] T.-H. Yang, *Existence of algebraic Hecke characters*, Comptes rendus de l'Académie des sciences, Série I, Mathématique **332** (2001), 1041–1046.