Tate-Shafarevich Groups of Jacobians of Fermat Curves

by

Benjamin Levitt

A Dissertation Submitted to the Faculty of the

Department of Mathematics

In Partial Fulfillment of the Requirements
For the Degree of

Doctor of Philosophy

In the Graduate College

The University of Arizona

2006

THE UNIVERSITY OF ARIZONA
GRADUATE COLLEGE

As memebers of the Dissertation Committee, we certify that we have read the dissertaion prepared by Benjamin L. Levitt

entitled Tate-Shafarevich Groups of Fermat Curves

and recommend that it be accepted as fulfilling the dissertation requirement for the

Degree of Doctor of Philosophy

______________________________ Date: 28 April 2006
William G. McCallum

______________________________ Date: 28 April 2006
Dinesh Thakur

______________________________ Date: 28 April 2006
Kirti Joshi

______________________________ Date: 28 April 2006
Klaus Lux

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copies of the dissertation to the Graduate Collge.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it be accepted as fulfilling the dissertation requirement.

______________________________ Date: 28 April 2006
Dissertation Director: William G. McCallum

Statement by Author

Acknowledgements

The completion of this dissertation would not have been possible without the help and support of many people.

I would like to thank my advisor, Professor William McCallum, for his guidance on my research and encouragement of my studies. Bill surpassed all reasonable notions of what an advisor should be and it has been a great priveledge to study with him these last few years. He has been an excellent teacher, mentor, and friend. He has my deepest gratitude.

I would also like to thank my wife, Jen Lowe. I owe whatever success I enjoy to her friendship, support, advice, and love. It is unlikely that I will ever be able to repay her for her vital help, but I look forward to about eighty years of trying.

Without the instruction and guidance of Professors Klaus Lux, Dinesh Thakur, Kirti Joshi, and Larry Grove this paper would not have been possible. I am thankful for their help.

Table of Contents

List of Tables

Abstract

For a fixed rational prime p and primitive p-th root of unity ζ, we consider the Jacobian, J, of the complete non-singular curve give by equation $y^p = x^a(1-x)^b$. These curves are quotients of the p-th Fermat curve, given by equation $x^p + y^p = 1$, by a cyclic group of automorphisms. Let $k = \mathbb{Q}(\zeta)$ and k_S be the maximal extension of k unramified away from p inside a fixed algebraic closure of k. We produce a formula for the image of certain coboundary maps in group cohomology given in terms of Massey products, applicable in a general setting. Under specific circumstance, stated precisely below, we can use this formula and a pairing in the Galois cohomology of k_S over k studied by W. McCallum and R. Sharifi in [MS02] to produce non-trivial elements in the Tate-Shafarevich group of J. In particular, we prove a theorem for predicting when the image of certain cyclotomic p-units in the Selmer group map non-trivially into $Ш(k, J)$.

Chapter 1
Introduction

1.1 General Introduction

Algebraic Number Theory is, first and foremost, the study of solutions to polynomial equations with integer coefficients. The same can be said for this dissertation. We begin with the non-singular, complete projective curve given by affine equation

$$y^p = x^a(1-x)^b$$

for a rational prime $p > 3$ and $1 \leq a, b \leq p-1$.

It is natural to ask about the set of solutions to this equation with coefficients in an algebraic extension of $\mathbb{Q}$. In particular, we would like to know the size of this set. However, it proves to be more convenient to first embed the curve inside a variety of higher dimension that has a richer algebraic structure and then ask the same questions about this new variety.

We take the Jacobian variety, J, of the curve, the points of which form an abelian group. The Mordell-Weil Theorem [Wei29] tells us that the group formed by the points of the jacobian that are rational over a finite extension K of $\mathbb{Q}$ is a finitely generated abelian group. Thus, the Fundamental Theorem of Finitely Generated Abelian Groups [Lan65] implies that this group is of the form

$$T \oplus \mathbb{Z}^r,$$

where T is a finite group and the non-negative integer r is called the Mordell-Weil rank of the Jacobian over K.

This rank is an elusive invariant. To get hold of it, an often fruitful strategy employs quotients of $J(K)$ and isogenies in a process called infinite descent (see

[IR90, Chapter 19] for a proof over $\mathbb{Q}$). This process gives rise to Selmer groups, the size of which give an upper bound on the rank of $J(K)$.

The failure of these Selmer groups to give the precise rank is measured by the size of subgroups of the Tate-Shafarevich group of J, denoted $Ш(K, J)$. This group, however, does not willingly subject itself to convenient study. Indeed, $Ш(K, J)$ is not known to be finite (though is conjectured to be so) nor is it demonstrably large, containing conveniently observed elements.

This dissertation proves a computable method for detecting the existence of non-trivial subgroups of $Ш(k, J)$ applicable in specific circumstances.

1.2 Summary of Results

The results of this paper provide ways to detect non-trivial elements in the Tate-Shafarevich group of certain Jacobians J, of Fermat curves defined over cyclotomic fields. This is done as follows:

We prove that non-triviality of elements in $Ш(k, J)$ can be shown by showing that corresponding elements of the Selmer group are not infinitely liftable in some tower of cohomology groups $H^1(G_S, J[\lambda^n]$, where λ is an endomorphism of J and S is a set of primes containing primes of bad reduction and primes dividing the degree of λ. The Selmer groups are contained in these larger cohomology groups, and any element of a Selmer group which is trivial in $Ш(k, J)$ must come from $J(k)/\lambda^n J(k)$, and thus must lift infinitely up the tower (since the map $J(k)/\lambda^{n+1}J(K) \to J(k)/\lambda^n J(K)$ is surjective).

The resulting theorem is the following:

Theorem 1.2.1. *If p is an irregular prime that divides the numerator of the r-th Bernoulli number, B_r, and $p - r + 3 \geq \frac{p+1}{2}$, then $\langle \eta_{p-r+3}, \eta_{p-3} \rangle \neq 0$ implies that the image of η_{p-r+3} in $Ш(J, k)$ is nontrivial.*

Here, $\langle\ ,\ \rangle$ denotes the cup product pairing in [MS02] and η_i are projections of cyclotomic p-units into the ith eigenspace of the action of Galois.

This proof of the theorem is provided in Chapter 4. A list of all of the primes that satisfy Theorem 1.2.1 up to 1000 is given in Table 4.1 and a list up to 10,000 can be found at [Lev]. A comparison to the elements produced in this paper with those found in [McC88] is given in Section 4.1.

The background material required for the proof of the theorem is given in Chapter 2.

Chapter 3 develops a method for computing certain coboundaries in group cohomology using Massey products. It completes Step 2 with a formula applicable in the cohomology of arbitrary groups with coefficient modules isomorphic to $(\mathbb{Z}/p\mathbb{Z})^k$ as groups, with action given by upper triangular matrices of the form

$$\begin{pmatrix} 1 & a_1 & a_2 & \dots & a_{k-1} \\ & 1 & a_1 & \dots & a_{k-2} \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & a_1 \\ & & & & 1 \end{pmatrix}. \tag{1.1}$$

This result is summarized in the Proposition 3.6.4 in Section 3.6. The result characterizes the image of the coboundary of certain distinguished elements in terms of Massey Products, which are defined in Section 3.4.

We exploit the computations done by McCallum and Sharifi in [MS02] for primes less than 15,000 to produce numerous examples of nontrivial subgroups of Ш(k, J).

Chapter 2
Background

2.1 Notation

If G, G' are groups and $\phi' : G \to G'$ is a homomorphism we denote the kernel of ϕ by

$$G[\phi] = \ker(\phi).$$

We use K to signify an arbitrary number field and denote by $\bar{K}$ a fixed algebraic closure of K contained in $\mathbb{C}$. We denote by K^* the multiplicative group of nonzero elements of K, $\mathcal{O}_K$ the ring of integers in K and $Cl(K)$ the ideal class group. The absolute Galois group of K is written

$$G_K = \mathrm{Gal}(\bar{K}/K).$$

For a G_K-module, M, we write $H^i(K, M)$ for the Galois cohomology groups $H^i(G_K, M)$.

We fix an odd rational prime p and choose a primitive p-th root of unity ζ.

We let

$$k = \mathbb{Q}(\zeta)$$

and

$$\Delta = \mathrm{Gal}(k/\mathbb{Q}).$$

The Teichmüller character

$$\omega : G_{\mathbb{Q}} \to (\mathbb{Z}/p\mathbb{Z})^*$$

is defined by

$$\zeta^\sigma = \zeta^{\omega(\sigma)}$$

for $\sigma \in G_{\mathbb{Q}}$.

2.2 Curves and Their Jacobians

In the next chapter we will be concerned with a family curves and their Jacobian varieties. In the first part of this section, we give the definitions and relevant properties of algebraic curves and their associated Jacobian varieties. We then go on to define the family of curves central to this paper and state those properties possessed by members of the family that will be useful in the next chapter.

By a *curve defined over* K we mean a nonsingular, projective, geometrically integral curve defined over the field K. For instance one can take the non-singular projective completion of the affine curve given by an equation of the form

$$f(x, y) = 0.$$

A fundamental invariant of curves is the *genus*. (For $K = \mathbb{C}$ curves can be regarded as real surfaces, and then this corresponds to the topological notion of genus.)

The genus of a curve X, defined over an algebraically closed field, is defined to be

$$g = \dim H^1(X, \mathcal{O}_X).$$

Theorem 2.2.1. *(Riemann-Hurwitz Formula) [e.g. [Har77, IV, cor. 2.4] Let $f : X \to Y$ be a finite separable morphism of curves defined over an algebraically closed field. Let $n = \deg f$. Then*

$$2g(X) - 2 = n \cdot (2g(Y) - 2) + \sum_{P \in Y} (e_P - 1)$$

where the sum is over all closed points in Y and e_P is the ramification degree of P.

For a curve X defined over a number field, K, of characteristic 0, we define the genus of X to be the genus of

$$X_{\bar{K}} = X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K}).$$

We will not give a formal definition of the Jacobian variety of a curve X here. Instead we give the following characterization. For general background in Jacobian varieties we refer the reader to [Mil86c] and for abelian varieties to [Mil86a] or [Har77].

Definition 2.2.2. *For a curve X of genus $g > 0$ defined over K, there is an abelian variety $Jac(X)$ of dimension g, also defined over K, such that, for any extension L/K, the L-rational points of $Jac(X)$ classify L-rational divisor classes of degree zero on X.*

If X has a K-rational point, then any K-rational divisor class contains a K-rational divisor, so we can think of K rational points on the Jacobian as classes of K rational degree zero divisors on X. Furthermore, the structure of $Jac(K)$ as an abelian group can be understood in terms of the group law on the degree zero piece of the divisor class group of X.

Note, then, that the Jacobians of curves of genus 1 are also curves. Such curves are elliptic curves and are the central object of a rich theory. The reader is referred to [Sil86] and [Tat74] for further reading. The curves we will study below are all of higher genus, and thus their Jacobians are abelian varieties of higher dimension.

Let us now return to the curves defined above by (2.2). The action of ζ on the points of $C_{a,b}$ naturally extends to an action on divisors and therefore, on the points of the Jacobian

$$J = Jac(C_{a,b}).$$

Let us now fix an odd rational prime p and consider the p-th Fermat curve

$$F_p : x^p + y^p = 1. \tag{2.1}$$

We fix a primitive p-th root of unity

$$\zeta \in \bar{\mathbb{Q}}$$

and integers $1 \leq a, b \leq p-1$, $a+b \not\equiv 0 \pmod{p}$. Then we can define an automorphism

$$\phi : F_p \to F_p$$

via

$$(x, y) \mapsto (\zeta^b x, \zeta^{-a} y).$$

This automorphism generates an automorphism group of order p, and the quotient of F_p by this group is another curve, the points of which parameterize the orbits of ϕ.

The equation of this quotient curve is

$$C_{a,b} : y^p = x^a(1-x)^b, \quad 1 \le a, b \le p-1, a+b \not\equiv 0 \pmod{p}. \tag{2.2}$$

By changing our choice of generator of the cyclic group of automorphisms generated by ϕ, we can assume that $b = 1$ and the equation of the curve is

$$y^p = x^s(1-x), \quad 1 \le s \le p-2. \tag{2.3}$$

We compute the genus of such a curve by using a map

$$\begin{aligned} f : C_{a,b} \to & \quad \mathbb{P}^1 \\ (x, y) \mapsto & \quad x. \end{aligned}$$

The assumptions on a and b imply that f is ramified at three points: the two affine points $(0, 0)$ and $(1, 0)$ and the point at infinity. For these three points $e_P = p$ and so from Theorem 2.2.1, we find that

$$g(C_{a,b}) = \frac{p-1}{2}. \tag{2.4}$$

We can use our primitive p-th root of unity, ζ to define an automorphism of $C_{a,b}$ which, by abuse of notation, we also call ζ :

$$\begin{aligned} C_{a,b} \to & \quad C_{a,b} \\ (x, y) \mapsto & \quad (x, \zeta_p y). \end{aligned}$$

The action of ζ on the points of $C_{a,b}$ naturally extends to an action on divisors and therefore, on the points of the Jacobian

$$J = Jac(C_{a,b}).$$

We recall that

$$k = \mathbb{Q}(\zeta)$$

and get that

$$\mathbb{Z}[\zeta] \subseteq \mathrm{End}_k(J).$$

Thus, if we let

$$\lambda = 1 - \zeta$$

we have a map, which we also call λ

$$\lambda : J(\bar{k}) \to J(\bar{k}).$$

These Jacobians will be central to the remainder of this paper. So, before moving on, we will collect some useful facts regarding the group structure of $J(k)$ and the rationality of the kernels

$$J[\lambda^i] = \mathrm{Ker}\left(\lambda^i : J(\bar{k}) \to J(\bar{k})\right).$$

Proposition 2.2.3. *[Gre81, Prop. 1] If $p \geq 5$, then*

$$J[\lambda^3] \subseteq J(k).$$

An immediate and obvious consequence of this proposition is that

$$J[\lambda^i] \subset J(k) \quad \text{for } i = 1, 2$$

as well, since

$$J[\lambda^i] \subset J[\lambda^{i+1}]$$

for all i.

Points of torsion for higher powers of λ are not in general rational over k. However, we do have the following characterization of the field over which they are rational.

Let

$$\Delta = \mathrm{Gal}(k/\mathbb{Q})$$

and let

$$\omega : G_{\mathbb{Q}} \to (\mathbb{Z}/p\mathbb{Z})^*$$

be the Teichmüller character, defined in Section 2.1.

Let C be the group of cyclotomic units in k^+, the maximal real subfield of k, and for j even and $2 \le j \le p-3$, let

$$(C/pC)_j = \{c \in C/pC | c^\sigma = \omega^j(\sigma)c \text{ for all } \sigma \in \Delta\}.$$

Then Proposition 8.13 of [Was82] gives us that $(C/pC)_j$ is cyclic of order p. Let η_j be a cyclotomic unit whose image in C/pC generates $(C/pC)_j$. For i odd and $3 \le i \le p-2$, let

$$L_i = k(\sqrt[p]{\eta_j}), \quad j = p - i. \tag{2.5}$$

If Vandiver's conjecture is satisfied (that the index of C in the units of k^+ is not divisible p), then L_i/k is a nontrivial extension. By Kummer theory, the natural conjugation action of Δ on $\mathrm{Gal}(L_i/k)$ is via the character ω^i.

Theorem 2.2.4. *[Gre81, Theorem 4] Let J be the jacobian of $C_{a,b}$, and for odd i, $3 \le i \le p-2$, let*

$$L_i^{(a,b)} = \begin{cases} k & \textit{if } a^i + b^i \equiv (a+b)^i \pmod{p} \\ L_i & \textit{otherwise.} \end{cases}$$

and let L be the compositum of the $L_i^{(a,b)}$. Then $k(J[p]) = L$

Since $\lambda^i | p$ for $1 \le i \le p-1$, this implies that $J[\lambda^{p-1}]$ is rational over the field L in the theorem, and thus so is $J[\lambda^i]$ for all $i \le p-1$.

Note that there is a natural action of Δ on $\mathrm{Gal}(k(J[p])/k)$, and Theorem 2.2.4 tells us that $\mathrm{Gal}(k(J[p])/k)$ is isomorphic to a product of copies of $\mathbb{Z}/p\mathbb{Z}$ and decomposes into eigenspaces of dimension 1 under the action of Δ, with eigenvalues that are odd powers of ω. There is a corresponding expression of L as a compositum of Kummer extensions of k Galois over $\mathbb{Q}$, and these are the $L_i^{(a,b)}$ To describe the smallest subfields of L over which $J[\lambda^i]$ is rational for $i < p-1$, we need the following lemma, the proof of which is given in Section 3.1.

Lemma 2.2.5. *The Galois group G acts on $J[\lambda^{i+1}]/J[\lambda^i]$ via the character ω^{-i}.*

Proposition 2.2.6. *For $2 \le i \le p-2$, we have*

$$k(J[\lambda^{i+1}]) = \begin{cases} k(J[\lambda^i]) & \text{if } i \text{ is even} \\ k(J[\lambda^i])L_i^{(a,b)} & \text{if } i \text{ is odd.} \end{cases}$$

Proof: First, we note that each of the fields $k(J[\lambda^i])$ is Galois over $\mathbb{Q}$, since for $\delta \in \Delta$, λ^δ is a unit times λ. Thus, by Theorem 2.2.4, $k(J[l^i])$ is a compositum of the fields $L_k^{(a,b)}$, where k ranges over some subset of odd k, $2 \le k \le p-2$. We now use Lemma 2.2.5 to identify that subset.

Choose $P \in J[\lambda^{i+1}] \setminus J[\lambda^i]$ such that P is an eigenvector for the action of Δ on $J[\lambda^{i+1}]$. Then, by Lemma 2.2.5,

$$\delta(P) = \omega^{-i}(\delta)P. \tag{2.6}$$

Take $\sigma \in \mathrm{Gal}(k(J[\lambda^{i+1}])/k(J[\lambda^i]))$. Then

$$\lambda(P^\sigma - P) = (\lambda P)^\sigma - \lambda P = \lambda P - \lambda P = 0, \tag{2.7}$$

so

$$\sigma(P) = P + P_0 \tag{2.8}$$

where $P_0 \in J[\lambda]$. Now take $\delta \in \Delta$ and let n be such that $\delta\sigma\delta^{-1} = \sigma^n$. Then

$$\delta\sigma(P) = \delta\sigma\delta^{-1}\delta(P) = \sigma^n\delta(P) = \sigma^n(\omega^{-i}(\delta)P) = \omega^{-i}(\delta)\sigma^n(P) =$$
$$\omega^{-i}(\delta)P + \omega^{-i}(\delta)nP_0. \tag{2.9}$$

by (2.6). On the other hand,

$$\delta\sigma(P) = \delta(P + P_0) = \omega^{-i}(\delta)P + P_0. \tag{2.10}$$

Therefore, if $P_0 \neq 0$, $n = \omega^i(\delta)$ for any $\delta \in \Delta$. That is, if $k(J[\lambda^{i+1}])/k(J[\lambda^i])$ is non-trivial, then Δ acts on $\mathrm{Gal}(k(J[\lambda^{i+1}])/k(J[\lambda^i])$ via ω^i. The Proposition now follows, because Theorem 2.2.4 tells us that the only possible i that can occur as eigenvalues of Galois groups of Kummer extensions in L are odd i satisfying $a^i + b^i \equiv (a+b)^i \pmod{p}$, and for those i the corresponding Kummer extension is $L_i^{(a,b)}$. Furthermore, each such $L_i^{(a,b)}$ must occur somewhere in the tower $k(J[\lambda^i])$.

2.3 Selmer Groups and Bernoulli Numbers

In this section we give the definition of the Selmer group and Tate-Shafarevich group of a variety. We then restrict the discussion to our specific case and describe the decomposition of the Selmer group into a sum of eigenspaces. We end the section by relating the non-triviality of certain eigenspaces to a divisibility property of numerators of Bernoulli numbers. This will allow us to deduce the existence of desired elements of the Selmer group in Chapter 4.

Let A and A' be abelian varieties defined over a number field K with an isogeny

$$\phi : A \to A'$$

defined over a finite extension K of $\mathbb{Q}$. Then we can write the short exact sequence of $G_K = \mathrm{Gal}(\bar{K}/K)$-modules

$$0 \to A(\bar{K})[\phi] \to A(\bar{K}) \to A'(\bar{K}) \to 0.$$

Thus we have a long exact sequence of Galois cohomology groups:

$$\begin{tikzcd} 0 \arrow[r] & H^0(K, A[\phi]) \arrow[r] & H^0(K, A(\bar{K})) \arrow[r, "\phi"] & H^0(K, A'(\bar{K})) \arrow[dll, rounded corners, to path={ -- ([xshift=2ex]\tikztostart.east) |- node[pos=0.75, below]{δ} ([yshift=-2ex, xshift=-18ex]\tikztotarget.north west) |- (\tikztotarget)}] \\ & H^1(K, A[\phi]) \arrow[r] & H^1(K, A(\bar{K})) \arrow[r] & H^1(K, A'(\bar{K})) \arrow[r] & \cdots \end{tikzcd} \tag{2.11}$$

We extract from this the short exact sequence:

$$0 \to A'(K)/\phi(A(K)) \to H^1(K, A(\bar{K})[\phi]) \to H^1(K, A(\bar{K}))[\phi] \to 0 \tag{2.12}$$

For any place v of K we repeat the procedure above, replacing K by K_v, its completion at v, and $\bar{K}$ by $\bar{K}_v$, the completion of $\bar{K}$ at a place above v, and get a short exact sequence analogous to (2.12). Furthermore, associated to each v is a restriction map

$$res : H^i(K, -) \to H^i(K_v, -).$$

So we have the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & A'(K)/\phi A(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, A[\phi]) \arrow[r] \arrow[d, "\prod res_v"'] & H^1(K, A(\bar{K}))[\phi] \arrow[r] \arrow[d, "\prod res_v"'] & 0 \\
0 \arrow[r] & \prod_v A'(K_v)/\phi A(K_v) \arrow[r, "\prod \delta_v"] & \prod_v H^1(K_v, A[\phi]) \arrow[r] & \prod_v H^1(K_v, A(\bar{K}_v))[\phi] \arrow[r] & 0
\end{tikzcd} \tag{2.13}$$

We now define the central objects of interest in the paper:

Definition 2.3.1. *The Selmer group, $S^\phi(A, K)$, is defined as*

$$S^\phi(A, K) = \text{Ker}\left(H^1(K, A[\phi]) \to \prod_v H^1(K_v, A(\bar{K}_v))\right).$$

Thus the Selmer group can be considered as the subgroup of $H^1(K, A(\bar{K}))$ satisfying certain local triviality conditions.

Definition 2.3.2. *The Tate-Shafarevich group, Ш(A, K), is defined to be*

$$Ш(A, K) = \text{Ker}\left(H^1(K, A) \to \prod_v H^1(K_v, A(\bar{K}_v))\right).$$

Elements in Ш(A, K) are represented by cocycles in $H^1(K, A(\bar{K}))$ that are locally trivial (for all places v). The nontrivial elements in Ш(A, K) correspond to those elements in $S^\phi(A, K)$ that are not the image of points of $A'(K)$.

This point of view is represented by the following short exact sequence:

$$0 \to A'(K)/\phi A(K) \to S^{\phi}(A,K) \to Ш(A,K)[\phi] \to 0.$$

Our goal in this paper is to exploit this exact sequence in order to produce non-trivial elements of the Tate-Shafarevich groups of certain varieties over certain number fields. We will establish a method that will take elements of a Selmer group and determine whether its image in the Tate-Shafarevich group is trivial or not. This method reduces the search for non-trivial elements in Tate-Shafarevich to a finite computation. However, it requires us to start with elements we know to be in the Selmer group. So it is natural to consider the structure of this group more closely at this point.

In order to do this as completely as the sections below require, we will specify the varieties and Selmer groups at hand.

Take our prime p and primitive p-th root of unity $\zeta \in \mathbb{C}$. Let X be the projective curve over $\mathbb{Q}$ given by equation

$$y^p = x^a(1-x)^b$$

and let $J = \mathrm{Jac}(X)$ be the Jacobian of X as in Section 2.2. Then multiplication by λ extends to a morphism

$$\lambda : J \to J$$

defined over the field

$$k = \mathbb{Q}(\zeta).$$

These are the same varieties and endomorphisms discussed in Section 2.2.

We recall from Section 2.2 that the kernel of λ is rational over $\mathbb{Q}$ and the points form a cyclic group of order p. Thus both $J[\lambda]$ and μ_p are trivial $\mathrm{Gal}(\bar{k}/k)$-modules. Choosing generators gives us an $\mathrm{Gal}(\bar{k}/k)$-isomorphism

$$J[\lambda] \cong \mu_p$$

and thus an isomorphism

$$H^1(k, J[\lambda]) \cong H^1(k, \mu_p).$$

Kummer theory gives us an isomorphism

$$H^1(k, \mu_p) \cong k^*/k^{*^p}$$

and so we have

$$H^1(k, J[\lambda]) \cong k^*/k^{*^p}. \tag{2.14}$$

Now the definition of the Selmer group $S^\lambda(k, J)$ and the isomorphism (2.14) identifies $S^\lambda(k, J)$ with a subgroup of k^*/k^{*^p}, defined by certain local conditions at every valuation of k. Since J has good reduction outside p, and since λ has degree p, the condition at a valuation v prime to p is simply that the image of the element in k_v/k_v^* lie in the image of the local units. For the valuation above p, the condition is that x lie in the image a certain subgroup W of $k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*p}$, which was calculated by Faddeev in [Fad61]. See also [McC88] for a precise statement. We summarize what is needed from Faddeev's calculation in the following statement.

Proposition 2.3.3. *[Fad61] Let $U^{(i)}$ denotes the units of $k_{\mathfrak{p}}$ congruent to $1 \pmod{\lambda^i}$. Then Faddeev's group W contains the image of $U^{(p+3)/2}$ in $k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*p}$. Thus an element $x \in k^*/k^{*p}$ is in the Selmer group if x_v is in the image of the local units for all v not above p, and $x_{\mathfrak{p}} \in U^{(p+3)/2}$.*

The following lemmas will provide us with readily accessible elements of k^*/k^{*^p} corresponding to elements of $S^\lambda(k, J)$. These elements will be of use to us in the next chapter.

Since every element of k^*/k^{*^p} is of exponent p, we get a natural action of $(\mathbb{Z}/p\mathbb{Z})^*$ on it. Let Δ act on k^*/k^{*^p} through its Galois action on K^*, and consider the eigenspaces

$$k^*/k^{*^p}(\omega^i) = \{\alpha \in k^*/k^{*^p} | \alpha^\sigma = \omega^i(\sigma)\alpha \text{ for every } \sigma \in \Delta\}.$$

For each $1 \leq i \leq p-1$ we define an idempotent element of $\mathbb{Z}_p[\Delta]$ as follows

$$\varepsilon_i = \frac{1}{p-1} \sum_{\sigma \in \Delta} \omega(\sigma)^{-i} \sigma.$$

Then we have that for each $\alpha \in k^*/k^{*p}$,

$$\varepsilon_i \alpha \in k^*/k^{*p}(\omega^i). \tag{2.15}$$

We let $\mathcal{C}$ denote the group of cyclotomic units and define elements

$$\eta_i \equiv (1-\zeta)^{\varepsilon_i} \pmod{\mathcal{C}^p}. \tag{2.16}$$

Under the proper circumstances, certain η_i will represent elements in $S^\lambda(k, J)$. In order to state those circumstances and identify the correct i, we need the following definition.

Definition 2.3.4. *The Bernoulli numbers, B_n, are defined by the following series expansion*

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

Theorem 2.3.5. *If $p | B_i$ for some i even and $2 \leq i \leq p-3$, then the image of the unit η_i in the completion k_λ at the prime $\lambda = 1 - \zeta$ is a p-th power.*

Proof: This follows from [Was82], Theorem 8.25 and Theorem 8.16. □

These results immediately combine to give us the following proposition:

Proposition 2.3.6. *If p satisfies Vandiver's conjecture, and if p divides the numerator of B_i, then η_i is a non-trivial element in the Selmer group $S^\lambda(J, k)$.*

Proof: First, η_i is nontrivial in k^*/k^{*p} because p satisfied Vandiver's conjecture [Was82, Theorem 8.14]. Since $(1-\zeta)$ has valuation 0 at all valuations not dividing p, so does η_i, and so it satisfies the local condition at these valuation. By Theorem2.3.5, η_i is a p-th power locally at the valuation above p, and hence is trivial in $k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*p}$.

Thus, in particular, it satisfies the local condition there as well. Therefore it is in the Selmer group. □

We will use Proposition 2.3.3 to produce different elements in $S^{\lambda}(k, J)$ after giving the following lemma.

Lemma 2.3.7. *If λ is as above and ω is the Teichmüller character defined in section 2.1, then*

$$\lambda^{\sigma} \equiv \omega(\sigma)\lambda \pmod{\lambda^2}$$

for $\sigma \in \Delta$.

Proof: We have that

$$\lambda^{\sigma} = (1-\zeta)^{\sigma} = (1-\zeta^{\sigma}) = (1-\zeta^{\omega(\sigma)}).$$

If we choose an integer $1 \leq n \leq p-1$ so that $n \equiv \omega(\sigma) \pmod{p}$ then we have that

$$\lambda^{\sigma} = (1-\zeta^{n}) = (1-\zeta)(1+\zeta+\cdots+\zeta^{n-1}).$$

Rewriting the second factor we have that

$$\lambda^{\sigma} = (1-\zeta)(n+(\zeta-1)+\cdots+(\zeta^{n-1}-1)) = (1-z)(n+(1-\zeta)t).$$

Thus

$$\lambda^{\sigma} \equiv n\lambda \equiv \omega(\sigma)\lambda \pmod{\lambda^2}.$$

□

Proposition 2.3.8. *If $\frac{p+3}{2} \leq i \leq p-2$ then the image of unit η_i in k^*/k^{*p} is contained in the Selmer group $S^{l}(k, J)$.*

Proof: By Proposition 2.3.3 it is sufficient to check that η_i is in $U^{(p+3)/2}$. Since i is not divisible by $p-1$, and since Δ acts trivially on the residue field of $\mathfrak{p}$, a simple calculation shows that the image of η_i in $k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*p}$ is contained in the image of U^0, and in fact, since U^0/U^1 has order $p-1$, it is contained in the image of U^1. Now, Lemma 2.3.7 implies that Δ acts U^k/U^{k+1} with eigenvalue ω^k. Therefore, since η_i has eigenvalue ω^i, it must be contained in U^i. □

The elements provided by Proposition 2.3.8 will be used in the next chapter to produce non-trivial elements in $Ш(k, J)$.

2.4 The McCallum-Sharifi Pairing

In this section we give a summary of the basic definitions and relevant properties of a cup product pairing studied by McCallum and Sharifi. The reader is referred to [MS02] for the full account.

For fixed odd rational prime p we choose a primitive p-th root of unity ζ and let

$$k = \mathbb{Q}(\zeta).$$

We let k^+ be the maximal real subfield of k, so

$$k^+ = \mathbb{Q}(\zeta + \zeta^{-1})$$

and fix the set

$$S = \{(1-\zeta)\}.$$

We assume that the prime p does not divide the class number of k^+; that is, that p satisfies Vandiver's conjecture.

Now let k_S denote the maximal extension of k unramified outside of the set S and

$$G_{k,S} = \mathrm{Gal}(k_S/k).$$

By the inflation-restriction exact sequence in cohomology [AW67] we have:

$$0 \longrightarrow H^1(G_{k,S}, \mu_p) \xrightarrow{inf} H^1(k, \mu_p) \xrightarrow{res} H^1(k_S, \mu_p) \tag{2.17}$$

and can, therefore, identify $H^1(G_{k,S}, \mu_p)$ with the kernel of the restriction map in (2.17). Kummer theory gives us the isomorphisms [Koc00]

$$H^1(k, \mu_p) \cong k^*/k^{*p}$$

and

$$H^1(k_S, \mu_p) \cong k_S^*/k_S^{*p}.$$

So we have the isomorphism

$$H^1(G_{k,S}, \mu_p) \cong \ker\left(res : k^*/k^{*p} \to k_S^*/k_S^{*p}\right).$$

If we let

$$D_k = \{\alpha \in k^* : \mathrm{ord}_v(\alpha) \equiv 0 \pmod{p} \text{ for all } v \notin S\}$$

then we have that

$$H^1(G_{k,S}, \mu_p) \cong D_k/k^{*p}. \tag{2.18}$$

We let $\mathcal{O}_{k,S}$ denote the ring of S-integers in $\mathcal{O}_k$ and $\mathcal{O}_S$ denote the ring of S-integers in $\mathcal{O}_{k_S}$. Since k_S is the maximal extension of k unramified away from the primes contained in S, it contains the Hilbert class field of k as a subextension. Moreover, k_S contains the Hilbert class field of any of its subfields. Therefore, an ideal $\mathfrak{a}$ of $\mathcal{O}_{k,S}$ becomes principal in $\mathcal{O}_S$. We write $\mathfrak{a} = (\alpha)$ for $\alpha \in k_S^*$. So for $\sigma \in G_{k,S}$ we have that

$$\mathfrak{a}^\sigma = (\alpha)^\sigma = (\alpha)$$

and so

$$\alpha^\sigma = u\alpha$$

for some $u \in \mathcal{O}_S^*$. Now we can associate to $\mathfrak{a}$ in $\mathcal{O}_{k,s}$ the class of the cocycle $(\sigma \mapsto \alpha^\sigma/\alpha)$ in $H^1(G_{k,S}, \mathcal{O}_S^*)$. This gives us a map

$$I_{k,S} \to H^1(G_{k,S}, \mathcal{O}_S^*), \tag{2.19}$$

where $I_{k,S}$ is the group of S-ideals in $\mathcal{O}_{k,s}$.

Hilbert's Theorem 90 gives us that $H^1(G_{k,S}, k_S^*) = 0$. We use this fact together with the exact sequence

$$0 \to \mathcal{O}_S^* \to k_S^* \to P_S \to 0$$

to get that the map (2.19) induces an isomorphism

$$C_{k,S} \cong H^1(G_{k,S}, \mathcal{O}_S^*) \tag{2.20}$$

where $C_{k,S}$ is the S-ideal class group of k. This exact sequence can also be used to show that

$$H^2(G_{k,S}, \mathcal{O}_S^*) = 0 \tag{2.21}$$

in this case, since S has exactly one prime. See [MS02] for details.

Lemma 2.4.1. *If $\alpha \in \mathcal{O}_S^*$, then $\alpha^{1/p} \in k_S$.*

Proof: Take $\alpha \in \mathcal{O}_S^*$ and let

$$L = k(\alpha^{1/p}).$$

Since S contains λ which is the only prime of k above p, the extension L of k is unramified outside of S. But since k_S is the maximal such extension, we have that $L \subseteq k_S$. □

This lemma gives us that p-th power map

$$p : \mathcal{O}_S^* \to \mathcal{O}_S^*$$

is surjective. Thus the sequence

$$0 \longrightarrow \mu_p \longrightarrow \mathcal{O}_S^* \xrightarrow{p} \mathcal{O}_S^* \longrightarrow 0 \tag{2.22}$$

is exact. We use the long exact sequence in the cohomology of $G_{k,S}$ arising from (2.22) to get

$$H^1(G_{k,S}, \mu_p) \longrightarrow H^1(G_{k,S}, O_S^*) \xrightarrow{p} H^1(G_{k,S}, O_S^*) \longrightarrow H^2(G_{k,S}, \mu_p) \longrightarrow \cdots \tag{2.23}$$

Using the isomorphisms (2.20) and (2.21) and tensoring with μ_p we extract the isomorphism

$$C_{k,S}/pC_{k,S} \otimes \mu_p \cong H^1(G_{k,S}, \mu_p^{\otimes 2}). \tag{2.24}$$

By (2.18) above, we can identify elements of D_k with elements of $H^1(G_{k,S}, \mu_p)$. Therefore, from the cup product

$$H^1(G_{k,S}, \mu_p) \times H^1(G_{k,S}, \mu_p) \xrightarrow{\cup} H^2(G_{k,S}, \mu_p^{\otimes 2})$$

we get a pairing

$$(\ ,\ )_S : D_k \times D_k \to C_{k,S}/pC_{k,S} \otimes \mu_p. \tag{2.25}$$

McCallum and Sharifi determined the following formula for $(a,b)_S$. (For a fractional ideal $\mathfrak{a}$, we write $[\mathfrak{a}]$ for the image of $\mathfrak{a}$ in the quotient $C_{k,s}/pC_{k,S}$.)

Theorem 2.4.2. *([MS02], Thm 2.4) Let $a, b \in D_k$, let $\alpha \in k_s^*$ be such that $\alpha^p = a$ and let $L = k(\alpha)$. We let $\mathfrak{b}$ be the ideal of $\mathcal{O}_{k,S}$ such that $b\mathcal{O}_{k,S} = \mathfrak{b}^p$ and write $b = N_{L/k}\gamma$ for some γ. We write*

$$\gamma\mathcal{O}_{L,S} = \mathfrak{c}^{1-\sigma}\mathfrak{b}$$

for ideal $\mathfrak{c}$ of $\mathcal{O}_{L,S}$ and $\sigma \in \mathrm{Gal}(L/k)$. Let $\xi \in \mu_p$ be the root of unity such that $\alpha^\sigma = \xi\alpha$. Then

$$(a,b)_S = [N_{L/k}(\mathfrak{c})] \otimes \xi.$$

In the next chapter, we will not be interested in this pairing directly, but rather in a related pairing which we will now define. We start with a pair (p, r) where p is a prime and r is an even integer $2 \le r \le p-3$ such that p divides the numerator of the r-th Bernoulli number B_r. Such a pair is called an irregular pair. It is equivalent to require that if A_k is the p-part of the ideal class group of k and ω is the Teichmuller character, then the eigenspace $A_k(\omega^{p-r})$ is non-trivial [[Was82], pp. 62-63]. In this case, we fix an isomorphism

$$A_k(\omega^{p-r}) \otimes \mu_p \cong \mathbb{Z}/p\mathbb{Z}(2-r), \tag{2.26}$$

where $\mathbb{Z}/p\mathbb{Z}(2-r)$ is the $G_{k,S}$ module that is group-theoretically isomorphic to $\mathbb{Z}/p\mathbb{Z}$ with module action given by a twist by ω^{2-r}.

We now define a new pairing

$$\langle\ ,\ \rangle_r \tag{2.27}$$

by the commutativity of the following diagram:

$$\begin{tikzcd} D_k \times D_k \arrow[r, "(\ ,\ )_S"] \arrow[dr, bend right, "\langle\ ,\ \rangle_r"'] & C_{k,S}/pC_{k,S} \otimes \mu_p \arrow[d, "(2.26)"] \\ & \mathbb{Z}/p\mathbb{Z}(2-r) \end{tikzcd} \tag{2.28}$$

We will be concerned with the restriction of $\langle\ ,\ \rangle_r$ to cyclotomic units $\mathcal{C} \times \mathcal{C}$. Before ending this section, we will collect some fundamental results regarding this pairing. The proofs can be found in [MS02].

Lemma 2.4.3. *For η_i defined as in* (2.16), *we have that*

$$\langle \eta_i, \eta_j \rangle_r = 0 \text{ if } (p-i) + (p-j) \not\equiv r \pmod{p-1}.$$

Theorem 2.4.4. *([MS02], Theorem 5.1) For all irregular pairs (p, r), with $p < 10{,}000$ there is a non-trivial, Galois equivariant, skew-symmetric pairing*

$$\langle\ ,\ \rangle : \mathcal{C} \times \mathcal{C} \to \mathbb{Z}/p\mathbb{Z}(2-p)$$

satisfying a linear relation on the $\langle \eta_{p-i}, \eta_{r-p+i} \rangle$ (stated in [MS02]). These properties uniquely determine the pairing, up to scalar multiple.

We note that this theorem has been extended for $p < 15{,}000$ by Sharifi. His computations can be found at [SM]. A consequence of this theorem is that the pairing $\langle\ ,\ \rangle_r$ must be a scalar multiple of the pairing provided by Theorem 2.4.4. McCallum and Sharifi conjectured in [MS02] that $\langle\ ,\ \rangle$ is always a non-zero scalar multiple of this non-trivial pairing.

Chapter 3
A Formula for a Coboundary

3.1 The maps δ_k

Let X be the curve over $\mathbb{Q}$ given by

$$y^p = x^s(1-x), \qquad 1 \leq s \leq p-2$$

for an odd rational prime p and let

$$J = \mathrm{Jac}(X)$$

be its Jacobian.

Recall our choice of primitive p-th root of unity ζ, and let

$$k = \mathbb{Q}(\zeta).$$

If we let

$$\lambda = 1 - \zeta$$

then J has complex multiplication by λ and we will consider the short exact sequence of $G_k = \mathrm{Gal}(\bar{k}/k)$-modules for each $1 \leq k \leq p-1$.

$$0 \longrightarrow J[\lambda] \xrightarrow{i} J[\lambda^{k+1}] \xrightarrow{\lambda} J[\lambda^k] \longrightarrow 0\,. \tag{3.1}$$

Let

$$\delta_k : H^1(k, J[\lambda^k]) \to H^2(k, J[\lambda])$$

be the coboundary map for the corresponding long exact sequence.

For each $k \geq 1$, let $S^{\lambda^k}(k, J)$ be the Selmer group of J over k associated to the endomorphism λ^k. Our immediate goal is to give a method to check when elements of S^{λ^k} determine non-trivial elements in $\text{Ш}(k, J)$. We reach this goal by way of the following two lemmas.

Lemma 3.1.1. *If $x \in S^{\lambda^k}(k, J)$ is such that $\delta_k(x)$ is not equal to zero, then the image of x is not equal to 0 in $Ш(k, J)$.*

Proof: Consider a short exact sequence of G_k-modules for each $k \geq 1$

$$0 \longrightarrow J[\lambda^k] \longrightarrow J(\bar{k}) \xrightarrow{\lambda^k} J(\bar{k}) \longrightarrow 0$$

and the long exact sequence in cohomology that arises. This long exact sequence gives us the injection

$$0 \to J(k)/\lambda^k J(k) \to H^1(k, J[\lambda^k]).$$

Putting the sequences for k and for $k+1$ together with the natural surjection:

$$\pi : J(k)/\lambda^{k+1} J(k) \to J(k)/\lambda^k J(k),$$

we form the following commutative diagram:

$$\begin{tikzcd} 0 \arrow[d] & 0 \arrow[d] & \\ J(k)/\lambda^{k+1}J(k) \arrow[r, "\pi"] \arrow[d] & J(k)/\lambda^k J(k) \arrow[d] & \\ H^1(k, J[\lambda^{k+1}]) \arrow[r, "\lambda_*"] & H^1(k, J[\lambda^k]) \arrow[r, "\delta_k"] & H^2(k, J[\lambda]). \end{tikzcd} \tag{3.2}$$

We expand the diagram (3.2) to incorporate this information.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & \\
J(k)/\lambda^{k+1}J(k) \arrow[r, "\pi"] \arrow[d] & J(k)/\lambda^k J(k) \arrow[d] & \\
S^{\lambda^{k+1}}(k,J) \arrow[r, "\lambda_*"] & S^{\lambda^k}(k,J) \arrow[r, "\delta_k"] \arrow[d] & H^2(k,J[\lambda]) \\
& Ш(k,J)[\lambda^k] \arrow[d] & \\
& 0 &
\end{tikzcd} \tag{3.3}$$

Therefore, if x is an element of $S^{\lambda^k}(k,J)$ that is trivial in $Ш(k,J)[\lambda^k]$, it comes from an element of $J(k)/\lambda^k J(k)$. Then taking a preimage under the surjection π and injecting into $S^{\lambda^{k+1}}(k,J)$ shows that x is in the image of λ_* and thus, $\delta_k(x)$ is zero.$\square$

Lemma 3.1.1 makes the image of δ_k of particular interest. Later in this chapter we will return to study this coboundary map.

3.2 The Structure of $J[\lambda^k]$

In this section we give a more explicit description of the structure of the torsion subgroups $J[\lambda^k]$ as G_k-modules. This will eventually provide a concrete description of the image of the coboundary map δ_k of the previous section.

Lemma 3.2.1. *For* $1 \leq k \leq p-1$

$$J[\lambda^k] \cong (\mathbb{Z}/p\mathbb{Z})^k$$

as $\mathbb{F}_p$*-vector spaces.*

Proof: Since $\lambda^{p-1}|p$, we have that p annihilates each $J[\lambda^k]$, $1 \leq k \leq p-1$ and so each group is a $\mathbb{F}_p$ vector space. All that is left to determine are the dimensions.

We do so by considering the degree of the map λ. The degree of multiplication by p on the jacobian of a genus g curve is p^{2g}. We found in (2.4) that the genus of $C_{a,b}$ is $\frac{p-1}{2}$. Therefore the degree of multiplication by p on J is also p^{p-1}. Since $\lambda^{p-1} = (p)$ as ideals, multiplication by λ^{p-1} and by p have the same degree. Thus

$$\deg(\lambda^{p-1}) = \deg(\lambda)^{p-1} = \deg(p) = p^{p-1} \tag{3.4}$$

$$\deg(\lambda) = p. \tag{3.5}$$

Thus $\deg(\lambda^k) = p^k$ for $1 \leq k \leq p-1$. $\square$

We use the convention of writing elements of $(\mathbb{Z}/p\mathbb{Z})^k$ as column vectors. This provides a k-dimensional representation of G_k over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We can determine the nature of this representation more precisely by way of the following lemma.

Lemma 3.2.2. *The Galois group $\mathcal{G}_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $J[\lambda^k]/J[\lambda^{k-1}]$ via ω^{1-k}, where ω is the Teichmuller character.*

Proof: For $k = 1$ we have that $J[\lambda]$ is rational over $\mathbb{Q}$ [2.2.4], and so this case is obvious.

To finish the proof we recall from Lemma 2.3.7 that $\lambda^\sigma \equiv \omega(\sigma)\lambda \pmod{\lambda^2}$. Now, if we take $P \in J[\lambda^{k+1}]$ and assume that the claim holds for $k \geq 1$, then $\lambda P \in J[\lambda^k]$ and our assumption says that

$$(\lambda P)^\sigma \equiv \omega^{1-k}(\sigma)(\lambda P) \pmod{J[\lambda^{k-1}]}.$$

Since $k \geq 1$, we have

$$(\lambda P)^\sigma = \lambda^\sigma P^\sigma \equiv \omega(\sigma)\lambda P^\sigma \pmod{J[\lambda^{k-1}]}.$$

So

$$\omega(\sigma)\lambda P^\sigma \equiv \omega^{1-k}(\sigma)\lambda P \pmod{J[\lambda^{k-1}]}$$

and

$$\lambda P^\sigma \equiv \lambda\omega^{1-(k+1)}(\sigma)P \pmod{J[\lambda^{k-1}]}$$

and therefore

$$P^\sigma \equiv \omega^{1-(k+1)}(\sigma)P \pmod{J[\lambda^k]}.$$

$\square$

Since every $\sigma \in G_k$ fixes ζ, we conclude that the action of G_k on $J[\lambda^k]/J[\lambda^{k+1}]$ is trivial.

Choosing an ordered $\mathbb{Z}/p\mathbb{Z}$ basis for$J[\lambda^k]$,

$$\mathcal{B}_k = \{\alpha_1, \ldots, \alpha_k\},$$

where α_i is a λ^i-torsion point and

$$\lambda\alpha_i = \alpha_{i-1},$$

we see that the matrix of the representation of G_k corresponding to the module $J[\lambda^k]$ is lower triangular, with ones along the diagonal.

Let us call this representation

$$\rho_k : G_k \rightarrow \mathrm{GL}_k\left(\mathbb{Z}/p\mathbb{Z}\right)$$

and write

$$\rho_k(\sigma) = \begin{pmatrix} 1 & a_{1,2}(\sigma) & a_{1,3}(\sigma) & \ldots & a_{1,k}(\sigma) \\ & 1 & a_{2,3}(\sigma) & \ldots & a_{2,k}(\sigma) \\ & & \ddots & \ddots & \vdots \\ & & & 1 & a_{k-1,k}(\sigma) \\ & & & & 1 \end{pmatrix}.$$

Since λ is defined over k, we have that

$$(\lambda\alpha_i)^\sigma \quad = \quad \lambda(\alpha_i)^\sigma, \qquad \text{for every } \sigma \text{ in } G_k.$$

Expanding each side of this equation we get

$$\begin{aligned}
(\alpha_{i-1})^\sigma &= \lambda(\alpha_i^\sigma) \\
\alpha_{i-1} + \sum_{j=1}^{i-2} a_{j,i-1}\alpha_j &= \lambda(\alpha_i + \sum_{j=1}^{i-1} a_{j,i}\alpha_j) \\
&= \alpha_{i-1} + \sum_{j=1}^{i-2} a_{j+1,i}\alpha_j
\end{aligned}$$

Setting the coefficients equal, we have that

$$a_{j-1,i-1} = a_{j,i}$$

for all $1 \leq j \leq i-1$ and for all i. Thus, all of the entries in each subdiagonal of $\rho(\sigma)$ are equal. This provides a simpler form of the matrix, namely

$$\rho_k(\sigma) = \begin{pmatrix} 1 & a_1(\sigma) & a_2(\sigma) & \dots & a_{k-1}(\sigma) \\ & 1 & a_1(\sigma) & \dots & a_{k-2}(\sigma) \\ & & \ddots & \ddots & \vdots \\ & & & 1 & a_1(\sigma) \\ & & & & 1 \end{pmatrix}. \tag{3.6}$$

Furthermore, Proposition 2.2.4 gives us that $J[\lambda^3]$ is rational over k; that is, G_k acts trivially on $J[\lambda^3]$. This implies that $a_1(\sigma) = a_2(\sigma) = 0$ for all $\sigma \in G_k$. Therefore, the matrix (3.6) simplifies to

$$\rho_k(\sigma) = \begin{pmatrix} 1 & 0 & 0 & a_3(\sigma) & \dots & a_{k-1}(\sigma) \\ & \ddots & \ddots & \ddots & \ddots & \vdots \\ & & 1 & 0 & 0 & a_3(\sigma) \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{pmatrix} \tag{3.7}$$

The description of the coboundary map we obtain will be in terms of this representation.

Motivated by this problem, we consider a more general situation, and study analogous coboundaries for a larger class of G_k modules. The image of the coboundary map above will then be determined explicitly as a corollary to the more general case.

3.3 A More General Family of Modules

In this section we construct families of modules of a group G, $\{V_k\}, \{W_i\}$, and $\{W^{(j)}\}$ that generalize the G_k structure of the family of the $J[\lambda^k]$ in the previous section. We will then consider the analogous coboundary maps and give a useful description of its image in terms of representations similar to the ρ_k given above. In Section 4.1, we will see how to relate these more general results to $J[\lambda^k]$ and use this to prove non-triviality of $\text{Ш}(k, J)$ in certain cases.

Let $V_k = (\mathbb{Z}/p\mathbb{Z})^k$ and take a unipotent representation

$$\rho : G \to \text{Aut}(V_k)$$

$$\rho(\sigma) = \begin{pmatrix} 1 & a_{1,k-1}(\sigma) & a_{2,k-2}(\sigma) & \dots & a_{k-1,1}(\sigma) \\ & 1 & a_{1,k-2}(\sigma) & \dots & a_{k-2,1}(\sigma) \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & a_{1,1}(\sigma) \\ & & & & 1 \end{pmatrix}.$$

Note the unconventional indexing. We are using the first index to count the diagonals and the second to count the distance from the right hand side.

The representation ρ makes V_k into a G_k-module. We give $\mathbb{Z}/p\mathbb{Z}$ the trivial G action and can consider extensions of $\mathbb{Z}/p\mathbb{Z}$ by V_k, that is, elements in $\text{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k)$.

We can represent an element of $\text{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k)$ by a short exact sequence of G-modules:

$$0 \to V_k \to M \to \mathbb{Z}/p\mathbb{Z} \to 0, \tag{3.8}$$

where M is a $k+1$ dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ with basis chosen so that the injection in (3.8) is inclusion into the first k components and the surjection is projection onto the last. The G-module structure of M is then given via a matrix of the form:

$$\begin{pmatrix} 1 & a_{1,k-1} & a_{2,k-2} & \dots & a_{k-1,1} & \chi_k \\ & 1 & a_{1,k-2} & \ddots & \dots & \chi_{k-1} \\ & & \ddots & \ddots & a_{2,1} & \vdots \\ & & & 1 & a_{1,1} & \chi_2 \\ & & & & 1 & \chi_1 \\ & & & & & 1 \end{pmatrix}. \tag{3.9}$$

Lemma 3.3.1. *If $M = (\mathbb{Z}/p\mathbb{Z})^{k+1}$ is a G-module with action given by* (3.9)*, then the χ_i satisfy the following condition:*

$$\chi_i(\sigma\tau) = \chi_i(\sigma) + \chi_i(\tau) + \sum_{j=1}^{i-1} a_{j,i-j}(\sigma)\chi_{i-j}(\tau).$$

Proof: This follows immediately from the fact that the matrix above comes from a representation of G. $\square$

Thus, elements of $\mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k)$ can be represented by modules $M \cong (\mathbb{Z}/p\mathbb{Z})^{k+1}$ with G action given by matrices of the form (3.9) whose last column satisfy Lemma 3.3.1. The next lemma will provide us with the converse of this statement.

The following lemmas will establish a relationship between elements of $H^1(G, V_k)$ and modules M satisfying lemma 3.3.1.

Lemma 3.3.2. *If $M = (\mathbb{Z}/p\mathbb{Z})^{k+1}$ and the matrix representing the G action on M is of the form* (3.9) *and is such that the elements in the rightmost column satisfy Lemma 3.3.1, then M is an extension of V_k by $\mathbb{Z}/p\mathbb{Z}$.*

Proof: It is obvious that the sequence (3.8) is an exact sequence of G modules in this case. $\square$

Lemma 3.3.3. *There is an exact sequence*

$$0 \longrightarrow V_k^G \longrightarrow \mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k) \longrightarrow H^1(G, V_k) \longrightarrow 0. \tag{3.10}$$

Proof: If we let $\mathbb{Z}$ be a trivial G module, then we have an exact sequence of G-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

This gives a long exact sequence of $\mathrm{Ext}^i_G(-, V_k)$ groups [HS71, p. 139]:

$$\mathrm{Ext}^0_G(\mathbb{Z}, V_k) \xrightarrow{p} \mathrm{Ext}^0_G(\mathbb{Z}, V_k) \longrightarrow \mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k) \longrightarrow \mathrm{Ext}^1_{G_k}(\mathbb{Z}, V_k) \xrightarrow{p} \tag{3.11}$$

Since V_k are of exponent p, multiplication by p is just the zero map by the definition of Ext_G groups [Bro82, ch. III, section 2] or [HS71, ch. IV, section 6], so this diagram can be written:

$$0 \longrightarrow \mathrm{Ext}^0_G(\mathbb{Z}, V_k) \longrightarrow \mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k) \longrightarrow \mathrm{Ext}^1_G(\mathbb{Z}, V_k) \longrightarrow 0. \tag{3.12}$$

And by [Bro82, p. 61], $\mathrm{Ext}^1_G(\mathbb{Z}, V_k) = H^1(G, V_k)$, giving us the exact sequence

$$0 \to V_k^{G_k} \to \mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k) \to H^1(G, V_k) \to 0. \tag{3.13}$$

□

We remark that in the case $V_k = \mathbb{Z}/p\mathbb{Z}$, elements of $H^1(G, V_k)$ are characters $\chi : G \to \mathbb{Z}/p\mathbb{Z}$. Such an element can be lifted in the exact sequence of Lemma 3.3.3 to an extension of $\mathbb{Z}/p\mathbb{Z}$ by itself on which G acts via the matrix

$$\begin{pmatrix} 1 & \chi \\ 0 & 1 \end{pmatrix}$$

Lemmas 3.3.2 and 3.3.3 tell us that every element of $H^1(G, V_k)$ can be represented by a module M satisfying the conditions of Lemma 3.3.2. Extensions M and M' determine the same element in $\mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k)$ if and only if there is an isomorphism ϕ making the following diagram commute:

$$\begin{tikzcd}
0 \arrow[r] & V_n \arrow[r] \arrow[d, equal] & M \arrow[r] \arrow[d, "\phi"] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & V_n \arrow[r] & M' \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & 0.
\end{tikzcd} \tag{3.14}$$

If we choose bases for M and M' so that the maps in the rows of (3.14) are as they are in (3.8), then the G actions on M and M' are given by matrices A and A' of the form (3.9). So we can specify a matrix representation of the isomorphism ϕ in (3.14). Indeed, the commutativity of (3.14) forces ϕ to be of the form

$$[\phi] = \begin{pmatrix} & & & \phi_1 \\ & I_k & & \vdots \\ & & & \phi_k \\ 0 & \dots & 0 & 1 \end{pmatrix} \tag{3.15}$$

where ϕ_i are functions $G \to \mathbb{Z}/p\mathbb{Z}$. Lemma 3.3.4 will specify this ambiguity in terms of the entries in the matrix (3.9) and the matrix (3.15) representing the isomorphism ϕ.

Lemma 3.3.4. *Let M and M' be G modules satisfying the hypotheses of Lemma 3.3.1 with G action given by matrices A and A', respectively. Let $[\chi_k, \dots, \chi_1, 1]^T$ and $[\chi'_k, \dots, \chi'_1, 1]^T$ be the $k+1$-th columns of A and A', respectively. If M and M' determine the same element in $\mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k)$, then*

$$\chi_i = \chi'_i + \sum_{j=1}^{i-1} a_{j,i-j}\phi_j.$$

Proof: ϕ is a G-isomorphism so for all $\sigma \in G$, if $m \in M \cong (\mathbb{Z}/p\mathbb{Z})^{k+1}$ then $\phi(m^\sigma) = \sigma\phi(m)$. So

$$[\phi] \cdot A(\sigma)m = A'(\sigma) \cdot [\phi]m.$$

Writing m as a $k+1$-dimensional column vector, we derive the formula above by expanding both sides of the equation. □

This says that modules M of rank $k+1$ over $\mathbb{Z}/p\mathbb{Z}$ with G action given by a matrix of the form (3.9) determines an element of $\mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k)$ and conversely, every element of $\mathrm{Ext}^1_G(\mathbb{Z}/p\mathbb{Z}, V_k)$ can be represented by such a module, with choice of χ_i as specified in Lemma 3.3.4. This characterization of elements in $H^1(k, V_k)$ will be of use below.

3.4 Coboundary Maps and Massey Products

We begin this section by defining certain submodules and quotient modules of the V_k of Section 3.3. These new modules will be used with V_k to produce long exact sequences in G cohomology. Certain coboundary maps in these long exact sequences will be related back to $J[\lambda^k]$ and the maps δ_k from Section 3.1.

We let W_i be the subrepresentation of V_k consisting of vectors with entries equal to zero after the i-th component, and let and $W^{(i)}$ be the quotient representation V_k/W_{k-i}. Thus G acts on W_i (resp. $W^{(i)}$) via the upper left (resp. lower right) $i \times i$ block of the matrix (3.9). We get an exact sequence:

$$0 \to W_1 \to V_k \to W^{(k-1)} \to 0.$$

The maps

$$H^1(G, W_1) \to H^1(G, V_k) \to H^1(k, W^{(k-1)}) \tag{3.16}$$

are induced from the natural inclusion and projection maps, respectively. We calculate the image of the coboundary map

$$\delta_k : H^1(G, W^{(k-1)}) \to H^2(G, W_1).$$

For the case $k = 2, i = 1$, we have the following lemma.

Proposition 3.4.1. *If G acts on V_2 via multiplication by*

$$\begin{pmatrix} 1 & a_{1,1} \\ 0 & 1 \end{pmatrix}$$

and $x \in H^1(G, W^{(1)})$, then $a_{1,1}$ is a cocycle with coefficients in $\mathbb{Z}/p\mathbb{Z}$ and

$$\delta_2(x) = x \cup a_{1,1}$$

Note that $W^{(1)}$ and W_1 are both just $\mathbb{Z}/p\mathbb{Z}$ and we are writing $a_{1,1} \cup x$ for the image of the cup product of x and $a_{1,1}$ in $H^2(G, W_1)$ under the map induced by the multiplication map

$$W_1 \otimes W_1 \to W_1.$$

Proof: We check directly that $a_{1,1}$ is actually a homomorphism and therefore represents a class in $H^1(G, W^{(1)})$ (since G acts trivially on $W^{(1)}$).

Now, if we take a representative x for an element in $H^1(G, W_1)$ then we can lift it to the cochain

$$\bar{x} = (0, x) : G \to W_2.$$

Since $W_1 = \mathbb{Z}/p\mathbb{Z}$ is a trivial G module, we can choose x to be a homomorphism $G \to W_1$. Then $\delta_2(\bar{x})$ is represented by the cocycle

$$\begin{aligned} \delta(x)(\sigma, \tau) &= (0, x(\sigma\tau))^t - (0, x(\sigma))^t - \begin{pmatrix} 1 & a_{1,1}(\sigma) \\ 0 & 1 \end{pmatrix} (0, x(\tau))^t \\ &= -(a_{1,1}(\sigma)x(\tau), 0) = -(a_{1,1} \cup x)(\sigma, \tau). \end{aligned}$$

Thus the coboundary is $-(a_{1,1} \cup x)$, which is equal to $x \cup a_{1,1}$ by skew-symmetry of of the cup product on H^1. $\square$

Our goal is to generalize this formula for modules of higher rank. However, it is easy to check that the $a_{i,j}$ are not, in general, homomorphisms for $i, j > 1$, and do not represent cohomology classes. A formula for higher rank modules must therefore be of a more complicated nature. It is in the interest of determining this more complicated nature that we include the following definition.

Definition 3.4.2. *A defining system for the n-fold Massey product $\langle \alpha_1, \ldots, \alpha_n \rangle$ is an array, M, of cochains m_{ij} in $C^1(G, R)$ for a group G and R a ring with identity.*

$$M = \{m_{ij} | 1 \leq i < j \leq n+1, (i,j) \neq (1, n+1)\}$$

such that

(i) $m_{i,i+1}$ *is a representative of* α_i *for each* $i = 1, \dots, n$, *and*

(ii) $dm_{ij} = \sum_{k=i+1}^{j-1} m_{ik} \cup m_{kj}$, *for* $j \neq i+1$.

The value of the Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ is represented by the cocycle in $H^2(G, R)$

$$\sum_{k=2}^{n} m_{1,k} \cup m_{k,n+1}. \tag{3.17}$$

Note that the 2-fold Massey product is just the cup product. In general, however, the Massey product is not a well defined element of $H^2(G, R)$. Indeed, it depends upon the choice of defining system. However, this product is well defined in a certain quotient of $H^2(G, R)$. We will give a precise description of this quotient below. Before we do, we will state a theorem of Dwyer that gives a convenient re-characterization of Massey products.

Theorem 3.4.3. *[Dwy75, thm. 2.4] Let* $U(R, n)$ *be the group of upper* $n \times n$ *triangular matrices over* R *with ones along the diagonal. Let* $Z(R, n)$ *be the subgroup of* $U(R, n)$ *that has its only non-zero, non-diagonal entry in position* $(1, n)$. *Now let*

$$\bar{U}(R, n) = U(R, n)/Z(R, n).$$

Then the set of defining systems for the Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ *is in bijection with the set of homomorphisms* $\phi : G \to \bar{U}(R, n+1)$ *where* $\phi = (\phi_{i,j})$ *with* $\phi_{i,i-1} = -\alpha_i$ *for each* $i = 1, \dots, n$. *Moreover,* $\langle \alpha_1, \dots, \alpha_n \rangle = 0$ *in* $H^2(G, R)$ *if and only if the dotted arrow exists in the diagram:*

$$\begin{tikzcd} & U(R, n+1) \arrow[d] \\ G \arrow[ur, dashed] \arrow[r, "\phi"'] & \bar{U}(R, n+1). \end{tikzcd} \tag{3.18}$$

A homomorphism $\phi : G \to \bar{U}(R, n+1)$ can be represented by an $(n+1) \times (n+1)$-matrix $(\phi_{i,j})$ where $\phi_{i,i} = 1$ and $\phi_{i,j} = 0$ whenever $i > j$. The condition that ϕ be a homomorphism forces the nonzero $\phi_{i,j}$ to satisfy the following condition:

$$\phi_{i,j}(\sigma\tau) = \phi_{i,j}(\sigma) + \phi_{i,j}(\tau) + \sum_{k=i+1}^{j-1} \phi_{i,k}(\sigma)\phi_{k,j}(\tau) \tag{3.19}$$

for all $\sigma, \tau \in G$ where $1 \leq i < j \leq n+1$ (and $(i,j) \neq (1, n+1)$). This also forces the off diagonal elements, $\phi_{i,i+1}$, to be homomorphisms.

We return to the modules of section 3.3. By Lemma 3.3.3 and the remark following we can represent an element $\xi \in H^1(G_k, W^{(1)})$ by a matrix

$$\begin{pmatrix} 1 & \chi_1 \\ 0 & 1 \end{pmatrix}, \tag{3.20}$$

and by Lemma 3.4.1 the coboundary of ξ is $\chi_1 \cup a_{1,1},$.

We interpret Lemma 3.4.1 in terms of Massey products in the following lemma:

Lemma 3.4.4. *If $\xi \in H^1(G, W^{(1)})$ is represented by a matrix*

$$\begin{pmatrix} 1 & \chi_1 \\ & 1 \end{pmatrix}$$

then $\delta_2(\xi) = 0 \in H^2(G, W_1)$ if and only if the value of the Massey product with defining system $\langle -a_{1,1}, -\chi_1 \rangle$ is 0.

Note that this result can also be seen directly from Theorem 3.4.3, since the value of $\langle -a_{1,1}, -\chi_1 \rangle$ is 0 if and only if there is a map $\phi_2 : G \to W_1$ so that the following matrix is a homomorphism $G \to U(W_1, 3)$

$$\begin{pmatrix} 1 & a_{1,1} & \phi_2 \\ & 1 & \chi_1 \\ & & 1 \end{pmatrix}.$$

By Lemma 3.3.3, such a homomorphism represents an element of $\xi_2 \in H^1(G, V_2)$, which is a lift of ξ.

In the next section we define a filtration on the cohomology groups of a subfamily of modules, producing quotients in which the relevant Massey products are well defined. This will enable us to strengthen Lemma 3.4.4 and generalize it to coboundary maps of higher degree.

3.5 A Filtration of Cohomology

Let us now define modules modules M_k which will serve as a stepping stone between the V_k of section 3.3 and $J[\lambda^k]$. Let

$$M_k = (\mathbb{Z}/p\mathbb{Z})^k \text{ as } \mathbb{Z}/p\mathbb{Z}\text{-vector spaces}$$

with standard basis $\langle \alpha_k, \dots, \alpha_1 \rangle$, viewed as column vectors. We give M_k a G-module structure as follows:
The action on M_1 is trivial and for $k \geq 2$, an element σ of G acts on M_k via the $k \times k$-matrix

$$\begin{pmatrix} 1 & a_1 & a_2 & \dots & a_{k-1} \\ & 1 & a_1 & \dots & a_{k-2} \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & a_1 \\ & & & & 1 \end{pmatrix} \tag{3.21}$$

for maps $a_1, \dots, a_{k-1} : G \to \mathbb{Z}/p\mathbb{Z}$ that make this into a representation. We note that this construction is equivalent to that of the V_k where we are insisting that $a_{i,j} = a_{i,l}$ for all $1 \leq j, l \leq k - i$. We also note that this mimics the structure of the representations coming from $J[\lambda^k]$ in (3.7).

The a_i are not themselves homomorphisms for $i \geq 2$, but rather satisfy the condition

$$a_i(\sigma\tau) = a_i(\sigma) + \sum_{j=1}^{i-1} a_j(\sigma)a_{i-j}(\tau) + a_i(\tau). \tag{3.22}$$

(We have already seen this condition above, as it is satisfied by the maps in a defining system of a Massey product (3.4) and by the $a_{i,j}$ in the definition of the G-module structure of the V_k in Lemma 3.3.1.)

By choosing injections $M_i \to M_j$, for $i \leq j$, to be inclusion into the first i positions and surjections $M_j \to M_k$, for $k \leq j$, to be projection onto the last j positions, we get the commutative diagram of G-modules

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & M_h \arrow[r] \arrow[d] & M_i \arrow[r] \arrow[d] & M_j \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_k \arrow[r] \arrow[d] & M_l \arrow[r] \arrow[d] & M_m \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_u \arrow[r] \arrow[d] & M_v \arrow[r] \arrow[d] & M_w \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd} \tag{3.23}$$

where $h + u = k$, $i + v = l = k + m$, $j + w = m$, $h + j = i$, and $u + w = v$.

We consider the long exact sequences in cohomology that arise from sequences of the form

$$0 \to M_1 \to M_{j+1} \to M_j \to 0 \tag{3.24}$$

for each $j \geq 1$.

We index the coboundary from $H^1(G, M_j)$ to $H^2(G, M_1)$ by the dimension of the quotient. That is, for the sequence (3.24), we have

$$\delta_j : H^1(G, M_j) \to H^2(G, M_1).$$

Partially motivated by the ambiguity introduced by the Massey products of the previous section, we define a descending filtration, $F^{\cdot}$, on $H^1(G, M_1)$ and an ascending filtration, $G_{\cdot}$, on $H^2(G, M_2)$ and consider a map closely related to the δ_j.

Let

$$\begin{aligned}
\delta_1^* &= \delta_1, && (3.25)\\
F^0 &= H^1(G, M_1), && (3.26)\\
G_0 &= 0, && (3.27)\\
F^k &= \ker \delta_k^*, && (3.28)\\
H^2(G, M_1)/G_k &= \mathrm{coker}\delta_k^*. && (3.29)
\end{aligned}$$

Let

$$\delta_{k+1}^* : F^k \to H^2(G, M_1)/G_k \tag{3.30}$$

be defined via

$$\delta_{k+1}^*(x) = \delta_{k+1}(\overline{x}) \tag{3.31}$$

where $\overline{x}$ is a lift of x to $H^1(G, M_{k+1})$.

The fact that this definition of δ_k^* is well-defined follows from the following two claims:

Claim 3.5.1. *If we take*

$$0 \longrightarrow M_k \xrightarrow{f} M_{k+1} \longrightarrow M_1 \longrightarrow 0,$$

where f is inclusion into first k components, then

$$\delta_{k+1} \circ f_* = \delta_k.$$

Claim 3.5.2. *Any two lifts of $x \in F^k \subseteq H^1(G, M_1)$ to $H^1(G, M_{k+1})$ differ by an element of the form $f_*(y)$.*

Indeed, if we assume the claims, then

$$\begin{aligned}
\delta_{k+1}(\bar{x} + f_*(y)) &= \delta_{k+1}(\bar{x}) + \delta_{k+1}(f_*(y))\\
&= \delta_{k+1}(\bar{x}) + \delta_k(y) \equiv \delta_{k+1}(\bar{x}) \pmod{G_k}.
\end{aligned}$$

Now we prove the claims.

Proof of Claim 3.5.1: Since we have fixed f to be inclusion into the first k components of M_{k+1}, the claim follows from the definition of the coboundary map. Indeed, we have that if we choose a representative 1-cocycle of M_k, $x = (x_1, \ldots, x_k)^t$ then, at the level of cocycles,

$$f_*(x) = (x_1, \ldots, x_k, 0)^t$$

and $\delta_{k+1}(f_*(x))$ is represented by first entry of

$$-\sigma \cdot (0, x_1(\tau), \ldots, x_k(\tau), 0)^t.$$

Recall that the action of $\sigma \cdot (0, x_1(\tau), \ldots, x_k(\tau), 0)^t$ is given by

$$\begin{pmatrix} 1 & a_1 & a_2 & \ldots & a_{k+1} \\ & 1 & a_1 & \ddots & \vdots \\ & & \ddots & \ddots & a_2 \\ & & & \ddots & a_1 \\ & & & & 1 \end{pmatrix} (0, x_1(\tau), \ldots, x_k(\tau), 0)^t.$$

The first entry of this vector is the same as the first entry of

$$\begin{pmatrix} 1 & a_1 & a_2 & \ldots & a_k \\ & 1 & a_1 & \ddots & \vdots \\ & & \ddots & \ddots & a_2 \\ & & & \ddots & a_1 \\ & & & & 1 \end{pmatrix} (0, x_1(\tau), \ldots, x_k(\tau))^t,$$

which is in turn a representative of $\delta_k(x)$. □

Proof of claim 3.5.2: Take $x \in F^k$ and two lifts, $\bar{x}$ and $\hat{x}$, of x to $H^1(G, M_{k+1})$. Then by the exactness of the long exact sequence of cohomology coming from the short exact sequence in claim 3.5.1, $\bar{x} - \hat{x}$ is in the image of f_*. □

3.6 A Formula for δ_k^*

We proceed to derive a formula for the maps δ_k^* defined above in (3.31). Recall the condition satisfied by the a_i in the matrix (3.21) defining the G action on M_k :

$$a_i(\sigma\tau) = a_i(\sigma) + \sum_{j=1}^{i-1} a_j(\sigma)a_{i-j}(\tau) + a_i(\tau).$$

A formula for the coboundary will, necessarily, be more complicated than that in Lemma 3.4.1. However, we do have the following lemma:

Lemma 3.6.1. *Let $k \geq 1$, let $x \in F^k = \ker(\delta_k^*) \subseteq H^1(G, M_1),$, and let*

$$\bar{x} = (x_k, \ldots, x_1)^t : G \to M_k,$$

be a lift of x to $H^1(G, M_k)$, where $x_1 = x$. Then

$$\delta_{k+1}^*(x)(\sigma, \tau) = \sum_{j=1}^{k} a_j(\sigma)x_{k+1-j}(\tau). \tag{3.32}$$

Proof: We can lift $\bar{x}$ to a map

$$y = (0, x_k, \ldots, x_1)^t : G \to M_{k+1}.$$

Then, apply the coboundary operator d to y :

$$\mathrm{d}y(\sigma, \tau) = y(\sigma) - y(\sigma\tau) + \sigma y(\tau)$$

$$= (0, \bar{x}(\sigma))^t - (0, \bar{x}(\sigma\tau))^t + \sigma(0, \bar{x}(\tau))^t$$

Using the fact that $\bar{x}$ is a cocycle and the definition of the G-action on M_{k+1} this reduces to

$$\mathrm{d}y(\sigma, \tau) = (\sum_{j=1}^{k} a_j(\sigma)x_{k+1-j}(\tau), 0, \ldots, 0)^t. \tag{3.33}$$

$\square$

As was shown above, for $i \geq 2$, a_i is not a homomorphism, and thus does not represent a cohomology class in $H^1(G, M_1)$. However, by restricting to a subgroup of G, we do obtain the following proposition.

Proposition 3.6.2. *Let $H_k \leq G$ be a subgroup on which $a_j(\sigma) = 0$ whenever $\sigma \in H_k$ and $j \leq k-1$, then $a_k \in H^1(H_k, M_1)$, and so*

$$\delta_k^* \circ res^G_{H_k}(x) = a_k \cup x.$$

This proposition will not, however, prove itself to be of great use in the next chapter. Indeed, as soon as we return to Galois cohomology, Proposition 3.6.2 will require us to extend our ground field, refusing to grant results over $\mathbb{Q}(\zeta)$ as desired.

Lemma 3.4.1 can not be generalized for general k as it is. We turn instead to Proposition 3.6.4, using it to express the image of δ_k^* in terms of the value of certain restricted Massey products, defined below.

Let

$$\langle -a_1, -x\rangle^{(k)} \tag{3.34}$$

denote the value of the $k+1$-fold Massey product corresponding to the homomorphism $G \to \bar{U}(M_1, k+2)$ given by

$$\begin{pmatrix} 1 & a_1 & a_2 & \dots & a_k & * \\ & 1 & a_1 & \ddots & \dots & x_k \\ & & \ddots & \ddots & a_2 & \vdots \\ & & & 1 & a_1 & x_2 \\ & & & & 1 & x \\ & & & & & 1 \end{pmatrix} \tag{3.35}$$

where $a_1, \dots, a_{k-1}$ are as defined in (3.21) in section 3.5 and $x_2, \dots, x_{k-1}$ are any maps $x_i : G \to M_1$ that make the matrix into a homomorphism.

Lemma 3.6.3. *For $x \in F^k$, let $\bar{x}$, a lift of x to $H^1(G, M_k)$, be represented by the matrix*

$$\begin{pmatrix} 1 & a_1 & \dots & a_{k-1} & x_k \\ & \ddots & \ddots & a_2 & \vdots \\ & & 1 & a_1 & x_2 \\ & & & 1 & x \\ & & & & 1 \end{pmatrix}. \tag{3.36}$$

Then

$$\begin{pmatrix} 1 & a_1 & a_2 & \dots & a_k & * \\ & 1 & a_1 & \ddots & \dots & x_k \\ & & \ddots & \ddots & a_2 & \vdots \\ & & & 1 & a_1 & x_2 \\ & & & & 1 & x \\ & & & & & 1 \end{pmatrix} \tag{3.37}$$

is a defining system for a Massey product, the value of which is $\delta_k(\bar{x})$*.*

Proof: The claim that (3.37) is a defining system for a Massey product follows from Theorem 3.4.3. By (3.32) in the proof of Lemma 3.6.1, $\delta_k(\bar{x}) = \sum_{j=1}^{k} a_j x_{k+1-j}$. This is the value of the Massey product with defining system (3.37) by the definition of the value given in (3.17). □

Proposition 3.6.4. *Let* $k \geq 2$*. If* $x \in F^k$*, then*

$$\delta_k^*(x) = \langle -a_1, -x \rangle^{(k)}$$

in the quotient of $H^2(G, M_1)$ *where Massey products are well-defined. In particular, in the case* $k = 1$*, we have*

$$\delta_1^*(x) = \langle -a_1, -x \rangle^{(1)},$$

which is the cup product $-a_1 \cup -x$*, well-defined in* $H^2(G, M_1)$*.*

Proof: This follows from Lemma 3.6.3. □

We end this section by noting that Proposition 3.6.4 generalizes Proposition 3.4.1 after restricting to M_i from V_i. The next chapter will apply these results to the G_k modules $J[\lambda^k]$.

Chapter 4

A Pairing and Non-Triviality of Ш(k, J)

4.1 An Application of Proposition 4.1.2 to Ш(k, J)

We return now to the study of the torsion subgroups of the Jacobians of Section 3.2 as Galois modules.

Recall that we have fixed $\mathbb{F}_p$-bases for $J[\lambda^k]$,

$$\mathcal{B}_k = \{\alpha_k, \dots, \alpha_1\},$$

where α_i is a λ^i torsion point and

$$\lambda\alpha_i = \alpha_{i-1}.$$

We have the short exact sequences

$$0 \longrightarrow J[\lambda] \longrightarrow J[\lambda^k] \xrightarrow{\lambda} J[\lambda^{k-1}] \longrightarrow 0. \tag{4.1}$$

Note that the filtration on the cohomology groups $H^1(G, M_1)$ and $H^2(G, M_2)$ and the related maps δ_k^* can be defined for the groups $H^1(k, J[\lambda])$ and $H^2(k, J[\lambda])$ in the exact same manner as they were for G and M_i. We refer to the filtered coboundary as δ_k^* in both cases; the context will make clear which modules are at hand.

We define submodules $N_k \subseteq J[\lambda^k]$ via the basis

$$\{\alpha_k, \alpha_{k-3}, \dots, \alpha_1\}.$$

Then for $k \geq 5$ we get subsequences of (4.1):

$$0 \longrightarrow J[\lambda] \longrightarrow N_k \xrightarrow{\lambda} N_{k-1} \longrightarrow 0. \tag{4.2}$$

The fact that the N_k are G_k submodules of $J[\lambda^k]$ follows from the fact that $J[\lambda^3]$ is rational over k [Gre81]. Consequently, the G_k structure of $J[\lambda^k]$ is given by matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 & a_3(\sigma) & \dots & a_{k-1}(\sigma) \\ & \ddots & \ddots & \ddots & \ddots & \vdots \\ & & 1 & 0 & 0 & a_3(\sigma) \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{pmatrix} \tag{4.3}$$

(as we recall from (3.7)).

We have the natural projection of G_k-modules

$$\phi_k : J[\lambda^k] \to N_k$$

that induces a map

$$\phi_{k,*} : H^1(k, J[\lambda^k]) \to H^1(k, N_k).$$

We use this map to relate the image of the filtered coboundary δ_k^* to the image of the coboundary δ' coming from the sequences (4.2) via the following lemma.

Lemma 4.1.1. *If $\xi \in F^k \subseteq H^1(k, J[\lambda])$ and $\bar{\xi}$ is a lift of ξ to $H^1(k, J[\lambda^k])$ then*

$$\delta' \circ \phi_{k,*}(\bar{\xi}) \equiv \delta_k^*(\xi) \pmod{G_k}.$$

Proof: This follows easily from the commutativity of the diagram

$$\begin{tikzcd} 0 \arrow[r] & J[\lambda] \arrow[r] \arrow[d, equal] & J[\lambda^{k+1}] \arrow[r, "\lambda"] \arrow[d, "\phi_{k+1}"] & J[\lambda^k] \arrow[r] \arrow[d, "\phi_k"] & 0 \\ 0 \arrow[r] & J[\lambda] \arrow[r] & N_{k+1} \arrow[r, "\lambda"] & N_k \arrow[r] & 0. \end{tikzcd}$$

□

Thus,

Theorem 4.1.2. *If $\xi \in F^k \subseteq H^1(k, J[\lambda])$ and ξ is represented by a matrix*

$$\begin{pmatrix} 1 & \chi_1 \\ & 1 \end{pmatrix}$$

then

$$\delta_k^*(\xi) = \langle -a_3, -\chi_1 \rangle^{(k-2)}.$$

Proof: Lemma 4.1.1 gives us that $\delta_k^*(\xi) \equiv \delta' \circ \phi_*(\bar{\xi}) \pmod{G_k}$. Using the notation of the filtration of section 3.5, we can write

$$\delta_k^*(\xi) = \delta'^*_{k-2}(\xi)$$

after recalling that $J[\lambda] = M_1 = \mathbb{Z}/p\mathbb{Z}$. Thus, Proposition 3.6.4 gives us that

$$\delta'^*_{k-2}(\xi) = \langle -a_1, -\chi_1 \rangle^{(k-2)}.$$

□

Recall from section 2.1 that $\Delta = \mathrm{Gal}(k/\mathbb{Q})$ and from (2.16)

$$\eta_{p-j} = (1-\zeta)^{\epsilon_j},$$

where ϵ_j is the idempotent

$$\frac{1}{p-1} \sum_{\sigma \in \Delta} \omega(\sigma)^{-j} \sigma,$$

which projects onto the j-th eigenspace of the cyclotomic p-units of k.

Corollary 4.1.3. *Let J be the jacobian of $C_{a,b}$, suppose that $a^3 + b^3 \not\equiv (a+b)^3 \pmod{p}$, and let $x \in F^3 \subset H^1(G, J[\lambda])$. Let*

$$\langle \eta_j, x \rangle$$

denote the cup product pairing of a cocycle x with the character associated to the extension $k(\eta_j^{1/p})/k$. Then

$$\delta_3^*(x) = \langle \eta_{p-3}, x \rangle.$$

Proof: Theorem 4.1.2 gives us that

$$\delta_3^*(x) = \langle a_3, x\rangle^{(1)}$$

where the action of G_k on $J[\lambda^4]$ is given by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & a_1 \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}.$$

Proposition 2.2.6 gives us that the field $k(J[\lambda^4])$ is obtained from $k(J[\lambda^3]) = k$ by adjoining the element $\sqrt[p]{\eta_{p-3}}$, proving the corollary. $\square$

We will use the formula for δ_3^* given in Corollary 4.1.3 to detect non-trivial subgroups of Ш(k, J). To do so, we will require the following lemma.

Lemma 4.1.4. *If C has wild non-split or tame reduction and $i \geq \frac{p+3}{2}$ then the lift of η_i to $H^1(k, J)$ represented by $(1, 1, \eta_i)$ is contained in the Selmer group $S^{(\lambda^3)}(k, J)$.*

Proof: Since η_i defines a cocycle which is unramified outside the primes above p, $(1, 1, \eta_i)$ satisfies the all the local conditions for membership in $S^{(\lambda^3)}(k, J)$ except the one at λ. Thus membership in $S^{(\lambda^3)}(k, J)$ is equivalent to being in the image of the local descent map at λ

$$d_3 : J(k_\lambda) \to \left(k_\lambda^*/k_\lambda^{*p}\right)^3.$$

Following [MT03, section 2], we write

$$d_3 = \iota_{P_3} \times \iota_{P_2} \times \iota_{P_1}$$

where $\iota_{P_i} \circ \lambda = \iota_{P_{i-1}}$. Now take $\eta_i \in \bigoplus_{(p+1)/2}^{p} k_\lambda^*/k_\lambda^{*p(i)}$. By [MT03, prop. 4.1], $\eta \in \iota_{P_1}(J(k_\lambda))$. Take a such that $\iota_{P_1}(a) = \eta_i$.

Consider, $d_3(a) = (\iota_{P_3}(a), \iota_{P_2}(a), \eta_i)$. Proposition 4.1 of [MT03] also gives us that

$$\iota_{P_3}(a), \iota_{P_2}(a) \in \bigoplus_{(p+1)/2}^{p} \left(k_\lambda^*/k_\lambda^{*p}\right)^{(i)}.$$

For $b \in J(k_\lambda)$, $\iota_{P_i}(\lambda b) = \iota_{P_{i-1}}(b)$ and so

$$d_3(\lambda b) = (\iota_{P_2}(b), \iota_{P_1}(b), 1) = (d_2(b), 1).$$

By [MT03, prop. 4.2], the image of

$$\mathrm{im}(d_2) = \left(\bigoplus_{(p+1)/2}^{p} k_\lambda^*/k_\lambda^{*p} \right)^2$$

and so we can choose b so that $d_2(b) = (\iota_{P_3}(a)^{-1}, \iota_{P_2}(a)^{-1})$. Then we have that $d_1(a + \lambda b) = \eta_i$ and that $d_3(a + \lambda b) = (1, 1, \eta_i)$. □

Applying information regarding the vanishing of this cup product to the vanishing of this filtered coboundary map allows us to prove the following theorem.

Theorem 4.1.5. *Let p is an irregular prime that divides the numerator of the r-th Bernoulli number, B_r. Suppose that $p - r + 3 \geq \frac{p+1}{2}$, that $C_{a,b}$ has wild non-split or tame reduction, and that $a^3 + b^3 \not\equiv (a+b)^3 \pmod{p}$. Then $\langle \eta_{p-r+3}, \eta_{p-3} \rangle \neq 0$ implies that the image of η_{p-r+3} in $\text{Ш}(J, k)$ is nontrivial.*

Proof: The fact that $p - r + 3 \geq \frac{p+1}{2}$ tells us that η_{p-r+3} represents an element in the Selmer group $S^\lambda(k, J)$. Lemma 4.1.4 tells us that the lift $(1, 1, \eta_{p-r+3})$ of η_{p-r+3} is contained in $S^{\lambda^3}(k, J)$. Corollary 4.1.3 implies that

$$\langle \eta_{p-r+3}, \eta_{p-3} \rangle = \delta_3^*(\eta_{p-r+3})$$

and Lemma 3.1.1 then proves that if $\delta_3^*(\eta_{p-r+3}) \neq 0$ then the image of η_{p-r+3} in $\text{Ш}(k, J)$ is non-trivial. □

Recall the cup product pairing (2.28) from section 2.4. We would like to apply the data computed by McCallum and Sharifi in [MS02] to the production of examples satisfying the hypotheses of Theorem 4.1.5. However, the McCallum-Sharifi pairing is developed for $H^1(G_{k,S}, \mu_p) = H^1(G_{k,S}, J[\lambda])$ where

$$S = \{1 - \zeta\},$$

k_S is the maximal extension of k unramified outside of S, and

$$G_{k,S} = \mathrm{Gal}(k_s/k).$$

However, by the characterization

$$k(J[p]) = k(\{\sqrt[p]{\eta_{p-j}} : j \text{ even}, 1 \leq j \leq p-3\})$$

given by Proposition 2.2.6, we have that

$$k(J[\lambda]) \subseteq \cdots \subseteq k(J[\lambda^{p-2}]) \subseteq k(J[p]) \subseteq k_S.$$

Then, the inflation map

$$0 \to H^1(G_{k,S}, J[\lambda]) \to H^1(k, J[\lambda]),$$

induces an isomorphism of λ-Selmer groups and the λ^k torsion in Tate-Shafarevich groups [Mil86b, cor. 6.6].

Also, the $G_{k,S}$ structure of the $J[\lambda^k]$ is identical to the G_k structure described above. Therefore, the cup product pairing in Theorem 4.1.5 is the same as the pairing (2.27). So we can use the computations of the values of this pairing to find non-trivial elements in $Ш(k, J)$.

In [McC88], McCallum found nontrivial elements in the Tate-Shafarevich group, and in [MT03] McCallum and Tzermias found further nontrivial elements. However, McCallum's result applies only when $C_{a,b}$ is wild split, and the result of McCallum-Tzermias applies only when p is regular. Therefore, the nontrivial elements we find here are new.

In [MT03], McCallum and Tzermias proved the following result. This will allow us to use the subgroups found by Theorem 4.1.5 to imply the existence of larger subgroups of $Ш(k, J)$.

Theorem 4.1.6. *[MT03, Corollary 1.3] Let C be the curve given by equation $y^p = x^a(1-x)^b$ for $p \geq 5$ and J be its Jacobian. If either* *(a) C has wild split reduction at p and $p \equiv 3 \pmod 4$ or*

(b) C has wild non-split or tame reduction and $p \nmid B_{(p-1)/2}$ or $p \nmid B_{(p-3)/2}$

then $|Ш(k,J)[p^\infty]| < p^3$ implies that $Ш(k,J) = 0$.

Example 4.1.7. *Let $p = 691$ and let J be the Jacobian variety of the curve with affine equation $y^{691} = x^5(1-x)^{29}$. Then this curve has wild non-split reduction (using the criteria from [McC88]). Since 691 divides the numerator of B_{12}, the 12-th Bernoulli number. A direct computation by McCallum and Sharifi verified that*

$$\langle \eta_{682}, \eta_{688} \rangle \neq 0.$$

Thus, Theorem 4.1.5 implies that the image of η_{682} is non-trivial in the corresponding Tate-Shafarevich group. So $Ш(k,J)$ contains an element of order 691. Furthermore, 691 also divides the numerator of the 200-th Bernoulli number. Checking the same calculation finds that

$$\langle \eta_{494}, \eta_{688} \rangle \neq 0$$

also. This gives us an other element of order 691. Because these elements are in different eigenspaces, they are necessarily independent. Thus $Ш(k,J)$ contains a subgroup isomorphic to $\mathbb{Z}/691\mathbb{Z} \oplus \mathbb{Z}/691\mathbb{Z}$. Then Theorem 4.1.6 implies that $Ш(k,J)$ contains a subgroup of order at least 691^3.

We list more instances of the results of this theorem below.

Table 4.1 lists the irregular primes, p, and the index of the Bernoulli number, r, the numerator of which p divides, for pairs (p,r) satisfying the hypotheses of Theorem 4.1.5. In the case that p divides the numerator of two Bernoulli numbers, B_{r_1} and B_{r_2}, and both (p,r_1) and (p,r_2) satisfy Theorem 4.1.5, both r_1 and r_2 are listed in the table. We note that in this case, with the appropriate reduction type, the theorem provides for the existence of two nontrivial elements in $Ш(k,J)$, as in Example 4.1.7, that are necessarily independent in $Ш(k,J)$ and thus implies a subgroup of $Ш(k,J)$ isomorphic to $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, while Theorem 4.1.6 implies the presence of an even larger subgroup. A list for all pairs (p, r) satisfying the assumptions of Theorem 4.1.5 with $p \leq 15{,}000$ is available at [Lev].

For any p on this list, choosing values of a and b and checking the reduction types of the resulting curves allows us to apply Theorems 4.1.5 4.1.6 in order to guarantee subgroups of $Ш(k, J)$ of size at least p^3. Table 4.2 presents the results of this application for a small sample of curves. The reduction types have been determined using the criteria stated in [MT03]. A full list of data can be found at [Lev].

Table 4.1. Sample of Results of Theorem 4.1.5

p	r	p	r
103	24	131	22
233	84	263	100
307	88	379	100;174
409	126	461	196
467	94	541	86
547	270	557	222
557	52	577	52
587	90; 92	593	22
617	20; 174	631	80; 226
647	236; 242	653	38
659	224	683	32
691	12; 200	751	290
761	260	809	330
827	102	839	66
881	162	887	418
953	156	971	166

Table 4.2. A Sample of Results of Theorems 4.1.6 and 4.1.5

Curve	Reduction Type	Lower Bound on $\lvert Ш(k,J)\rvert$
$y^{103} = x(1-x)^{51}$	Tame	103^3
$y^{103} = x^{18}(1-x)^{9}$	Wild Non-split	103^3
$y^{233} = x^{12}(1-x)^{158}$	Wild Non-split	233^3
$y^{263} = x^{7}(1-x)^{31}$	Wild Non-split	263^3
$Y^{271} = x^{110}(1-x)^{5}$	Tame	271^3

References

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (J. W. S. Cassels and A. Frölich, eds.), Academic Press, 1967.

[Bro82] Kenneth S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, no. 87, Springer, 1982.

[Dwy75] William G. Dwyer, *Homology, massey products and maps between groups*, Journal of Pure and Applied Algebra **6** (1975), 177–190.

[Fad61] D. K. Faddeev, *Invariants of divisor classes for the curves $x^k(1-x) = y^l$ in an l-adic cyclotomic field*, Tr. Mat. Inst. Steklova **64** (1961), 284–293.

[Gre81] Ralph Greenberg, *On the jacobian variety of some algebraic curves*, Compositio Math. **42** (1980/81), 345–359.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, no. 52, Springer, 1977.

[HS71] P.J. Hilton and U. Stammbach, *A course in homological algebra*, Graduate Texts in Mathematics, no. 4, Springer-Verlag, New York, 1971.

[IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory, second edition*, Graduate Texts in Mathematics, no. 84, Springer, 1990.

[Koc00] Helmut Koch, *Number theory; algebraic numbers and functions*, American Mathematical Society, 2000.

[Lan65] Serge Lang, *Algebra*, Addison-Wesley, 1965.

[Lev] Benjamin L. Levitt, *Two tables of data related to my dissertation for $p <$ 15,000*, http://www.math.arizona.edu/~lvtt/computations.html.

[McC88] William G. McCallum, *On the shafarevich-tate group of the jacobian of a quotient of the fermat curve*, Invent. math **93** (1988), 637–666.

[Mil86a] J. S. Milne, *Abelian varieties*, Arithemetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer, 1986.

[Mil86b] ———, *Arithmetic duality theorems*, Perspectives in Mathematics, Academic Press, Inc., 1986.

[Mil86c] ———, *Jacobian varieties*, Arithemetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer, 1986.

[MS02] William G. McCallum and Romyar Sharifi, *A cup product in the galois cohomology of number fields*, Duke Mathematical Journal **120** (2002), 269–310.

[MT03] William G. McCallum and Pavlos Tzermias, *On shafarevich-tate groupd and arithmetic of fermat curves*, Number Theory and Algebraic Geometry (Miles Reid and Alexei Skorobogotov, eds.), London Mathematical Society Lecture Notes, no. 303, Cambridge Univeristy Press, 2003.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer, 1986.

[SM] Romyar Sharifi and William G. McCallum, *Computations...related to a cup product*, http://www.math.mcmaster.ca/∼sharifi/computations.html.

[Tat74] John T. Tate, *The arithemtic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

[Was82] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, no. 83, Springer, 1982.

[Wei29] A. Weil, *Sur un théorèm de mordell*, Bull. Sci. Math. **54** (1929), no. 2, 281–291.