THE COATES-SINNOTT CONJECTURE FOR CYCLIC CUBIC EXTENSIONS

THE GENERALIZED COATES-SINNOTT CONJECTURE FOR SOME FAMILIES OF CUBIC EXTENSIONS OF NUMBER FIELDS

By

DARREN GRAY, B.SC.

A Thesis
Submitted to the School of Graduate Studies
in Partial Fulfilment of the Requirements
for the Degree
Master of Science

McMaster University

MASTER OF SCIENCE (2009) McMaster University
(Mathematics) Hamilton, Ontario

TITLE: The generalized Coates-Sinnott Conjecture for some families of cubic extensions of number fields
AUTHOR: Darren Gray, B.Sc. (Queens University)
SUPERVISOR: Professor Manfred Kolster
NUMBER OF PAGES: vi, 48

Abstract

Let E/k be an S_3 extension of totally real number fields with quadratic subextension F/k. The generalized Coates-Sinnott conjecture predicts that for $n \geq 2$, the integralized Stickelberger element $w_n(E)\theta_{E/F}(1-n)$ attached to the cyclic cubic extension E/F should annihilate the p-part of $H^2_{\mathcal{M}}(\mathcal{O}_E, \mathbb{Z}(n))$ for all primes p. We show this to be true for all $p \neq 2, 3$.

Acknowledgements

I would like to begin by thanking my thesis advisor, Dr. Manfred Kolster, for introducing me to the realm of algebraic number theory. Without his guidance and unfailing patience I could never have completed this thesis. His welcoming demeanour and sense of humour made our weekly meetings an enjoyable event.

I would also like to thank my friends and colleagues at McMaster, who have made my time here truly memorable. Special thanks to Dan for the music sessions and showing me around Hamilton, and to the McMaster waterpolo team for two wonderful seasons.

Finally I thank my parents, David and Joyce, and my brother Jeff for their love and support throughout the years, and also Tara, for her companionship, encouragement and especially understanding through the ups and downs of this endeavour.

Contents

0.1 Introduction

Let E/F be a finite abelian extension of totally real number fields with Galois group G. Let $\chi \in \hat{G}$ be an absolutely irreducible character of G. We denote by $L(s,\chi)$ the Artin L-function associated to χ with Euler factors removed at infinite primes and primes which ramify in E. We define the *generalized Stickelberger element* with values in $\mathbb{C}[G]$ as

$$\theta_{E/F}(s) = \sum_{\chi \in \hat{G}} L(s, \overline{\chi})\, e_\chi$$

where e_χ denotes the group ring idempotent $\frac{1}{|G|}\sum_{g\in G}\chi(g)g^{-1}$. For positive integers n, results by Klingen-Siegel ([18]) show that $\theta_{E/F}(1-n) \in \mathbb{Q}[G]$.

When $n = 1$ and E is a cyclotomic extension of $\mathbb{Q}$ we obtain the classical Stickelberger element, denoted simply θ. The classical Stickelberger theorem ([22]) states that

$$\beta\theta \in Ann_{\mathbb{Z}[G]}(Cl(\mathcal{O}_E))$$

for all $\beta \in \mathbb{Z}[G]$ such that $\beta\theta \in \mathbb{Z}[G]$. Brumer conjectured that a similar result should hold for arbitrary abelian extensions E/F while a conjecture by Coates-Sinnott ([3]) states a similar result (over $\mathbb{Q}$) for $n \geq 2$ in terms of Quillen K-groups.

For $n \geq 2$, Deligne-Ribet ([4]) showed that suitable multiples of $\theta_{E/F}(1-n)$ are contained in $\mathbb{Z}[G]$. Specifically,

$$Ann_{\mathbb{Z}[G]}(H^0(E, \mathbb{Q}/\mathbb{Z}(n))) \cdot \theta_{E/F}(1-n) \subset \mathbb{Z}[G].$$

Extended to arbitrary base fields (see [14] and [20]), the generalized Coates-Sinnott conjecture then predicts that

$$Ann_{\mathbb{Z}[G]}(H^0(E, \mathbb{Q}/\mathbb{Z}(n))) \cdot \theta_{E/F}(1-n) \subseteq Ann_{\mathbb{Z}[G]}(K_{2n-2}(\mathcal{O}_E));$$

Coates-Sinnott proved the conjecture, up to powers of 2, for abelian extensions over $\mathbb{Q}$ and $n = 2$.

Assuming the Bloch-Kato Conjecture, there are isomorphisms between the higher K-groups $K_{2n-2}(\mathcal{O}_E)$ and the motivic cohomology groups $H^2_{\mathcal{M}}(\mathcal{O}_E, \mathbb{Z}(n))$ for $n \geq 2$, up to known 2-torsion. A recent paper by Kolster and Sands ([10]) suggests that restating Coates-Sinnott in terms of motivic cohomology should give the correct conjecture, including 2-primary parts:

$$Ann_{\mathbb{Z}[G]}(H^0(E, \mathbb{Q}/\mathbb{Z}(n))) \cdot \theta_{E/F}(1-n) \subseteq Ann_{\mathbb{Z}[G]}(H^2_{\mathcal{M}}(\mathcal{O}_E, \mathbb{Z}(n))).$$

The $\mathbb{Z}[G]$-annihilator of $H^0(E, \mathbb{Q}/\mathbb{Z}(n))$ is generated by its order, denoted $w_n(E)$. As the groups $H^2_{\mathcal{M}}(\mathcal{O}_E, \mathbb{Z}(n))$ are finite, we can approach the problem prime by prime. Proving the conjecture then reduces to showing that the integralized Stickelberger element $w_n(E)\theta_{E/F}(1-n)$ annihilates the p-part of $H^2_{\mathcal{M}}(\mathcal{O}_E, \mathbb{Z}(n))$ for all primes.

Let E/k be an S_3 extension of totally real number fields with quadratic subextension F/k. In this paper we examine the (motivic) Coates-Sinnott conjecture for the extension E/F. We will show that the p-part of the conjecture holds for any prime $p \neq 2, 3$. It is inspired by a paper by Lloyd Simons ([19]), who proves the case when $n = 2$. We will generalize the result to all $n \geq 2$.

Under the assumption that the Bloch-Kato conjecture holds, we can identify the p-part of $H^2_{\mathcal{M}}(\mathcal{O}_E, \mathbb{Z}(n))$ with the étale cohomology groups $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ for all p. To prove our theorem we need to use a result of Lichtenbaum's ([11]) relating the values of certain L-functions to the order of these groups. We also need the Main Conjecture of Iwasawa Theory, proved by Wiles in [24].

In Chapter 1 we review the theory of linear representation and characters, while Chapter 2 provides the background needed to state Lichtenbaum's result. Finally, in Chapter 3 we present the main result of our thesis.

Chapter 1

Representation Theory

In this chapter we introduce the concept of linear representations of groups. Section 1.1 gives some basic definitions and theorems on representation theory. Section 1.2 builds up the theory of characters, and shows how the irreducible characters of a group allows us to break representations into a direct sum of subrepresentations. In Section 1.3 we show that modules over a group algebra are the same as representations, and finish with a discussion of the p-adic numbers.

The background material in this chapter, especially of the first two sections, is taken primarily from [8] and [15].

1.1 Linear Representations

Let G be a finite group, F a field and V a vector space over F. A *linear representation* of G in V is a homomorphism ρ from G into $GL(V)$, the group of automorphisms of V. We restrict ourselves to the case when V has finite dimension n and say that n is the *degree* of the representation. In this case we identify $GL(V)$ with $GL_n(F)$, the group of n by n invertible matrices with entries in F. When ρ is given, V is called a *representation space* of G. For brevity, the term 'representation' is usually applied to both ρ and V, and it should be clear from the context whether we are referring to the vector space or the group homomorphism.

A linear representation assigns to each element $s \in G$ an element $\rho(s) \in GL(V)$. (For convenience we will sometimes write ρ_s for $\rho(s)$.) By definition, linear representations preserve the identity and inverse properties of G:

- $\rho(1) = 1$ (The identity matrix in $GL(n, F)$.
- $\rho(s^{-1}) = \rho(s)^{-1}$ for all $s \in G$.

The degree n of the representation plays a significant role. When $n = 1$, $GL(V)$ consists simply of the invertible elements of F. As G is a finite group, each element $s \in G$ must have finite order, and it follows that ρ_s is then a root of unity in F. We can always construct a representation of degree 1: we simply set $\rho_s = 1$ for all $s \in G$. It is known as the *trivial representation.*

On the other hand, consider the case when $n = |G|$, the order of the group G. We can index the basis of V by the elements of G, i.e. $(e_g)_{g \in G}$. For each $s \in G$ we define ρ_s by its action on the basis elements of V:

$$\rho_s(e_g) = e_{sg} \tag{1.1}$$

It is easy to show that this defines a linear representation of G. It is known as the *(left) regular representation* of G.

Before moving on, we give two more definitions. The *kernel* of a representation ρ consists of all $s \in G$ whose image is the identity matrix. When ρ is injective we call the representation *faithful.*

Subrepresentations

Let ρ be a representation of G over V with degree n. Suppose that V has a non-zero vector subspace W of dimension $m < n$ that is *stable* (or *invariant*) under the group action of G. (In other words, $w \in W$ implies $\rho_s(w) \in W$ for all $s \in G$.) We choose an ordered basis $\{e_1, \ldots, e_n\}$ for V such that $\{e_1, \ldots, e_m\}$ is an ordered basis

for W. Then it is easy to show that ρ_s (an n by n matrix in $GL(V)$) must have the block form

$$\rho_s = \begin{bmatrix} A_s & B_s \\ 0 & C_s \end{bmatrix} \tag{1.2}$$

where A_s and C_s are square matrices of order m and $(n-m)$, respectively. We further note that the action of ρ_s on W is completely determined by A_s, which we call the *restriction* of ρ_s to W and denote by ρ_s^W. It is easy to check that ρ_s^W is an automorphism of W for all $s \in G$. Then ρ^W is a linear representation of G in W, and we call W a *subrepresentation* of V. If V has no non-trivial subrepresentations, we say that V and ρ are *irreducible*. This brings us to an important result:

Theorem 1.1. *Let V be a linear representation of G defined over the field F. Suppose the characteristic of F does not divide the order of G. Then for every subrepresentation W of V there exists a complement W' of W in V which is also a subrepresentation of G.*

Proof. We follow along the lines of the proof given in [15, p. 6]. Let W^0 be an arbitrary vector space complement of W in V. Let π_0 be the corresponding projection of V onto W (i.e. $\pi_0^2 = \pi_0$ and $\pi_0(w) = w$ for all $w \in W$). The characteristic of F does not divide the order of G, so $|G|$ is invertible in F and we define a linear transformation $\pi : V \to W$ by

$$\pi = \frac{1}{|G|} \sum_{g \in G} \rho_g \cdot \pi_0 \cdot \rho_g^{-1}$$

with ρ the group homomorphism associated with the representation V. It is easy to check that this is a projection of V into W. We now claim that $W' = ker(\pi)$ is stable under G. First we show that $\rho_s \cdot \pi = \pi \cdot \rho_s$ for all $s \in G$:

$$\rho_s \cdot \pi \cdot \rho_s^{-1} = \frac{1}{|G|} \sum_{g \in G} \rho_s \rho_g \cdot \pi_0 \cdot \rho_g^{-1} \rho_s^{-1} = \frac{1}{|G|} \sum_{g \in G} \rho_{sg} \cdot \pi_0 \cdot \rho_{sg}^{-1} = \pi$$

Now suppose $x \in W'$. Then for any $s \in G$, $\pi \cdot \rho_s(x) = \rho_s \cdot \pi(x)$ which, as $x \in ker(\pi)$, must be zero. Then $\rho_s(x) \in W'$ as well, showing that W' is stable under G and therefore a subrepresentation of V.

We finish by showing that $V = W \oplus W'$. For any $v \in V$, write $v = \pi(v) + (v - \pi(v))$. The first term is in W and the second is in W', so $V = W + W'$. Now suppose $v \in W \cap W'$. Then $v = \pi(v)$ because $v \in W$, but $\pi(v) = 0$ because $v \in W'$. So $W \cap W' = 0$ and V is a direct sum of the two subrepresentations. □

For the remainder of this chapter we will assume that all representations of a group G are defined over a field whose characteristic does not divide the order of G and that Theorem 1.1 holds.

We return to the representation described in (1.2). As W is a subrepresentation of V there exists another subrepresentation W' of V such that $V = W \oplus W'$. Then $B_s = 0$ and (1.2) reduces to

$$\rho_s = \begin{bmatrix} \rho_s^W & 0 \\ 0 & \rho_s^{W'} \end{bmatrix}.$$

In fact, a consequence of Theorem 1.1 is that every representation is the direct sum of irreducible representations. If ρ is a representation of G, then for every $s \in G$ the element $\rho_s \in GL(V)$ can be expressed in block diagonal form. To study a representation V, we should therefore look at its decomposition

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$$

into a direct sum of irreducible representations. Unfortunately this decomposition may not be unique. To construct a unique decomposition we must first introduce the idea of 'similar' representations. Suppose V and V' are both representation spaces of G with linear representations ρ and ρ', respectively. If there exists an isomorphism $\tau : V \to V'$ such that $\tau \cdot \rho_s \cdot \tau^{-1} = \rho'_s$ for all $s \in G$, we say that V and V' are *isomorphic* (or *similar*).

To form a unique decomposition we group together all the irreducible subrepresentations which are isomorphic to one another. Let $U_1, \ldots, U_h$ be a set of distinct (up to isomorphism) irreducible subrepresentations of V, and let V_i be the direct sum of all the subrepresentations of V which are isomorphic to U_i. Then

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_h \tag{1.3}$$

is a unique decomposition, known as the *canonical decomposition.*

It is then apparent that to study a given representation V, we need to understand the distinct irreducible subrepresentations of V. This is made much easier through the use of character theory, developed by Georg Frobenius.

1.2 Character Theory of Finite Groups

1.2.1 The Character of a Representation

Let ρ be a representation of G over V with degree n. The *character* χ *afforded by* ρ is the map from G into F defined by

$$\chi(s) = \text{trace}(\rho_s)$$

for all $s \in G$. We call χ *irreducible* when ρ is irreducible, and the *degree* of χ is simply the degree of ρ. In general characters are not homomorphisms. However, when $n = 1$, χ and ρ are indistinguishable and therefore χ is indeed a homomorphism. We call characters of degree 1 *linear characters.* The character afforded by the trivial representation is called the *principal character* of G and denoted χ_0.

The characters of a group G are closed under addition. Let χ and χ' be the characters afforded by representations V and V'. Then the sum $\chi + \chi'$ is the character of the representation $V \oplus V'$. As every representation can be written as the direct

sum of irreducible subrepresentations, so can every character be written as the sum of irreducible characters. The nature of the trace formula also gives the following facts about characters:

- $\chi(1) = n$
- For all $s, t \in G$, $\chi(tst^{-1}) = \chi(s)$

The second property shows that χ is a *class function* on G. As an immediate consequence, it is clear that similar representations afford the same character. The converse is also true, but before showing why we need to look at the orthogonality relations between irreducible characters of G.

Orthogonality Relations

For the remainder of this section we restrict ourselves to representations and characters defined over the field of complex numbers.

Let H be the set of class functions on G. For $\phi, \psi \in H$, we define a scalar product as follows:

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{t \in G} \phi(t)\psi(t^{-1})$$

This inner product gives the following results on characters of G [15, p. 15]:

- A character χ is irreducible if and only if $\langle \chi, \chi \rangle = 1$.
- For two distinct irreducible characters χ and χ' we have $\langle \chi, \chi' \rangle = 0$.

The irreducible characters of G clearly form an orthonormal system in H with respect to this inner product. In fact they form a basis for all the class functions of

G. If we let h be the number of irreducible characters of G, then $h = |H|$, the number of conjugacy classes of G.

We can use this inner product to prove that two representations affording the same character must be isomorphic. Let V be a representation of G with character φ. We can write V as the direct sum

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$$

of irreducible subrepresentations. If W_i affords the irreducible character χ_i then

$$\varphi = \chi_1 + \chi_2 + \cdots + \chi_k.$$

Let U be an irreducible representation with character χ. To find out how many of the W_i in V are isomorphic to U we simply take the inner product of φ with χ:

$$\begin{aligned} \langle \varphi, \chi \rangle &= \langle \chi_1 + \chi_2 + \cdots \chi_k, \chi \rangle \\ &= \langle \chi_1, \chi \rangle + \langle \chi_2, \chi \rangle + \cdots + \langle \chi_k, \chi \rangle \end{aligned}$$

Each of these terms is one or zero, depending on whether or not W_i is isomorphic to U. Then $\langle \varphi, \chi \rangle$ 'counts' the number of irreducible subrepresentations of V which are isomorphic to U.

If V' is another representation affording φ, then by the above argument V' and V will contain the same number of copies of U. We can do this for every irreducible representation U of G, showing that V' and V are isomorphic.

We return to the canonical decomposition of a representation V as given in (1.3):

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_h$$

Each V_i is the direct sum of isomorphic irreducible representations. Let χ_i be the characters of these representations. We can find the number of isomorphic copies of V_i contained in V by taking the inner product of the character of V with χ_i. We can also find the projection of V onto V_i by the linear map

$$p_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1}) \rho_g \tag{1.4}$$

where n_i is the degree of χ_i and ρ is the linear representation of G in V.

With these tools, it is possible to find the decomposition of a representation using only character theory and in general, the characters of a group G are much easier to compute that its representations.

Character Tables

As characters are class functions, they are constant on the conjugacy classes of G. The values of the irreducible characters on these classes are listed in a *character table.* The columns correspond to conjugacy classes and the rows correspond to characters. By convention we put the identity element in the first column and the principal character in the first row. It follows that the first column contains the degrees of the characters, and the first row contains only 1s.

There are a number of methods to determine the values in a character table, some of which we will discuss here. For one, the degrees must divide the order of the group [8, p. 38]. More information on the columns can be obtained by looking at the character χ_{reg} afforded by the regular representation given in (1.1). Let $\chi_1, \ldots, \chi_h$ be the set of irreducible characters of G, each with degree n_i. Then

$$\chi_{reg} = \sum_{i=1}^{h} n_i \chi_i$$

and evaluating $\chi_{reg}(s)$ at the elements $s \in G$ shows that $\chi_{reg}(1) = |G|$ and $\chi_{reg}(s) = 0$

for $s \neq 1$. This gives us the following:

$$\sum_{i=1}^{h} n_i^2 = |G| \quad \text{and} \quad \sum_{i=1}^{h} n_i \chi_i(s) = 0 \text{ for } s \neq 1 \tag{1.5}$$

In general, this won't be enough to determine the whole table, but can be used to complete the table once a few of the characters have been determined. Take for example S_3, the group of permutations of three elements. S_3 is of order 6 and has three conjugacy classes: the identity, the class of transpositions (denoted τ) and the class of cyclic permutations (denoted σ). Then there are exactly three irreducible characters. Their degrees divide 6 and, when squared, sum to 6. The only possible combination is 1, 1 and 2.

We start by listing the characters in order of ascending degree. Let Ψ_0 denote the principal character, Ψ_1 the other character of degree 1 and Ψ_2 the character of degree 2. The character Ψ_1 is a homomorphism of G, respectively sending τ and σ to 2nd and 3rd roots of unity. Given a representation ρ of a group into a vector space defined over $\mathbb{C}$, one can easily check that the complex conjugate $\overline{\rho}$ is also a representation, and so complex characters must come in conjugate pairs. As Ψ_1 is the only non-trivial character of degree 1, then it cannot admit complex values. So $\Psi_1(\tau) = -1$ and $\Psi_1(\sigma) = 1$. We can then complete the table using the equations given in (1.5):

Table 1.1: Character Table of S_3

	1	τ	σ
Ψ_0	1	1	1
Ψ_1	1	-1	1
Ψ_2	2	0	-1

The character tables of abelian groups are particularly simple to determine. In this case every element of G is its own conjugacy class, and therefore the number of irreducible characters of G is equal to the order of G. Furthermore, the set of irreducible characters of an abelian group is isomorphic to the group itself, making it very easy to complete the table.

1.2.2 Subgroups and Quotient Groups

After finding the characters of a group G, we may wish to determine the characters of its subgroups and quotient groups. Conversely, knowing the character tables of these smaller groups can usually give us information about the characters of G that we might not otherwise have been able to determine. We study the relationship between these characters over the next few pages.

Restricted Characters

Let H be a subgroup of G, and suppose we have a representation ρ of G which affords the character χ. We restrict ρ to the elements of H. This is certainly a representation of H and we denote it by ρ_H and its afforded character by χ_H.

If χ_H is irreducible in H, then χ must be irreducible in G. On the other hand, irreducibility of χ does not imply irreducibility of χ_H. So we cannot determine the character table of H simply from the character table of G. The next question should be, given the character table of H, can we determine the character table of G?

Induced Characters

We start with an arbitrary class function ϕ of H, and we construct the *induced class function* ϕ^G on G by defining

$$\phi^G(g) = \frac{1}{|H|} \sum_{x \in G} \phi^\circ \left(xgx^{-1}\right) \tag{1.6}$$

where $\phi^\circ = \phi$ when evaluated at elements of H and zero otherwise. This is clearly a class function of G, and we now ask whether characters of H induce characters of G.

We make use of *Frobenius' Reciprocity Theorem* ([15, p. 56]): For a subgroup H of G and class functions ϕ and ψ of H and G respectively, we have the equality

$$\langle \phi, \psi_H \rangle_H = \langle \phi^G, \psi \rangle_G$$

where $\langle \cdot, \cdot \rangle_H$ and $\langle \cdot, \cdot \rangle_G$ are the inner products on H and G and ψ_H is the restriction of ψ to the elements of H.

Let ϕ be a character of H, and suppose χ is an irreducible character of G. Then χ_H is a character of H and $\langle \phi, \chi_H \rangle_H$ must be a non-negative integer. It follows that $\langle \phi^G, \chi \rangle_G$ is a non-negative integer for every irreducible character χ of G. As these form a basis for the class functions of G, we conclude that ϕ^G is the sum of irreducible characters and is therefore a character of G as well. When dealing with characters, we use the notation $Ind_H^G \phi$ instead of ϕ^G.

If $Ind_H^G \phi$ is irreducible in G, then ϕ is irreducible in H. Unfortunately, as with the restricted character, the converse is not always true. We still need to investigate the induced characters to see if they are irreducible.

Quotient Groups

Let N be a normal subgroup of G. Two equivalent definitions of normality are:

- N is the union of conjugacy classes of G.
- N is the kernel of some group homomorphism of G.

To find the normal subgroups of G one must simply look at its character table. It is easy to show that the kernel of a representation affording χ is the set of $g \in G$ such that $\chi(g) = \chi(1)$. Scanning the row beside χ, we look for the columns of conjugacy classes whose values match the first column. The union of these conjugacy classes is the kernel of the representation, and therefore a normal subgroup. In fact, every normal subgroup $N \triangleleft G$ is the intersection of some of these kernels, and can be found by inspection.

Once we find a normal subgroup $N \triangleleft G$, it is very easy to determine the irreducible characters of the quotient group G/N. If N is in the kernel of a representation

affording χ, then χ is constant on the cosets of N in G. The class function $\hat{\chi}$ of G/N defined by $\hat{\chi}(gN) = \chi(g)$ is a character of G/N and irreducible if χ is irreducible. Similarly, for any character of G/N we can define a character on G using this same definition, which also preserves irreducibility.

As an example, consider the group $G \cong S_4$, with character table shown below:

Table 1.2: Characters of G

	1	(12)	(12)(34)	(1234)	(123)
χ_0	1	1	1	1	1
χ_1	1	-1	1	-1	1
χ_2	2	0	2	0	-1
χ_3	3	1	-1	-1	0
χ_4	3	-1	-1	1	0

We look at the third row and determine that the kernel of the representation affording χ_2 is the conjugacy class of (12)(34) along with the identity. This must be a normal subgroup, which we will call N. We now wish to know the irreducible characters of G/N. By inspection N is contained in the kernel of the representations affording χ_0, χ_1 and χ_2, and these must be irreducible characters of the quotient group. This gives us the Table 1.3, where $\overline{g}$ is the coset in G/N containing the conjugacy class of $g \in G$. This table has too many columns for a character table, but some of these are simply repeats. In G/N the elements of columns two and four are conjugate, as are the elements of columns three and five. Eliminating the last two columns gives us the character table of S_3, which is indeed a quotient group of S_4.

Table 1.3: Characters of G/N

	$\overline{1}$	$\overline{(12)}$	$\overline{(12)(34)}$	$\overline{(1234)}$	$\overline{(123)}$
χ_0	1	1	1	1	1
χ_1	1	-1	1	-1	1
χ_2	2	0	2	0	-1

Knowing the character table of G, it is a trivial task to construct the character tables of all the quotient groups of G. On the other hand, knowing the irreducible characters of quotient groups can help fill in many of the values of the character table of G.

1.3 Representations as Modules

1.3.1 Changing the Field

The nature of a representation V depends greatly on the field F over which V is defined. When we want to emphasize F we will refer to representations and characters over F as F-representations and F-characters.

Unfortunately, some of the orthogonality relations we developed in the last section do not necessarily apply to representations over arbitrary fields. Take the case when G is the cyclic group of order 3 generated by an element σ. We consider the representation of G defined by

$$\rho_\sigma = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

and ask whether or not ρ is reducible. As a $\mathbb{C}$-representation it must be, because ρ would afford a character of degree two, and the irreducible $\mathbb{C}$-characters of an abelian group are always linear. As a $\mathbb{Q}$-representation, however, it is irreducible, as $\mathbb{Q}$ does not contain any primitive 3rd roots of unity.

We introduce the concept of absolute irreducibility. Let ρ be an F-representation. We say that ρ is *absolutely irreducible* if ρ is irreducible over E for every field extension $E \supseteq F$. Characters afforded by absolutely irreducible representations are also called absolutely irreducible. Every character ϕ is the sum of absolutely irreducible characters, which we call the *absolutely irreducible components of* ϕ.

When F is algebraically closed (such as $\mathbb{C}$), then every irreducible F-representation is absolutely irreducible ([8, p. 146]).

1.3.2 Module Theory

Let G be a group of finite order and V a vector space over F. Consider the group algebra $F[G]$. The elements of $F[G]$ may be written uniquely in the form

$$f = \sum_{g \in G} a_g g$$

with $a_g \in F$. If ρ is a representation of G in V, then we can define an algebra homomorphism from $F[G]$ into $End(V)$ by linear extension:

$$\rho\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \rho_g$$

This gives V the structure of an $F[G]$-module. Conversely, if given an $F[G]$-module V, we can easily construct an F-representation of G in V: for $g \in G$ and $x \in V$ we simply define $\rho_g(x)$ as the module action of g on x. This shows that there is a bijection between modules and representations:

$$\left\{ \begin{array}{c} V \text{ an } F[G]\text{-module} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} V \text{ a vector space over } F \\ \text{and} \\ \rho : G \to GL(V) \text{ a representation} \end{array} \right\}$$

This allows us to use representation theory when trying to determine the features of an $F[G]$-module. Some of the terminology is different when speaking of modules. Subrepresentations are the same as *submodules*, and irreducible representations are *simple modules*. If V is the direct sum of simple modules we call it *semisimple*. For

the purposes of this paper we are interested in the semisimple case, for which we need the following important theorem.

Theorem 1.2. (Maschke's Theorem) *Let G be a finite group and F a field whose characteristic does not divide $|G|$. Then every $F[G]$-module is semisimple.*

Maschke's Theorem is equivalent to Theorem 1.1, but expressed in terms of module theory. If we replace the field F by an integral domain R, the theorem applies to $R[G]$-modules as well, provided that $|G|$ is invertible in R.

1.3.3 Decomposition over the p-adic numbers

Let p be a prime. The p-adic numbers, denoted $\mathbb{Q}_p$, are constructed by completing $\mathbb{Q}$ with respect to the p-adic metric. The theory of p-adic numbers was developed by Kurt Hensel in 1897 and is used extensively in number theory. An equivalent definition of $\mathbb{Q}_p$ is as the field of fractions of $\mathbb{Z}_p$, the p-adic integers, which we now define.

Let f_i denote the canonical homomorphisms from $\mathbb{Z}/p^i\mathbb{Z}$ to $\mathbb{Z}/p^{(i-1)}\mathbb{Z}$ for $i \geq 2$. If S is the ordered Cartesian product of the sets $\mathbb{Z}/p^i\mathbb{Z}$, then we define the p-adic integers as the ring

$$\mathbb{Z}_p = \{(x_i) \in S \mid f_i x_i = x_{i-1} \text{ for } i \geq 2\}.$$

In other words, $\mathbb{Z}_p$ is the inverse limit of the following sequence of rings:

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{f_2} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{f_3} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{f_4} \cdots$$

We are going to need to work with the p-adic numbers throughout this paper, and so we state some important properties of $\mathbb{Z}_p$.

Theorem 1.3. *([13, p. 63]) The ring $\mathbb{Z}_p$ has the following properties:*

- *$\mathbb{Z}_p$ is a local ring with unique maximal ideal $p\mathbb{Z}_p$.*
- *$\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*
- *We can embed the integers $\mathbb{Z}$ in $\mathbb{Z}_p$ by mapping $x \mapsto (x_i)$ where x_i is the image in $\mathbb{Z}/p^i\mathbb{Z}$ of x.*
- *$(a_i) \in \mathbb{Z}_p$ is a unit if and only if $a_1 \neq 0$.*
- *$\mathbb{Z}_p$ is an integral domain of characteristic zero.*

Let n be an integer. The ring $\mathbb{Z}/p\mathbb{Z}$ contains the n-th roots of unity if and only if n divides $(p-1)$, and by the properties above, the same applies to $\mathbb{Z}_p/p\mathbb{Z}_p$. Hensel's Lemma shows that we can lift these roots into $\mathbb{Z}_p$, giving the following corollary:

Corollary 1.4. *(Proposition 3.4.2 of [7]) The p-adic integers $\mathbb{Z}_p$ contain the n-th roots of unity if and only if n divides $(p-1)$.*

Let A be a finite abelian group. We denote by $A(p)$ the Sylow p-subgroup of A, consisting of all elements $x \in A$ whose order is a power of p. (This is also called the p-primary component of A.)

Theorem 1.5. *Let A be a finite abelian group. Then $A \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is isomorphic to $A(p)$.*

Proof. We begin by looking at $A \otimes_{\mathbb{Z}} \mathbb{Z}/p^i\mathbb{Z}$ for $i \geq 1$. Let $q \neq p$ be a prime and consider the subgroup $A(q)$ of A. An element $x \in A(q)$ has order q^m for some m. As q^m is prime to p then it is invertible in $\mathbb{Z}/p^i\mathbb{Z}$, and for any $y \in \mathbb{Z}/p^i\mathbb{Z}$ we get

$$x \otimes_{\mathbb{Z}} y = x \otimes_{\mathbb{Z}} \frac{q^m}{q^m} y = q^m x \otimes_{\mathbb{Z}} \frac{1}{q^m} y = 0.$$

So $A(q) \otimes_{\mathbb{Z}} \mathbb{Z}/p^i\mathbb{Z}$ vanishes for all $q \neq p$. Then

$$A \otimes_{\mathbb{Z}} \mathbb{Z}/p^i\mathbb{Z} \cong A(p) \otimes_{\mathbb{Z}} \mathbb{Z}/p^i\mathbb{Z}$$

$$\cong A(p)/p^i A(p)$$

by a result in [5, p. 370]. Inverse limits commute with tensor products, and so we now take the inverse limit of $A \otimes_{\mathbb{Z}} \mathbb{Z}/p^i\mathbb{Z}$ to get

$$A \otimes_{\mathbb{Z}} \mathbb{Z}_p = \varprojlim A(p)/p^i A(p)$$

For i large enough, $p^i A(p)$ must be zero. Then the inverse limit is isomorphic to $A(p)$ as claimed. □

Let G be a finite group. The p-part of any finite $\mathbb{Z}[G]$-module can be found by tensoring with $\mathbb{Z}_p$, producing a $\mathbb{Z}_p[G]$-module. We will be working with $\mathbb{Z}_p[G]$-modules in the main theorem of our paper, and will need to know when they decompose into a direct sum of submodules. By Theorem 1.3 the order of G is invertible in $\mathbb{Z}_p$ if and only if it is prime to p. Maschke's Theorem then gives the following:

Corollary 1.6. *Let p be a prime and G a finite group whose order is prime to p. Then any $\mathbb{Z}_p[G]$-module is semisimple.*

To decompose a $\mathbb{Z}_p[G]$-module M into a direct sum of submodules we need the irreducible $\mathbb{Q}_p$-characters of G. For each such χ we form the *group ring idempotents*

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g \tag{1.7}$$

which are exactly the projections given in (1.4) but written in terms of module theory. These idempotents are actually elements of $\mathbb{Z}_p[G]$ and so we may write $M = \oplus e_\chi M$ for any $\mathbb{Z}_p[G]$-module M.

Chapter 2

L-Series and Cohomology

In this chapter we build towards a theorem of Lichtenbaum's that relates the values of Artin L-functions at negative integers to the order of certain étale cohomology groups. Beginning with the Riemann Zeta Function, Section 2.1 takes us through various types of Dirichlet series before showing how to construct the Artin L-series, along with some well-known results. Section 2.2 tackles cohomology. We begin with the definition of group cohomology and discuss the relationship between étale cohomology and Galois cohomology. Finally, in Section 2.3 we introduce Lichtenbaum's theorem and discuss its application.

The theory of Artin L-functions presented in this paper is taken primarily from [12] and the cohomology theory from [2] and [16].

2.1 Artin L-Functions

We introduce the Artin L-Functions that form the basis for our Stickelberger element, and quote some results that will prove useful. We begin with one of the most prominent functions in number theory, the **Riemann Zeta Function**:

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

This function is given in terms of a complex variable s and is absolutely convergent when $\mathrm{Re}(s) > 1$. On this half-plane, we also have the equality

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

where p runs through the prime numbers, known as *Euler's Identity.* The Riemann Zeta Function can be continued meromorphically to the entire plane with a simple pole at $s = 1$.

Closely related to the Riemann Zeta Function are the *Dirichlet L-series.* Let χ be an irreducible character from $(\mathbb{Z}/m\mathbb{Z})^*$ into $\mathbb{C}$. By extending the definition of χ to all of $\mathbb{Z}$ we obtain the *Dirichlet character mod m*:

$$\chi(n) = \begin{cases} \chi(n \bmod m) & \text{if } \gcd(n, m) = 1 \\ 0 & \text{otherwise} \end{cases}$$

We now define the **Dirichlet L-series**

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

where s is a complex variable with $\mathrm{Re}(s) > 1$. The L-series is very similar to the Riemann Zeta Function, as it also converges absolutely on the half-plane $\mathrm{Re}(s) > 1$ and obeys Euler's Identity:

$$L(s, \chi) = \prod_{p} \frac{1}{1 - \chi(p)p^{-s}} \tag{2.1}$$

Similarly, it can be continued to a meromorphic function on the whole complex plane, and is then called the *Dirichlet L-function.* For χ_0 the principal character ($\chi_0(n) = 1$ for all n) we see that the Riemann Zeta Function is actually a special case of the Dirichlet L-functions.

Both the Riemann Zeta Function and the Dirichlet L-functions are attached to the field of rational numbers $\mathbb{Q}$. We now introduce the *Dedekind Zeta Function* and *Hecke L-series*, which extend the definitions of these previous tools to an arbitrary number field K.

The **Dedekind Zeta Function** is defined as the series

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

where $\mathfrak{a}$ runs through the non-zero integral ideals of K with $\mathfrak{N}(\mathfrak{a})$ their absolute norm. For an integral ideal $\mathfrak{m}$, we define $J^{\mathfrak{m}}$ to be the group of all ideals of K relatively prime to $\mathfrak{m}$. Given a character χ of finite order from $J^{\mathfrak{m}}$ into the complex numbers, we define the **Hecke L-series**

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

setting $\chi(\mathfrak{a}) = 0$ whenever $(\mathfrak{a}, \mathfrak{m}) \neq 1$. The Dedekind Zeta Function and Hecke L-series reduce to the Riemann Zeta Function and Dirichlet L-series when $K = \mathbb{Q}$. Both functions are absolutely convergent when $\mathrm{Re}(s) > 1$, and both have analogues to the Euler Identity, where $\mathfrak{p}$ runs through the prime ideals of K:

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

$$L(s, \chi) = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s}}$$

We should mention that the notation $L(s,\chi)$ is used both for Dirichlet L-series and Hecke L-series, but that this does not lead to confusion as the character χ will tell us whether we are working over $\mathbb{Q}$ or a number field K.

The Dirichlet L-series and Hecke L-series are defined for characters of abelian groups. Artin wished to expand the theory in terms of characters of Galois extensions. As an introduction, consider the field $\mathbb{Q}(\mu_m)$ obtained by adjoining the m-th roots of unity to $\mathbb{Q}$. Let G be the Galois group $Gal(\mathbb{Q}(\mu_m)/\mathbb{Q})$. Then it is a well-known fact that $(\mathbb{Z}/m\mathbb{Z})^*$ is isomorphic to G via the map

$$a \bmod m \longmapsto \sigma_a$$

where $\sigma_a \in G$ is an automorphism of the m-th roots of unity defined by $\sigma_a(\zeta_m) = (\zeta_m)^a$ for ζ_m a primitive m-th root. Then any Dirichlet character mod m can be considered as a linear character χ from G into the complex numbers. We can rewrite (2.1) in terms of this linear character as long as the product runs over primes p which don't divide m. When p is a prime, the automorphism σ_p defined above is known as the *Frobenius automorphism* and denoted φ_p. Putting it all together, we obtain the following expression for the Dirichlet L-series of χ in terms of the Galois extension G:

$$L(s,\chi) = \prod_{p \nmid m} \frac{1}{1 - \chi(\varphi_p)p^{-s}}$$

We can similarly view the characters of the Hecke L-series over K as characters of $Gal(K^{\mathfrak{m}}/K)$ with $K^{\mathfrak{m}}$ the ray class field extension with respect to the modulus $\mathfrak{m}$. This field extension $K^{\mathfrak{m}}/K$ generalizes the cyclotomic fields to arbitrary base fields K. We know that any abelian extension of $\mathbb{Q}$ (or relative abelian extension of K) is contained in a cyclotomic extension (or ray class field extension). In this way, we can view the Dirichlet L-series and Hecke L-series as series defined for characters of relative abelian extensions of $\mathbb{Q}$ and K respectively. The Artin L-series were developed to generalize this notion to arbitrary Galois extensions L/K and representations of $Gal(L/K)$.

Let $\mathfrak{p}$ be a prime ideal of K and let $\mathfrak{P}$ be a prime ideal of L lying over $\mathfrak{p}$. Suppose $\mathfrak{p}$ is unramified in L. Then there exists a unique automorphism $\varphi_{\mathfrak{P}} \in Gal(L/K)$ such that

$$\varphi_{\mathfrak{P}}(\alpha) \equiv \alpha^{\mathfrak{N}(\mathfrak{p})} \bmod \mathfrak{P} \tag{2.2}$$

for all $\alpha \in \mathcal{O}_L$ [12, p. 58]. It is the Frobenius automorphism mentioned earlier, defined for arbitrary number fields instead of $\mathbb{Q}$. Suppose ρ is a representation of $Gal(L/K)$ in V. Then $\varphi_{\mathfrak{P}}$ is sent by ρ to an invertible matrix in $GL(V)$. Consider now the determinant

$$\det\left(I - \rho(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}\right)$$

defined for $Re(s) > 1$. For $\mathfrak{P}$ and $\mathfrak{P}'$ above $\mathfrak{p}$, the elements $\varphi_{\mathfrak{P}}$ and $\varphi_{\mathfrak{P}'}$ are conjugate in $Gal(L/K)$, and so $\rho(\varphi_{\mathfrak{P}})$ depends only on $\mathfrak{p}$, not the choice of $\mathfrak{P}$. We define the (partial) **Artin L-series** associated to the representation ρ as

$$L(s,\rho) = \prod_{\mathfrak{p}} \frac{1}{\det\left(I - \rho(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}\right)} \tag{2.3}$$

where $\mathfrak{p}$ runs through those prime ideals of K which are unramified in L.

The Artin L-series defined above is not quite complete, as we still need Euler factors for those primes $\mathfrak{p}$ which ramify in L. There are only finitely many such primes, but when it is the case, the Frobenius automorphism $\varphi_{\mathfrak{P}}$ as given in (2.2) is not well-defined. It is, however, well-defined on the submodule $V^{I_{\mathfrak{P}}}$ where $I_{\mathfrak{P}}$ is the inertia group of $\mathfrak{P}$ over $\mathfrak{p}$. For a prime $\mathfrak{p}$ which ramifies in L we define the Euler factor

$$\det\left(I - \rho(\varphi_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}; V^{I_{\mathfrak{P}}}\right),$$

the characteristic polynomial of $\varphi_{\mathfrak{P}}$ on $V^{I_{\mathfrak{P}}}$. Including these factors in (2.3) completes the Artin L-series.

The Artin L-series are attached to representations ρ of $Gal(L/K)$, whereas the Dirichlet and Hecke L-series are attached to characters. However, the Euler terms in

the Artin L-series are identical for isomorphic representations, and we showed earlier that two representations are isomorphic if and only if they afford the same character. In light of this, we define the Artin L-series associated to the character χ of $Gal(L/K)$ as

$$L(s, \chi) = L(s, \rho)$$

where ρ is any representation of $Gal(L/K)$ affording χ. Once again, to distinguish an Artin L-series from the Dirichlet or Hecke L-series, one simply has to consider the Galois group over which χ is defined.

For an abelian extension of $\mathbb{Q}$, the Artin L-series is identical to the Dirichlet L-series. Taking a relative abelian extension of a number field K similarly gives us the Hecke L-series over K. We can also obtain the Dedekind and Riemann Zeta-Functions by taking χ to be the principal character; we include this result in the following theorem.

Theorem 2.1. *([12, p. 522]) The Artin L-series have the following properties:*

- *For the principal character χ_0 of $Gal(L/K)$ we have*

$$L(s, \chi_0) = \zeta_K(s). \tag{2.4a}$$

- *If χ_1 and χ_2 are characters of $Gal(L/K)$ then*

$$L(s, \chi_1 + \chi_2) = L(s, \chi_1)\, L(s, \chi_2). \tag{2.4b}$$

- *For an intermediate field $L \supseteq M \supseteq K$, and a character χ of $Gal(L/M)$ we have*

$$L(s, \chi) = L(s, \chi^*) \tag{2.4c}$$

  with χ^* the induced character of χ on $Gal(L/K)$.

- *For a bigger extension $L' \supseteq L \supseteq K$, and a character $\hat{\chi}$ of $Gal(L/K)$ we have*

$$L(s, \chi) = L(s, \hat{\chi}). \tag{2.4d}$$

  with χ the character of $Gal(L'/K)$ identified with $\hat{\chi}$.

These properties are well known and used extensively when studying Artin L-series. They also give the following useful corollary:

Corollary 2.2. *Letting χ vary over the nontrivial irreducible characters of $Gal(E/F)$ we have*

$$\zeta_E(s) = \zeta_F(s) \prod_{\chi} L_{E/F}(s,\chi)^{\chi(1)}.$$

Proof. Consider $Gal(E/E)$ as a trivial subgroup of $Gal(E/F)$. This subgroup can only afford one character, the principal character χ_0. On $Gal(E/F)$ it will induce the character of the regular representation: $\chi_{reg} = \sum \chi(1)\chi$. Then $L(s,\chi_{reg}) = L(s,\chi_0) = \zeta_E(s)$, and (2.4b) of Theorem 2.1 gives us the right hand side. □

2.2 Cohomology

Definition of Cohomology

Let $\mathcal{C}$ be a sequence of abelian groups or modules C^n connected by group homomorphisms $d^n : C^n \to C^{n+1}$ (also called boundary operations) as shown below:

$$0 \longrightarrow C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} \cdots \xrightarrow{d^{n-1}} C^n \xrightarrow{d^n} \cdots$$

When $d^n \circ d^{n-1} = 0$ for all $n \geq 1$ we say that $\mathcal{C}$ is a *cochain complex.* It is clear that $im(d^{n-1}) \subseteq ker(d^n)$, and if the two are equal the sequence is exact at C^n. In a sense, cohomology measures the 'exactness' of this chain at each step. We give the following definitions:

- Let $Z^n(\mathcal{C}) = ker(d^n)$ for $n \geq 0$. The elements of $Z^n(\mathcal{C})$ are called *n-cocycles.*
- Let $B^n(\mathcal{C}) = im(d^{n-1})$ for $n \geq 1$ and let $B^0(\mathcal{C}) = 1$. The elements of $B^n(\mathcal{C})$ are called *n-coboundaries.*

We now define $H^n(\mathcal{C})$ as the quotient group $Z^n(\mathcal{C})/B^n(\mathcal{C})$. The collection of $H^n(\mathcal{C})$ are called the cohomology groups of $\mathcal{C}$. If $\mathcal{C}$ is exact at some C^n, $H^n(\mathcal{C})$ is just the trivial group.

2.2.1 Group Cohomology

Let G be a group and A a G-module. As usual, let A^G denote the set of elements in A fixed by G. We can then consider $A \mapsto A^G$ as a functor from G-modules to abelian groups, sending G-module homomorphisms to abelian group homomorphisms. This functor is left exact; a short exact sequence of G-modules

$$0 \to A \to B \to C \to 0$$

will induce an exact sequence

$$0 \to A^G \to B^G \to C^G \to \tag{2.5}$$

which does not, in general, terminate with a surjective map. In this case we can construct a cohomological extension of the functor. The right derived functors thus obtained are denoted $H^n(G, A)$ with $H^0(G, A) = A^G$ and are called the cohomology groups of G with coefficients in A.

The right derived functors are obtained using projective resolutions. We begin by noting that A^G can be identified with $\mathrm{Hom}_G(\mathbb{Z}, A)$, the group of G-module homomorphisms from $\mathbb{Z}$ (upon which G acts trivially) into A. A *projective resolution* of $\mathbb{Z}$ (as a G-module) is an exact sequence

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

of projective G-modules. Taking the set of G-module homomorphisms from the resolution into A will induce a sequence

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \xrightarrow{\epsilon} \mathrm{Hom}_G(P_0, A) \xrightarrow{d^0} \mathrm{Hom}_G(P_1, A) \xrightarrow{d^1} \cdots$$

$$\cdots \xrightarrow{d^{n-1}} \mathrm{Hom}_G(P_n, A) \xrightarrow{d^n} \cdots$$

heading in the other direction. We note some important properties of the sequence. First of all, the first four terms

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \xrightarrow{\epsilon} \mathrm{Hom}_G(P_0, A) \xrightarrow{d^0} \mathrm{Hom}_G(P_1, A)$$

are exact ([5, p. 393]), giving us the following:

$$ker(d^0) = im(\epsilon) \cong \mathrm{Hom}_G(\mathbb{Z}, A) \cong A^G$$

Secondly, although the rest of the sequence may not be exact, it is a cochain complex ([16, p. 11]). Let $K^n = \mathrm{Hom}_G(P_n, A)$ for $n \geq 0$. Replacing $\mathrm{Hom}_G(\mathbb{Z}, A)$ by zero will not affect the cochain property of the sequence, and so we construct the cochain $\mathcal{K}$:

$$0 \longrightarrow K^0 \xrightarrow{d^0} K^1 \xrightarrow{d^1} \cdots \xrightarrow{d^{n-1}} K^n \xrightarrow{d^n} \cdots$$

The cohomology groups of this cochain are the right derived functors we desire. Let $H^n(G, A) = H^n(\mathcal{K})$ and note that $H^0(\mathcal{K}) = ker(d^0) \cong A^G$ as desired. The cohomology groups $H^n(G, A)$, along with connecting homomorphisms δ^n, allow us to extend the sequence given in (2.5) to a cohomology sequence which is exact:

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta^0} H^1(G, A) \to H^1(G, B) \to \cdots$$

$$\cdots \to H^n(G, C) \xrightarrow{\delta^n} H^{n+1}(G, A) \to \cdots$$

The Standard Complex

One of the important facts about the cohomology groups $H^n(G, A)$ is that they are independent of the chosen resolution. We now present the 'standard resolution', a relatively simple construction allowing us to explicitly compute these groups.

Let P_n be the free $\mathbb{Z}$-module with basis $G \times \ldots \times G$ (with $n+1$ factors). It is a G-module under the action $g \cdot (g_0, g_1, \ldots, g_n) = (g \cdot g_0, g \cdot g_1, \ldots, g \cdot g_n)$. As before, let $K^n = \mathrm{Hom}_G(P_n, A)$. We can then show the following:

- $K^0 = \mathrm{Hom}_G(G, A) \cong A$
- For $n \geq 1$, K^n is the collection of all maps from G^n (n copies of G) to A.

The elements of K^n are known as 'inhomogeneous cochains' and form a cochain complex with the connecting homomorphisms $d^n : K^n \to K^{n+1}$ given by the following:

$$\begin{aligned}(d^n f)(g_1, \ldots, g_{n+1}) &= g_1 \cdot f(g_2, \ldots, g_{n+1}) \\ &\quad + \sum_{i=1}^{i=n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &\quad + (-1)^{n+1} f(g_1, \ldots, g_n) \qquad (2.6)\end{aligned}$$

This is known as the standard complex, from which we can explicitly compute the cohomology groups $H^n(G, A)$ of G with coefficients in A. To demonstrate, we will compute the 'zeroth' and first such groups.

The 'zeroth' group $H^0(G, A)$ is simply $ker(d^0)$. This is a subset of K^0, which we identified with A. Then for $f \in K^0$, $f = a$ for some $a \in A$ and (2.6) gives us

$$(d^0 f)(g) = g \cdot a - a$$

for all $g \in G$. The kernel of this homomorphism is clearly the elements of a fixed under G. In other words, $H^0(G, A) = A^G$, as expected.

To compute the first cohomological group, we must look at the 1-cocycles. They are in the kernel of the map

$$(d^1 f)(g, g') = g \cdot f(g') - f(g \cdot g') + f(g).$$

For f a 1-cocycle, the equation above is equal to zero, and so $f(g \cdot g') = g \cdot f(g') + f(g)$, which is called a *crossed homomorphism*. The 1-coboundaries are functions which obey $f(g) = g \cdot a - a$ for some $a \in A$, as shown in the computation of $H^0(G, A)$. Consider the case when G acts trivially on A. In this case the crossed homomorphisms are actually just homomorphisms, and so $ker(d^1) = \mathrm{Hom}(G, A)$. Furthermore, the only 1-coboundary is the zero function, and so $H^1(G, A) = \mathrm{Hom}(G, A)$ whenever G acts trivially on A.

We will write $H^n(G, \bullet)$ when we wish to discuss the cohomology groups of G without specifying a G-module.

2.2.2 Galois Cohomology

Of special interest is the cohomology of Galois groups. Let F be a field with separable closure $\bar{F}$ and let $G_F = Gal(\bar{F}/F)$ be the absolute Galois group of F. Then the groups $H^i(G_F, \bullet)$ are called the *Galois cohomology groups of* F and denoted $H^i(F, \bullet)$.

We assume F to be a number field and fix p a prime. Let μ_{p^m} denote the group of p^m-th roots of unity and $\mu_{p^m}^{\otimes n}$ the n-fold tensorproduct of this group. Define

$$\mathbb{Z}_p(n) = \varprojlim \mu_{p^m}^{\otimes n}$$

and

$$\mathbb{Q}_p/\mathbb{Z}_p(n) = \mu_{p^\infty}^{\otimes n} = \varinjlim \mu_{p^m}^{\otimes n}.$$

Letting G_F act diagonally on $\mu_{p^m}^{\otimes n}$, we wish to examine the Galois cohomology group

$$H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n)) = \varinjlim H^0(F, \mu_{p^m}^{\otimes n}),$$

consisting of the elements of $\mu_{p^\infty}^{\otimes n}$ invariant under $Gal(F(\mu_{p^\infty})/F)$. Let ζ be a primitive p^m-th root of unity and suppose $\alpha \in G_F$ acts on ζ as $\alpha(\zeta) = \zeta^a$ for some $a \in \mathbb{Z}$. To find the order of $H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n))$ we note that

$$\begin{aligned}
\alpha\left(\zeta^{\otimes n}\right) &= \alpha\left(\zeta \otimes \ldots \otimes \zeta\right) \\
&= \zeta^a \otimes \ldots \otimes \zeta^a \\
&= \left(\zeta^{\otimes n}\right)^{a^n}
\end{aligned}$$

and so α acts on $\mu_{p^m}^{\otimes n}$ in the same way that α^n acts on μ_{p^m}. Then $\mu_{p^m}^{\otimes n}$ is fixed under $Gal(F(\mu_{p^m})/F)$ precisely when the order of this group divides n, and taking the limit we have

$$|H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n))| = \max\left(p^m : Gal(F(\mu_{p^m})/F) \text{ has exponent } n\right).$$

Finally we define

$$w_n(F) = |H^0(F, \mathbb{Q}/\mathbb{Z}(n))| = \prod_p |H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n))|.$$

2.2.3 Étale Cohomology

We now introduce étale cohomology, developed by Alexander Grothendieck in order to prove the Weil Conjectures. Instead of groups and modules, étale cohomology is defined in terms of schemes and sheaves.

We are interested in the étale cohomology groups $H^i_{\text{ét}}(\mathcal{O}_F[\frac{1}{p}], \mu_{p^m}^{\otimes n})$ of the scheme *spec* $\mathcal{O}_F[\frac{1}{p}]$ with values in the étale sheaf $\mu_{p^m}^{\otimes n}$. (For brevity we will write $\mathcal{O}'_F$ for $\mathcal{O}_F[\frac{1}{p}]$ from now on.) These can be identified with Galois cohomology as follows: Let $\Omega_F^{(p)}$ be the maximal algebraic extension of F which is unramified outside primes above p and infinite primes. Let $G_F^{(p)}$ denote the Galois group of this extension, $G_F^{(p)} = Gal(\Omega_F^{(p)}/F)$. We call $H^i(G_F^{(p)}, \bullet)$ the Galois cohomology groups of F with restricted ramification. Then the étale sheaf $\mu_{p^m}^{\otimes n}$ can be viewed as a $G_F^{(p)}$-module with diagonal action and we identify $H^i_{\text{ét}}(\mathcal{O}'_F, \mu_{p^m}^{\otimes n})$ with $H^i(G_F^{(p)}, \mu_{p^m}^{\otimes n})$.

Following the conventions set earlier, we define the *p-adic étale cohomology groups*

$$H^i_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n)) = \varprojlim H^i_{\text{ét}}(\mathcal{O}'_F, \mu_{p^m}^{\otimes n})$$

and

$$H^i_{\text{ét}}(\mathcal{O}'_F, \mathbb{Q}_p/\mathbb{Z}_p(n)) = \varinjlim H^i_{\text{ét}}(\mathcal{O}'_F, \mu_{p^m}^{\otimes n}).$$

The étale cohomology groups are defined for a prime p. We wish to consider them as p-parts of a 'global' cohomology and there are two candidates: Algebraic K-Theory and motivic cohomology. Providing the Bloch-Kato conjecture holds, then for $i = 1, 2$ there are isomorphisms

$$K_{2n-i}(\mathcal{O}_F) \cong H^i_{\mathcal{M}}(\mathcal{O}_F, \mathbb{Z}(n))$$

up to 2-torsion. Of the two, motivic cohomology provides the correct 2-part for étale cohomology: for all p there are isomorphisms

$$H^i_{\mathcal{M}}(\mathcal{O}_F, \mathbb{Z}(n)) \otimes \mathbb{Z}_p \cong H^i_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n)). \tag{2.7}$$

It is believed that the Bloch-Kato Conjecture has been proven by Rost and Voevodsky, though the full proof has not yet been published. If we don't assume Bloch-Kato, we can still construct a global model for $i = 2$ by defining

$$H^2(\mathcal{O}_F, \mathbb{Z}(n)) = \prod_p H^2_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n))$$

and replacing motivic cohomology by this construction in the remainder of the paper.

We will mostly be working with the 2nd étale cohomology groups $H^2_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n))$ for odd p and $n \geq 2$. An important result from [1] and [21] is that these groups are finite for all p and trivial for almost all p. As we shall see, there is a relationship between the order of these groups and special values of Artin L-functions.

We also note that the groups $H^0_{\text{ét}}(\mathcal{O}'_F, \mathbb{Q}_p/\mathbb{Z}_p(n))$ are exactly the Galois groups $H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n))$ discussed earlier.

2.3 Lichtenbaum

Let E/F be a finite abelian extension of totally real number fields with Galois group G. Let p be an odd prime not dividing the order of G. The action of G on E gives a $\mathbb{Z}_p[G]$-module structure to $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$. If M is any $\mathbb{Z}_p[G]$-module, then M can be written as the direct sum of eigenspaces $e_\phi M$ where ϕ runs through the irreducible $\mathbb{Q}_p$-characters of G. For brevity, we sometimes write M^ϕ for $e_\phi M$.

Let χ be an absolutely irreducible component of ϕ. There is a relationship between the Artin L-series of χ evaluated at negative integers $1-n$ and the order of the ϕ-th eigenspace of $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$. There are two cases, depending on whether or not χ is a power of the Teichmüller character, which we now introduce.

Let $\Delta = Gal(F(\mu_p)/F)$. The Teichmüller character

$$\omega : \Delta \to \mu_{(p-1)} \subseteq \mathbb{Q}_p{}^*$$

can be defined by its action on a generator α of Δ. If ζ is a p-th root of unity, then

$$\alpha(\zeta) = \zeta^a$$

for some $a \in \mathbb{Q}_p{}^*$. The order of Δ divides $(p-1)$, so a must also be a $(p-1)$-th root of unity in $\mathbb{Q}_p{}^*$ and we define ω by $\omega(\alpha) = a$.

The result we are interested in is given by Lichtenbaum as Theorem 6.1 in [11]. The theorem assumes the Main Conjecture of Iwasawa Theory, as proven by Wiles in [24]. For the remainder of this paper we write $a \sim_p b$ when the numbers a and b have the same p-adic valuation.

Theorem 2.3. (Lichtenbaum & Wiles) *Let E/F be an abelian extension of totally real number fields. Let ϕ be an irreducible $\mathbb{Q}_p$-character of $Gal(E/F)$ with absolutely irreducible component χ. Let $\mathcal{O}_\chi = \mathbb{Z}_p[\chi]$ and let $d_\chi = [\mathcal{O}_\chi : \mathbb{Z}_p]$. Then for p an odd prime not dividing the order of $Gal(E/F)$ and $n \geq 2$ an even integer we have*

$$L(1-n, \overline{\chi})^{d_\chi} \sim_p |H^2_{\acute{e}t}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\phi|$$

if $\chi \neq \omega^n$ and

$$L(1-n, \overline{\chi}) \sim_p \frac{|H^2_{\acute{e}t}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\phi|}{|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))|}$$

otherwise.

We are going to write Lichtenbaum's theorem as one equation, using some results from [9] and [24]. First we define, for χ an absolutely irreducible character of G, the χ-th component of a $\mathbb{Z}_p[G]$-module M as

$$M^\chi = (M \otimes \mathcal{O}_\chi)^\chi = \{x \in M \otimes \mathcal{O}_\chi | g \cdot x = \chi(g)x \text{ for all } g \in G\}.$$

If χ is a $\mathbb{Q}_p$-character, then this is exactly the χ-th eigenspace of M. On the other hand, if χ is a component of an irreducible $\mathbb{Q}_p$-character ϕ, we can show that $M^\phi \cong M^\chi$. We can therefore replace $|H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\phi|$ with $|H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\chi|$ in Theorem 2.3. We can also look at the χ-th component of $H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))$. This group is cyclic and therefore has only one non-trivial eigenspace, which is exactly the ω^n-th eigenspace. Then $|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))^\chi| = 1$ unless $\chi = \omega^n$. Using this new notation we can restate Theorem 2.3 as

$$L(1-n, \overline{\chi})^{d_\chi} \sim_p \frac{|H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\chi|}{|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))^\chi|}.$$

We can also consider the theorem from a global standpoint. We noted in (2.7) the relationship between étale cohomology and motivic cohomology. If we define

$$H^0(E, \mathbb{Q}/\mathbb{Z}(n))^\chi = \prod_p H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))^\chi$$

then we obtain the global version of Lichtenbaum's theorem, valid for all p not dividing the order of $Gal(E/F)$ and $n \geq 2$ even:

$$L(1-n, \overline{\chi})^{d_\chi} \sim_p \frac{|H^2_{\mathcal{M}}(\mathcal{O}_E, \mathbb{Z}(n))^\chi|}{|H^0(E, \mathbb{Q}/\mathbb{Z}(n))^\chi|}$$

For the principal character χ_0, by Theorem 2.1 we obtain the zeta function $\zeta_F(1-n)$ on the left hand side. The χ_0-th eigenspace of a $\mathbb{Z}_p[G]$-module M is exactly those elements fixed under G. Noting that $|H^0(F, \mathbb{Q}/\mathbb{Z}(n))|$ is just the p-part of $w_n(F)$ and once again assuming that the Bloch-Kato conjecture holds we get

$$\zeta_F(1-n) \sim_p \frac{|H^2_{\mathcal{M}}(\mathcal{O}_F, \mathbb{Z}(n))|}{w_n(F)}.$$

Suppose F is a totally real number field and let $n = 2$. Taking the product over all primes p and replacing motivic cohomology by K-Theory gives us the Birch-Tate conjecture, which holds for all F abelian over $\mathbb{Q}$:

$$\zeta_F(-1) = \pm\frac{|K_2((O)_F|}{w_2(F)}$$

For non-abelian extensions over $\mathbb{Q}$ the Birch-Tate conjecture is true up to possible powers of 2.

We finish with a corollary of Theorem 2.3 regarding the annihilation of the p-adic étale cohomology groups.

Corollary 2.4. *Suppose χ is an absolutely irreducible character of $Gal(E/F)$. If p is an odd prime not dividing the order of $Gal(E/F)$ and $n \geq 2$ an even integer, then*

$$w_n(E)L(1-n,\overline{\chi})^{d_\chi}$$

annihilates $H^2_{\acute{e}t}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\chi$ as a $\mathbb{Z}_p[G]$-module.

Proof. By Lichtenbaum's theorem we know that the order of $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\chi$ is equal to the p-part of $L(1-n,\overline{\chi})^{d_\chi}$ with a factor of $|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))|$ depending on whether or not $\chi = \omega^n$. As $|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))|$ divides $w_n(E)$, we know that $|H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\chi|$ divides the p-part of $w_n(E)\, L(1-n,\overline{\chi})^{d_\chi}$. A finite abelian group is always annihilated by its order, and so it follows that

$$w_n(E)L(1-n,\overline{\chi}) \in Ann_{\mathbb{Z}_p[G]}(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\chi),$$

completing the proof. □

With these tools in place, we are now ready to state and prove the main theorem of this paper.

Chapter 3

Main Theorem and Proof

We defined in this paper's introduction the generalized Stickelberger element

$$\theta_{E/F}(s) = \sum_{\chi \in \hat{G}} L(s, \overline{\chi}) e_{\chi} \tag{3.1}$$

of a finite abelian extension E/F with Galois group $G = Gal(E/F)$. The motivic Coates-Sinnott conjecture predicts that for $n \geq 2$, the integralized Stickelberger element $w_n(E)\theta_{E/F}(1-n)$ should annihilate $H^2_{\mathcal{M}}(\mathcal{O}_E, \mathbb{Z}(n))$. Approaching the problem prime by prime, this reduces to showing that

$$w_n(E)\theta_{E/F}(1-n) \in Ann_{\mathbb{Z}_p[G]}(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n)))$$

for each prime p. We look at a particular family of extensions and show (except for the primes 2 and 3) that this is true.

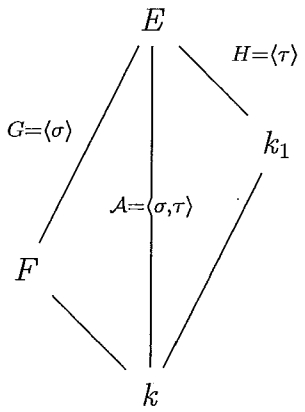
Main Theorem. *Let E/k be an S_3 extension of totally real number fields with quadratic subextension F. Let $G = Gal(E/F)$. For any prime $p \neq 2, 3$ and $n \geq 2$, the integralized Stickelberger element $w_n(E)\theta_{E/F}(1-n)$ is contained in the $\mathbb{Z}_p[G]$-annihilator of the étale cohomology group $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$.*

3.1 Preliminaries

Characters of the Extension

Let $\mathcal{A} = Gal(E/k)$. Then $\mathcal{A}$ is isomorphic to S_3 and generated by two elements, one of order three, which we denote σ, and another of order two, denoted τ. This gives us two subgroups: $G = \langle\sigma\rangle$ and $H = \langle\tau\rangle$. The field F is exactly the subfield of E fixed under G. We denote by k_1 the subfield of E fixed under H. This is all shown in Figure 3.1.

Figure 3.1: Extension Diagram



We are going to need the irreducible characters (over $\mathbb{C}$) of G to define the Stickelberger element. In our proof we will also need the characters of $\mathcal{A}$, H and the quotient group $\mathcal{A}/G$. The methods for finding these characters were explained in Chapter 1 and we summarize the results in Tables 3.1 through 3.4. In each table, we let the zero subscript denote the principal character and ξ a primitive 3rd root of unity.

All these characters have associated Artin L-functions. While only the L-functions over the characters of G are used to construct the Stickelberger element, we will need some of these other L-functions at certain points in the proof. As G and H are subgroups of $\mathcal{A}$, the characters χ, $\overline{\chi}$ and φ induce (not necessarily irreducible) characters of $\mathcal{A}$. Using equation 1.6 on page 12, we find that $\mathrm{Ind}_G^{\mathcal{A}}\chi = \mathrm{Ind}_G^{\mathcal{A}}\overline{\chi} = \Psi_2$ and

$\mathrm{Ind}_H^{\mathcal{A}}\varphi = \Psi_1 + \Psi_2$. Applying Theorem 2.1 we obtain the following useful relationships:

$$L(s, \Psi_2) = L(s, \chi) = L(s, \overline{\chi}) \tag{3.2a}$$

$$L(s, \varphi) = L(s, \Psi_1 + \Psi_2) = L(s, \Psi_1)L(s, \Psi_2) \tag{3.2b}$$

$$L(s, \Psi_1) = L(s, \hat{\Psi}_1) \tag{3.2c}$$

Table 3.1: Characters of $\mathcal{A}$

	1	τ	σ
Ψ_0	1	1	1
Ψ_1	1	-1	1
Ψ_2	2	0	-1

Table 3.2: Characters of G

	1	σ	σ^2
χ_0	1	1	1
χ	1	ξ	ξ^2
$\overline{\chi}$	1	ξ^2	ξ

Table 3.3: Characters of $\mathcal{A}/G$

	G	τG
$\hat{\Psi}_0$	1	1
$\hat{\Psi}_1$	1	-1

Table 3.4: Characters of H

	1	τ
φ_0	1	1
φ	1	-1

The Stickelberger Element

We can now compute the Stickelberger element given in (3.1), using the characters of Table 3.2. As these are linear characters over the complex numbers, the group ring idempotent formula given in equation 1.7 (page 19) reduces to

$$e_\chi = \frac{1}{|G|}\sum_{g \in G} \overline{\chi}(g)g$$

and we can explicitly compute these idempotents for the characters of G:

$$e_{\chi_0} = \frac{1}{3}(1+\sigma+\sigma^2)$$

$$e_{\chi} = \frac{1}{3}(1+\xi^2\sigma+\xi\sigma^2)$$

$$e_{\overline{\chi}} = \frac{1}{3}(1+\xi\sigma+\xi^2\sigma^2)$$

We now write out the Stickelberger element, evaluated at $s = 1-n$:

$$\theta_{E/F}(1-n) = L(1-n,\chi_0)e_{\chi_0} + L(1-n,\chi)e_{\overline{\chi}} + L(1-n,\overline{\chi})e_{\chi} \tag{3.3}$$

We wish to show that $w_n(E)\theta_{E/F}(1-n)$ annihilates the étale cohomology groups $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ for primes $p \neq 2,3$ and $n \geq 2$. We will break $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ into eigenspaces with respect to the $\mathbb{Q}_p$-valued characters of G and show that each of these submodules is in turn annihilated. There are two cases. When 3 divides $(p-1)$, all the characters of G are $\mathbb{Q}_p$-valued and $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ breaks into three submodules. This is the easy case. When 3 does not divide $(p-1)$, we can only break $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ into two submodules, and showing that they are annihilated takes some more work.

For E and F totally real, the L-functions $L(1-n,\chi)$ vanish when n is odd. In this case, the Stickelberger element also vanishes and proving annihilation is trivial. For the rest of this paper, we will restrict ourselves to even $n \geq 2$.

3.2 The Easy Case: $3|(p-1)$

We show that this case is part of a larger theorem:

Theorem 3.1. *Let E/F by a cyclic extension of totally real number fields of degree q*

and p a prime. If q divides $(p-1)$, then $w_n(E)\theta_{E/F}(1-n)$ annihilates $H^2_{\acute{e}t}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ for $n \geq 2$ even.

Proof. Let $G = Gal(E/F)$. As this extension is cyclic, G is abelian and the set of characters in $\hat{G}$ is isomorphic to G itself. We choose a generator χ of $\hat{G}$. As a linear character, it sends G to q-th roots of unity, and as q divides $(p-1)$ we know from Theorem 1.4 that these values lie in $\mathbb{Z}_p$. As $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ is a $\mathbb{Z}_p[G]$-module, we can write it as the sum of simple submodules:

$$H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n)) = \bigoplus_{\chi \in \hat{G}} H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\chi}$$

We need to show that the integralized Stickelberger element

$$w_n(E)\theta_{E/F}(1-n) = \sum_{\chi \in \hat{G}} w_n(E)L(1-n, \chi)e_{\overline{\chi}}$$

annihilates $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$. Due to the orthogonality of the group ring idempotents, this reduces to showing that $w_n(E)L(1-n, \overline{\chi})$ annihilates $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\chi}$ for each character χ, which is true by Corollary 2.4. □

3.3 The Difficult Case: $3 \nmid (p-1)$

In this case $\mathbb{Q}_p$ does not contain 3rd roots of unity, so χ are $\overline{\chi}$ are not $\mathbb{Q}_p$-valued. Then neither are the idempotents e_χ and $e_{\overline{\chi}}$ and the $\mathbb{Z}_p[G]$-module $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ no longer breaks into eigenspaces with respect to these characters. We introduce a new character

$$\phi = \chi + \overline{\chi}$$

which, along with the principal character χ_0, make up the irreducible $\mathbb{Q}_p$-characters of G. The group ring idempotent associated to ϕ is easily calculated:

$$\begin{aligned} e_\phi &= e_\chi + e_{\overline{\chi}} \\ &= \frac{1}{3}(2 - \sigma - \sigma^2) \end{aligned}$$

Then $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ breaks down into the direct sum of two submodules with respect to these characters:

$$H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n)) = H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\chi_0} \oplus H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi}$$

We are going to rewrite the Stickelberger element to reflect these new eigenspaces. The L-functions $L(s, \chi)$ and $L(s, \overline{\chi})$ are equal by (3.2a) and so

$$w_n(E)\theta_{E/F}(1-n) = w_n(E)L(1-n, \chi_0)e_{\chi_0} + w_n(E)L(1-n, \chi)e_\phi.$$

To show that $w_n(E)\theta_{E/F}(1-n)$ annihilates the $\mathbb{Z}_p[G]$-module $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$, it suffices to show that each term annihilates $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ separately. Due to the orthogonality of the idempotents e_{χ_0} and e_ϕ, the problem reduces to proving that $w_n(E)L(1-n, \chi_0)$ annihilates $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\chi_0}$ and that $w_n(E)L(1-n, \chi)$ annihilates $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi}$. The first statement is true by Corollary 2.4, but the second statement will take some work.

Table 3.2 shows us that the image of χ contains 3rd roots of unity. As 3 does not divide $(p-1)$ then $\mu_{(p-1)}$ does not contain 3rd roots of unity and χ cannot be a power of the Teichmuller character. Then by Lichtenbaum's theorem we know that

$$L(1-n, \chi)^2 \sim_p |H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi}|$$

and therefore the order of $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\phi$ is the power of p dividing $L(1-n,\chi)^2$. Unfortunately this isn't good enough; it only shows that $L(1-n,\chi)^2$ annihilates $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\phi$. We claim the following:

Proposition 3.2. *The $\mathbb{Z}_p[G]$-module $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\phi$ can be written as the direct sum of two subspaces, each with order equal to the power of p dividing $L(1-n,\chi)$.*

Proof. So far we have only considered $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ as a $\mathbb{Z}_p[G]$-module. We can also look at the action of H on $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$; as $p \neq 2$, $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))$ will decompose into a direct sum of $\mathbb{Z}_p[H]$-submodules with respect to the idempotents of H given below:

$$e_{\varphi_0} = \frac{1}{2}(1+\tau)$$

$$e_{\varphi} = \frac{1}{2}(1-\tau)$$

We claim that these idempotents commute with e_{χ_0} and e_ϕ, which we computed earlier:

$$e_{\chi_0} = \frac{1}{3}(1+\sigma+\sigma^2)$$

$$e_{\phi} = \frac{1}{3}(2-\sigma-\sigma^2)$$

The elements τ and σ do not commute. However, as they are the generators of $\mathcal{A}$, they obey the relation $\sigma\tau = \tau\sigma^2$. It is easy to show that e_{χ_0} and e_ϕ commute with τ, and therefore with e_{φ_0} and e_φ as well.

As a consequence, the eigenspace $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^\phi$ can be decomposed into subspaces with respect to e_{φ_0} and e_φ:

$$H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi} = (H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi})^{\varphi_0} \oplus (H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi})^{\varphi}. \tag{3.4}$$

To prove the proposition, we need to prove that one of these subspaces has order equal to the power of p dividing $L(1-n, \chi)$. Because the idempotents commute, we note that

$$(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi})^{\varphi} = (H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\phi}$$

and will show that the right-hand side has the desired order.

We begin by looking at the $\mathbb{Z}_p[H]$-module $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi}$. Applying Lichtenbaum's theorem to the extension E/k_1 gives the order of this group:

$$|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\varphi}|\ L(1-n, \varphi) \sim_p |H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi}| \tag{3.5}$$

We decompose this group into subspaces with respect to e_{χ_0} and e_{ϕ}, giving us the direct sum

$$H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi} = (H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\chi_0} \oplus (H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\phi}.$$

Equations 3.2a and 3.2b show that

$$\begin{aligned} L(1-n, \varphi) &= L(1-n, \Psi_1)\ L(1-n, \Psi_2) \\ &= L(1-n, \hat{\Psi}_1)\ L(1-n, \chi) \end{aligned}$$

and so we can rewrite (3.5) as

$$|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\varphi}|\, L(1-n, \hat{\Psi}_1)\, L(1-n, \chi)$$

$$\sim_p |(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\chi_0}| \cdot |(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\phi}|. \quad (3.6)$$

Applying Lichtenbaum's theorem to the extension F/k gives us

$$L(1-n, \hat{\Psi}_1) \sim_p \frac{|H^2_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n))^{\hat{\Psi}_1}|}{|H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\hat{\Psi}_1}|}.$$

We replace $L(1-n, \hat{\Psi}_1)$ in (3.6) by these terms. Then the order of the subspace $(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\phi}$ is the power of p dividing

$$L(1-n, \chi) \cdot \frac{|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\varphi}|}{|H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\hat{\Psi}_1}|} \cdot \frac{|H^2_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n))^{\hat{\Psi}_1}|}{|(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\chi_0}|}$$

which we will show reduces to $L(1-n, \chi)$.

Tables 3.3 and 3.4 show that $\hat{\Psi}_1$ acts on F as φ acts on E. We note that $H^2_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n)) \cong H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\chi_0}$; then $H^2_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n))^{\hat{\Psi}_1} \cong (H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\chi_0})^{\varphi}$ and so

$$\frac{|H^2_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n))^{\hat{\Psi}_1}|}{|(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\chi_0}|} = \frac{|H^2_{\text{ét}}(\mathcal{O}'_F, \mathbb{Z}_p(n))^{\hat{\Psi}_1}|}{|(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\chi_0})^{\varphi}|} = 1.$$

Next we prove that $|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\varphi}| = |H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\hat{\Psi}_1}|$. As E/F is an extension of totally real fields, E and $F(\mu_{p^\infty})$ are disjoint. Then $Gal(F(\mu_{p^\infty})/F) \cong Gal(E(\mu_{p^\infty})/E)$ and so $H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n)) \cong H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))$, giving us

$$\frac{|H^0(E, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\varphi}|}{|H^0(F, \mathbb{Q}_p/\mathbb{Z}_p(n))^{\hat{\Psi}_1}|} = 1.$$

Then $|(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\varphi})^{\phi}| \sim_p L(1-n, \chi)$ as claimed. □

We return to the direct sum decomposition of $H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi}$ given in (3.4):

$$H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi} = (H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi})^{\varphi_0} \oplus (H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi})^{\varphi}$$

As $|H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi}| \sim_p L(1-n, \chi)^2$ and $|(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi})^{\varphi}| \sim_p L(1-n, \chi)$, it follows that $|(H^2_{\text{ét}}(\mathcal{O}'_E, \mathbb{Z}_p(n))^{\phi})^{\varphi_0}| \sim_p L(1-n, \chi)$ as well. Then both these eigenspaces are annihilated by $L(1-n, \chi)$, and therefore the direct sum must be annihilated as well. With both the easy and difficult case solved, we have completed the proof of the main theorem of our thesis.

Bibliography

[1] A. Borel, *Stable real cohomology of arithmetic groups*, Ann. Sci. École Norm. Sup. **7** (1977), 613–636.

[2] J.W.S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press (London), 1967.

[3] J. Coates and W. Sinnott, *An analogue of Stickelberger's theorem for the higher K-groups*, Inv. Math. **24** (1974), 149–161.

[4] P. Deligne and K.A. Ribet, *Values of Abelian L-functions at negative integers over totally real fields*, Inv. Math. **59** (1980), 227–286.

[5] D.S. Dummit and R.M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, 2004.

[6] A. Fröhlich and M.J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press (Cambridge), 1991.

[7] F.Q. Gouvêa, *p-adic Numbers: An Introduction*, Universitext, Springer-Verlag (Berlin Heidelberg), 1997.

[8] I.M. Isaacs, *Character Theory of Finite Groups*, Pure and Applied Mathematics, vol. 69, Academic Press (New York), 1976.

[9] M. Kolster, *Special values of L-functions at negative integers*, PCMI Lecture Notes AMS (2009), to appear.

[10] M. Kolster and J.W. Sands, *Annihilation of motivic cohomology groups in cyclic 2-extensions*, Ann. Sci. Math. Québec **32** (2008).

[11] S. Lichtenbaum, *On the values of zeta and L-functions, I*, Ann. of Math. **96** (1972), no. 2, 338–360.

[12] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag (Berlin Heidelberg), 1999.

[13] B.M. Puttaswamaiah and J.D. Dixon, *Modular Representations of Finite Groups*, Pure and Applied Mathematics, vol. 73, Academic Press (New York), 1977.

[14] J.W. Sands, *Base change for higher Stickelberger ideals*, J. Num. Th. **73** (1998), 518–526.

[15] J.-P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics, vol. 42, Springer-Verlag (New York), 1977.

[16] ———, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag (New York), 1979.

[17] ———, *Galois Cohomology*, Springer-Verlag (Berlin Heidelberg), 1997.

[18] C.L. Siegel, *Über die Fourierschen Koeffizienten von Modulformen*, Nachr. Akad. Wiss. Göttingen **3** (1970), 15–56.

[19] L.D. Simons, *Annihilation of the tame kernel for a family of cyclic cubic extensions*, Ann. Sci. Math. Québec **32** (2008).

[20] V.P. Snaith, *Algebraic K-groups as Galois Modules*, Progress in Mathematics, vol. 206, Birkhäuser (Boston), 2002.

[21] C. Soulé, *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Inv. Math. **55** (1979), 251–295.

[22] L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, Math. Ann. **37** (1890), 321–367.

[23] L.C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag (New York), 1997.

[24] A. Wiles, *The Iwasawa Conjecture for totally real fields*, Ann. of Math. **131** (1990), 493–540.