Unramified $p$-Extensions of $\mathbb{Q}(N^{1/p})$ via Cup Products in Galois Cohomology

Karl Schaefer and Eric Stubley

June 5, 2018

Abstract

We use Galois cohomology to study the $p$-rank of the class group of $\mathbb{Q}(N^{1/p})$, where $N \equiv 1 \pmod{p}$ is prime. We prove a partial converse to a theorem of Calegari–Emerton, and provide a new explanation of the known counterexamples to the full converse of their result. In the case $p = 5$, we prove a complete characterization of the 5-rank of the class group of $\mathbb{Q}(N^{1/5})$ in terms of whether or not $\prod_{k=1}^{(N-1)/2} k^k$ and $\sqrt[5]{N - 1}$ are 5th powers mod $N$.

Contents

1 Introduction 2
  1.1 The Problem .......................................................... 2
  1.2 Results .................................................................. 2
  1.3 Strategy .................................................................... 3
  1.4 Acknowledgements ..................................................... 4

2 Cohomology Computations 4
  2.1 Notation .................................................................. 4
  2.2 The Selmer Condition $\Sigma$ ........................................... 6
  2.3 Selmer Groups in the Cohomology of the Cyclotomic Character ............................................. 7

3 Selmer groups and $\text{Cl}_K$ 10
  3.1 Indecomposability of some $\text{Gal}(K(\zeta_p)/\mathbb{Q})$-modules arising from $\text{Cl}_K$ .................. 11
  3.2 An Auxiliary Selmer Group ........................................... 15
  3.3 An Exact Sequence of Selmer Groups ................................... 18
  3.4 $\text{Cl}_K$ and Selmer Groups of Characters ...................... 20
  3.5 Climbing The Ladder .................................................... 21

4 Effective Criteria for $H^1_{\Sigma}(\mathbb{F}_p(-i)) \neq 0$ 23
  4.1 A Criterion for $H^1_{\Sigma}(\mathbb{F}_p(-i)) \neq 0$, $i$ Odd .................................................. 23
  4.2 Relationship with Lecouturier’s Results .......................... 28
  4.3 Relationships with Known Criteria for $H^1_{\Sigma}(\mathbb{F}_p(-i)) \neq 0$ .............................. 29
  4.4 A Criterion for $H^1_{\Sigma}(\mathbb{F}_p(-i)) \neq 0$, $i$ Even .................................................. 30

5 Specific Primes 31
  5.1 $p = 3$ ................................................................. 31
  5.2 $p = 5$ ................................................................. 32
  5.3 $p = 7$ ................................................................. 35
  5.4 Irregular $p$ ............................................................ 36

Appendix A Data for $p = 5, 7$ 37
  A.1 $p = 5$ ................................................................. 37
  A.2 $p = 7$ ................................................................. 37
1 Introduction

Let $N$ and $p \geq 3$ be prime numbers with $p|\phi(N-1)$. Let $S = \{N, p, \infty\}$ and let $G_{Q,S}$ be the Galois group of the maximal unramified extension of $Q$ unramified outside of $S$. Put $G_Q = \text{Gal}(\overline{Q}/Q)$ and let $K$ denote the field $Q(N^{1/p})$.

1.1 The Problem

The goal of this article is to study the class group $Cl_K$ of $K$, and in particular its $p$-rank $r_K = \dim_{F_p}(Cl_K \otimes F_p)$. It is immediate that $r_K \geq 1$ by genus theory (explicitly, the degree $p$ subfield of $K(\zeta_N)/K$ is unramified everywhere). Our starting point is the following theorem of Calegari–Emerton.

**Theorem** (Calegari–Emerton, Theorem 1.3, (ii) of [1]). Suppose that $p \geq 5$, and let $C = \prod_{k=1}^{(N-1)/2} k^i$. If $C$ is a $p$th power in $F_N^\times$, then $r_K \geq 2$.

This theorem is proved using deformation theory of Galois representations. Previous work of Merel [5] showed that whether or not the number $C$ is a $p$th power determines whether the $\mathbb{Z}_p$-rank of a certain Hecke algebra is at least 2. Calegari–Emerton identify this Hecke algebra with a deformation space, and construct an unramified $\mathbb{F}_p$-extension in the case that the deformation space has $\mathbb{Z}_p$-rank $\geq 2$. More recently, this theorem was reproven by Wake–Wang-Erickson (see Proposition 11.1.1 of [10], restated in this article as Proposition 1.2.1).

Calegari–Emerton also raise the question of whether or not the converse to this theorem holds. Numerical computations suggested that it was true when $p = 5$, but not in general. Indeed, Lecouturier noticed in [1] that the converse fails in the case $p = 7$, $N = 337$.

In this article, we aim to give a proof of the theorem of Calegari–Emerton without using deformation theory of Galois representations or Hecke algebras. We also aim to prove (partial) converses to the theorem of Calegari–Emerton.

1.2 Results

For odd $i$ satisfying $1 \leq i \leq p - 4$, let

$$M_i = \prod_{k=1}^{N-1} \prod_{a=1}^{k-1} k^{a^i},$$

as first defined by Lecouturier in [4]. We prove

**Theorem 1.2.1.** Let $\mu$ be the number of $M_i$ which are not $p$th powers in $F_N^\times$. Then

$$r_K \leq r_{Q(\zeta_p)} + p - 2 - \mu$$

where $r_{Q(\zeta_p)}$ is the $p$-rank of the class group of $Q(\zeta_p)$. If $p$ is regular (i.e. $r_{Q(\zeta_p)} = 0$), then

$$r_K \leq p - 2 - 2\mu.$$

The first inequality of Theorem 1.2.1 is due to Lecouturier [4]. Our proof of this theorem is by a new method, and gives a sharper bound in the case of regular $p$. An immediate corollary of Theorem 1.2.1 in the case of regular $p$ is the following partial converse to the theorem of Calegari–Emerton:

**Theorem 1.2.2.** Suppose that $p$ is regular, and that $r_K \geq 2$. Then at least one of the $M_i$ is a $p$th power in $F_N^\times$.

**Proof.** If $r_K \geq 2$, then the bound in the regular case of Theorem 1.2.1 shows that $2 \leq p - 2 - 2\mu$. As there are $\frac{p - 3}{2}$ many $M_i$, it must be the case that $\mu < \frac{p - 3}{2}$, i.e. at least one of the $M_i$ is a $p$th power. \qed

The quantity $M_1$ is a $p$th power if and only if $C = \prod_{k=1}^{(N-1)/2} k^i$ is (see Section 4.3 for this comparison). When $p = 5$, this is therefore the full converse to the theorem of Calegari–Emerton, as the only relevant number $M_i$ is $M_1$. Furthermore, we are able to give an effective method for completely determining $r_K$ in this case.
Theorem 1.2.3. Assume $p = 5$. Then, $1 \leq r_K \leq 3$ according to the following conditions:

1. $r_K \geq 2$ if and only if $M_1$ is a $p$th power in $\mathbb{F}_N^\times$.

2. $r_K = 3$ if and only if both $M_1$ and $\frac{\sqrt[p-1]}{2}$ are $p$th powers in $\mathbb{F}_N^\times$.

The converse to Theorem 1.2.2 is not true in general: in the case $p = 11$, $N = 353$ one has both $r_K = 1$ and $M_3 \in \mathbb{F}_N^\times$. However, the converse to Theorem 1.2.2 is true in the case $p = 7$, which we prove:

Theorem 1.2.4. Assume $p = 7$. Then $r_K \geq 2$ if and only if one of $M_1$ or $M_3$ is a $p$th power in $\mathbb{F}_N^\times$.

This also explains the counterexample $p = 7$, $N = 337$ to the naive converse of the theorem of Calegari–Emerton: in that case, $r_K = 2$ and $M_1$ is not a $p$th power in $\mathbb{F}_N^\times$, but $M_3$ is.

1.3 Strategy

The methods used in this article are inspired by the strategy that Wake–Wang-Erickson use to prove the theorem of Calegari–Emerton. They show that $M_1$ being a $p$th power in $\mathbb{F}_N^\times$ is equivalent to the vanishing of a certain cup product in Galois cohomology. The vanishing of this cup product implies the existence of a reducible representation $G_{\mathbb{Q},S} \to \text{GL}_3(\mathbb{F}_p)$, from which an unramified $\mathbb{F}_p$-extension of $K$ is constructed.

Let $b : G_{\mathbb{Q},S} \to \mathbb{F}_p(1)$ be the cocycle defined by $b(\sigma) = \sigma(N^{1/p})/N^{1/p}$. Let $V$ be the two-dimensional vector space on which $G_{\mathbb{Q},S}$ acts in some basis by the matrix

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

In an abuse of notation, we will also use $b$ to refer to the class of this cocycle in $H^1(G_{\mathbb{Q},S}, \mathbb{F}_p(1))$, which is just the Kummer class of $N$. Let $\chi$ be the mod-$p$ cyclotomic character. Starting with an unramified $\mathbb{F}_p$-extension of $K$, we use the classification of indecomposable $\mathbb{F}_p$-representations of $\mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times \cong \text{Gal}(K(\zeta_p)/\mathbb{Q})$ to show the existence of a Galois representation of the form

$$
\begin{pmatrix}
\text{Sym}^{-m}V \otimes \mathbb{F}_p(m) & \star \\
\chi & \cdots & \chi^{-2}b & \cdots & \chi^{-m}\frac{b^m}{m!} & \chi^{-m}(m-1)! & \star \\
& & & & & & \\
\chi^{-2} & & & \cdots & \cdots & \cdots & \chi^{-m}b & \star \\
& & & & & & & \chi^{-m} & \star \\
& & & & & & & & \chi & \cdots & \cdots & \chi^{-2}b & \chi^{-2} & \cdots & \chi^{-1}b & \chi^{-1} & 1
\end{pmatrix}.
$$

Note that this symmetric power is written using a slightly non-standard basis, see Remark 3.1.9 for an explanation as to why we use this basis.

The representations arising in this fashion give rise to classes in the $G_{\mathbb{Q},S}$-cohomology of certain high-dimensional Galois representations. We study the local properties of these cohomology classes and show that they satisfy a Selmer condition $\Sigma$, first considered by Wake–Wang-Erickson for the Galois module $\mathbb{F}_p(-1)$ (see Section 2.2 for the definition of $\Sigma$ in general). This Selmer condition $\Sigma$ is created exactly to detect those classes whose cup product with $b$ is equal to 0. This leads to the following bound on $r_K$ in terms of the dimensions of the cohomology groups:

Theorem 1.3.1. Let $h_{\Sigma}(\mathbb{F}_p(-i))$ denote the $\mathbb{F}_p$-dimension of $H^1_{\Sigma}(\mathbb{F}_p(-i))$. We have

$$1 + h_{\Sigma}(\mathbb{F}_p(-1)) \leq r_K \leq 1 + \sum_{i=1}^{p-3} h_{\Sigma}(\mathbb{F}_p(-i)).$$

See Section 3 for the proof of this theorem. Note that this theorem has as a corollary the statement that if $r_K \geq 2$, then at least one $H^1_{\Sigma}(\mathbb{F}_p(-i)) \neq 0$. By a computation using Gauss sums, we relate the dimensions $h_{\Sigma}(\mathbb{F}_p(-i))$ to the quantities $M_i$ introduced earlier.
Theorem 1.3.2. Suppose that $p$ is regular, then $H_1^F_p(-i)$ is at most 1-dimensional, and is non-zero if and only if $M_i$ is a $p$th power in $F_N^\times$.

See Section 4.1 for the proof of this theorem. Theorem 1.2.1 in the regular case follows from Theorems 1.3.1 and 1.3.2 combined with Corollary 2.3.3. See Section 5.4 for a discussion of what happens when $p$ is irregular.

The outline of this article is as follows. In Section 2, we recall some facts about Selmer groups, define the Selmer condition $\Sigma$, and prove several lemmas about the relationship between this condition and cup products. In Section 3, we relate the $p$-part of $\mathrm{Cl}_K$ to Selmer groups of higher-dimensional representations of $G_{Q,S}$ and prove the first part of Theorem 1.3.1. In Section 4, we demonstrate relationships between Selmer groups of characters and the quantities $M_i$ for odd $i$. For even $i$, the Selmer group is shown to be related to both $M_{i-1}$ and another quantity arising from the units of the cyclotomic field $Q(\zeta_p)$. Finally, in Section 5, we analyze the cases $p = 5$ and $p = 7$ in more detail. Appendix A contains computer calculations of $r_K$ and the dimensions $h_1^F(F_p(-i))$ for $p = 5, N \leq 20,000,000$ and $p = 7, N \leq 100,000,000$.

One might ask if the techniques of this article can be applied to composite $N$. The authors are currently considering this generalization.

1.4 Acknowledgements

The authors would like to thank Frank Calegari and Matthew Emerton for many helpful discussions on this topic. We would in particular like to thank Frank Calegari for drawing our attention to this problem and for suggesting the techniques that led to the theorems in Section 3.1. The authors would also like to thank Emmanuel Lecouturier, Romyar Sharifi, Preston Wake, and Carl Wang-Erickson for their encouragement and interest in our results, and for feedback on an early draft of this article.

The second author wishes to acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC).

2 Cohomology Computations

Throughout this article we will work with Selmer groups in the cohomology of various mod-$p$ representations of $G_Q$. In fact all representations we consider will be unramified outside of $S$, so will be representations of $G_{Q,S}$.

2.1 Notation

We first establish some notation and conventions used throughout the article as well as recall some facts about group cohomology. Let $A$ be an $F_p$-vector space with an action of $G_Q$ via $\rho : G_Q \to \mathrm{GL}_n(F_p)$.

- Let $F_p$ and $F_p(1)$ be the 1-dimensional $F_p$-vector spaces on which $G_Q$ acts trivially and by the mod-$p$ cyclotomic character $\chi$, respectively. Let $A(i) = A \otimes_{F_p} F_p(1)^{\otimes i}$. Throughout, fix a primitive $p$th root of unity $\zeta_p$, which determines an isomorphism $\mu_p = F_p(1)$.
- Let $b : G_{Q,S} \to F_p(1)$ be the cocycle defined by $\sigma \mapsto \sigma(N^{1/p})/N^{1/p}$. By Kummer Theory,

$$H^1(G_{Q,S}, F_p(1)) = \frac{Z[1/pN]^\times}{Z[1/pN]^\times_{p}}.$$ 

The class of $b$ in $H^1(G_{Q,S}, F_p(1))$, which we also denote by $b$, is the class of $N$ under this isomorphism.

- We let $A^\vee = \mathrm{Hom}_{G_Q}(A, F_p)$ and $A^* = A^\vee(1) = \mathrm{Hom}_{G_Q}(A, F_p(1))$.
- Given a class $a \in H^1(G_Q, A)$ represented by a cocyle $a : G_Q \to A \cong F_p^n$, we can write

$$a(\sigma) = \begin{bmatrix} a_0(\sigma) \\ \vdots \\ a_{n-1}(\sigma) \end{bmatrix}$$ 

4
for σ ∈ G_Q. This defines a new (n + 1)-dimensional G_Q-representation which is an extension of F_p by A via the map

\[ σ \mapsto \begin{pmatrix} ρ(σ) & a_0(σ) & \vdots & a_{n-1}(σ) \\ 0 & 1 \end{pmatrix} ∈ GL_{n+1}(F_p) \]

whose kernel cuts out a Galois extension of Q. Conversely, given a G_Q-representation which is an extension of F_p by A of the above form, we get a cohomology class which we denote by

\[ a = \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} ∈ H^1(G_Q, A). \]

- Given any two characters χ, χ′ : G_Q → F_p^×, let F_p(χ) and F_p(χ′) be the lines on which G_Q acts by χ and χ′, respectively. Classes a ∈ H^1(G_Q, F_p(χ)) and a′ ∈ H^1(G_Q, F_p(χ′)) correspond to 2-dimensional G_Q-representations of the forms

\[ \begin{pmatrix} χ & a \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} χ' & a' \\ 0 & 1 \end{pmatrix}, \]

respectively. These patch together to form a 3-dimensional representation

\[ \begin{pmatrix} χχ' & χ'a' & c \\ 0 & χ' & a' \\ 0 & 0 & 1 \end{pmatrix} \]

if and only if a ∪ a′ = 0 as cohomology classes, in which case the coboundary of −c is the cochain a ∪ a′.

For a G_Q-module A, recall that a Selmer condition is a collection \( L = \{ L_v \} \) of subspaces \( L_v ⊆ H^1(G_{Q_v}, A) \) where v runs over all places of Q, such that \( L_v \) is the unramified subspace

\[ H^1_{ur}(G_{Q_v}, A) := H^1(G_{\mathbb{F}_v}, A)^{I_v} \]

for almost all places v, where \( I_v ⊆ G_{Q_v} = \text{Gal}(\overline{Q_v}/Q_v) \) is the inertia subgroup and \( G_{\mathbb{F}_v} = G_{Q_v}/I_v \) is the absolute Galois group of the residue field at v. The Selmer group associated to a set of conditions \( L \) is then

\[ H^1_L(G_Q, A) = \ker \left( H^1(G_Q, A) \to \prod_{v} \frac{H^1(G_{Q_v}, A)}{L_v} \right). \]

We will use the following conventions in describing Selmer groups.

- To simplify notation, we will denote a Selmer group \( H^1_L(G_Q, A) \) simply by \( H^1_L(A) \).
- As every module A we will consider will be an F_p-vector space, we will use the following notation for dimensions:

\[ h^1_L(A) = \dim_{F_p}(H^1_L(A)). \]

- All Selmer conditions we use have the unramified condition at places outside of S. In particular, since p is assumed to be odd, we will always have \( H^1(G_{\mathbb{R}}, A) = 0 \), removing the need to specify a local condition at the infinite place.
- Given a subset \( T ⊆ S = \{ N, p, ∞ \} \), we will use the notation \( H^1_T(A) \) to denote the Selmer group with the unramified condition at all places outside of T, and any behaviour allowed at the places of T.

**Remark 2.1.1.** If A is a module for \( G_{Q,S} \) then the Selmer group \( H^1_L(A) \) is equal to the \( G_{Q,S} \)-cohomology \( H^1(G_{Q,S}, A) \). Every \( G_Q \)-module we consider will in fact be a \( G_{Q,S} \)-module.
Given a Selmer condition $\mathcal{L} = \{L_v\}$ for $A$, $\mathcal{L}^\ast = \{L_v^\perp\}$ is a Selmer condition for $A^\ast$, where the complements are taken with respect to the Tate pairing on local cohomology groups. A main tool that we will use is the following formula for sizes of Selmer groups, due to Greenberg and Wiles.

**Theorem 2.1.2.** Let $v$ are taken with respect to the Tate pairing on local cohomology groups. A main tool that we will use is the

**Proposition 2.2.2.** Suppose that $v$ where the product is over all places $v$ of $\mathbb{Q}$.

See [11] for a proof of this theorem. For all $v$ that don’t divide $\#A$ and for which $L_v$ is the subgroup of unramified classes, one has $\#L_v = \#H^0(G_{\mathbb{Q}_v}, A)$. Since every Selmer condition that we will use will have the unramified condition at places outside $S$ and since all of our modules will be $\mathbb{F}_p$-vector spaces, the only terms of the above product which will ever contribute in our applications are the $H^0$ term and the local terms at $N$, $p$, and $\infty$.

### 2.2 The Selmer Condition $\Sigma$

We define here the Selmer condition $\Sigma = \{L_v\}$. The local conditions of $\Sigma$ are defined by

- $L_p = 0$.
- $L_N = \ker (\text{res} : H^1(G_{\mathbb{Q}_N}, A) \rightarrow H^1(G_{K_N}, A))$ where $K_N = \mathbb{Q}_N(N^{1/p})$ is the completion of the field $K$ at the unique prime above $N$.
- $L_v$ is the unramified condition at places outside $S$.

As usual, we define the dual Selmer condition $\Sigma^\ast = \{L_v^\perp\}$, where $L_v^\perp$ is the annihilator of $L_v$ under the local cup product pairing. Applied to a $G_{\mathbb{Q}_S}$-module $A$, it is clear that $L_p^\perp = H^1(G_{\mathbb{Q}_p}, A)$, and $L_v^\perp = H^1_{\text{ur}}(G_{\mathbb{Q}_v}, A)$ for places $v$ outside $S$. See Proposition 2.2.2 for the determination of the condition $L_N^\perp$.

We will only consider these Selmer conditions $\Sigma$ and $\Sigma^\ast$ for modules which are isomorphic as $G_{\mathbb{Q}_N}$-modules to $\text{Sym}^n(V)$ for some $n \geq 0$, where $V$ is the 2-dimensional $\mathbb{F}_p$-vector space on which $G_{\mathbb{Q}_S}$ acts in some basis by

\[
\begin{pmatrix}
\chi \\
0
\end{pmatrix}
\begin{pmatrix}
b \\
1
\end{pmatrix}.
\]

Note that when viewed as a $G_{\mathbb{Q}_N}$-module the cyclotomic character $\chi$ is trivial, as $\mu_p \subset \mathbb{Q}_N^\times$.

**Lemma 2.2.1.** For $n \leq p - 1$, $(\text{Sym}^n V)^\vee \cong \text{Sym}^n V \otimes \mathbb{F}_p(-n)$.

**Proof.** Note that the action of $G_{\mathbb{Q}}$ on $\text{Sym}^n V$ factors through $G = \text{Gal}(K(\zeta_p)/\mathbb{Q})$. The range of $n$ considered are in fact those symmetric powers of $V$ which are indecomposable as $\mathbb{F}_p$-representations of $G$ (see Theorem 3.1.6). The only indecomposable representations of $G$ of dimension $n$ are the twists by $\chi$ of $\text{Sym}^n V$: since the dual of an indecomposable representation will certainly also be indecomposable and of the same dimension, it suffices to show that the twist by $-n$ gives us the correct pairing between $\text{Sym}^n V$ and $\text{Sym}^n V)^\vee$. Indeed this is the case, as the 1-dimensional subrepresentation of $\text{Sym}^n V$ is $\mathbb{F}_p(n)$, which is in perfect pairing to $\mathbb{F}_p$ with the 1-dimensional quotient of $(\text{Sym}^n V)^\vee(-n)$, which is $\mathbb{F}_p(-n)$.

**Proposition 2.2.2.** Suppose that $A \cong \text{Sym}^n(V)$ as a $G_{\mathbb{Q}_N}$-representation for some $n \geq 0$. Under the cup product pairing

$H^1(G_{\mathbb{Q}_N}, A) \otimes H^1(G_{\mathbb{Q}_N}, A^\ast) \rightarrow H^2(G_{\mathbb{Q}_N}, \mathbb{F}_p(1))$

the annihilator of $L_N$ is

$L_N^\perp = \ker (\text{res} : H^1(G_{\mathbb{Q}_N}, A^\ast) \rightarrow H^1(G_{K_N}, A^\ast))$

That is, the dual condition $L_N^\perp$ is again the condition $L_N$ (applied to the module $A^\ast$).
Proof. By the Local Euler Characteristic Formula (Theorem 2.8 of [6]), $H^1(G_{\mathbb{Q}_N}, A)$ is 2-dimensional. Using the long exact sequence in $G_{\mathbb{Q}_N}$-cohomology, it can be seen that a basis for this group is
\[
\begin{bmatrix}
0 \\
0 \\
\vdots \\
0
\end{bmatrix}
\begin{bmatrix}
\frac{a}{p} \\
\frac{b}{p^{n+1}} \\
\vdots \\
b
\end{bmatrix}
\]
where $a$ is a class spanning $H^1_{ur}(G_{\mathbb{Q}_N}, \mathbb{F}_p)$. The first class does not vanish when restricted to $K_N$, so this element is not in $L_N$, whereas $b$ is the Kummer class of $N$ which certainly does vanish when restricted to $K_N$. Therefore this second class spans $L_N$, which is thus 1-dimensional.

The modules $A$ are in fact all self-dual as $G_{\mathbb{Q}_N}$-modules, since globally they are self-dual up to twist by the cyclotomic character by Lemma 2.2.1 and locally at $N$ the cyclotomic character $\chi$ is trivial. We fix a $G_{\mathbb{Q}_N}$-module isomorphism $\phi: A \to A^*$. The induced isomorphism (also denoted by $\phi$) on $G_{\mathbb{Q}_N}$- and $G_{K_N}$-cohomology shows that
\[
\phi(L_N) = \ker(\text{res} : H^1(G_{\mathbb{Q}_N}, A^*) \to H^1(G_{K_N}, A^*)).
\]
We will show that $\phi(L_N)$ is the annihilator of $L_N$ by showing that $L_N \cup \phi(L_N) = 0$; note that $L_N^1$ must also be 1-dimensional as $H^1(G_{\mathbb{Q}_N}, A^*)$ is 2-dimensional, so the above suffices to prove that $\phi(L_N) = L_N^1$. Let $x$ span $L_N$. Under the cup product map
\[
\cup : H^1(G_{\mathbb{Q}_N}, A) \otimes H^1(G_{\mathbb{Q}_N}, A) \to H^2(G_{\mathbb{Q}_N}, A \otimes A)
\]
we certainly have that $x \cup x = 0$, as the cup product on $A \otimes A$ is an alternating map. This implies that $x \cup \phi(x) = 0 \in H^2(G_{\mathbb{Q}_N}, A \otimes A^*)$, hence also $x \cup \phi(x) = 0$ in $H^2(G_{\mathbb{Q}_N}, \mathbb{F}_p(1))$ under the evaluation map $A \otimes A^* \to \mathbb{F}_p(1)$. Since $\phi(x)$ spans $\phi(L_N)$ and $x \cup \phi(x) = 0$, we conclude that $\phi(L_N) = L_N^1$.

\[\square\]

2.3 Selmer Groups in the Cohomology of the Cyclotomic Character

Recall that $\mathbb{F}_p(i)$ is the 1-dimensional $\mathbb{F}_p$-vector space on which $G_{\mathbb{Q}}$ acts by $\chi^i$, the $i$-th power of the mod $p$ cyclotomic character.

Theorem 2.3.1. Assume that $p \geq 3$ is regular. The following statements are true.

1. $H^1_S(\mathbb{F}_p(i)) = 0$ for all $i$.

2. The group $H^1_S(\mathbb{F}_p)$ is 2-dimensional, spanned by the classes of the homomorphisms defining the degree $p$ subfields $\mathbb{Q}(\zeta_{p^i})$ and $\mathbb{Q}(\zeta_{p^{i+1}})$ of $\mathbb{Q}(\zeta_N)$ and $\mathbb{Q}(\zeta_{N^2})$, respectively.

3. The group $H^1_S(\mathbb{F}_p(1))$ is 2-dimensional, and spanned by the classes of $N$ and $p$ under the Kummer isomorphism
\[
H^1_S(\mathbb{F}_p(1)) = \frac{\mathbb{Z}[1/pN]}{(\mathbb{Z}[1/pN]^\times)^p}.
\]

4. If $i \equiv 1 \mod p - 1$ is odd, then
\[
\begin{align*}
h^0_S(\mathbb{F}_p(i)) &= 2 \\
h^1_S(\mathbb{F}_p(i)) &= 1 \\
h^1_N(\mathbb{F}_p(i)) &= 1.
\end{align*}
\]

5. If $i \equiv 0 \mod p - 1$ is even, we have
\[
h^1_S(\mathbb{F}_p(i)) = 1.
\]
6. For all $i \neq 0, 1 \mod p - 1$,

$$h_{21}^{1}(F_p(i)) \leq 1.$$ 

Proof. For part 1, note that the restriction map $H^1(G_{Q_S}, F_p(i)) \to H^1(G_{Q^+}, F_p(i))^{Gal(Q^+/Q)}$ is an isomorphism by the inflation-restriction sequence. By the regularity of $p$ there are no non-zero classes in the latter group which are unramified everywhere, hence the subgroup $H^1_{S}(F_p(i)) \subset H^1(G_{Q_S}, F_p(i))$ is zero. Parts 2 and 3 follow from the Kronecker-Weber theorem and Kummer theory, respectively. All but one of the statements in parts 4 and 5 are obtained via applying Theorem 2.1.2 and using the regularity assumption on $p$. As a sample proof we show that $H^1_{S}(F_p(i))$ is 2-dimensional for odd $i \neq 1 \mod p - 1$. By Theorem 2.1.2 we have

$$\frac{\#H^1_{S}(F_p(i))}{\#H^1_{S}(F_p(1 - i))} = \frac{\#H^0(F_p(i))}{\#H^0(F_p(1 - i))} \prod_{v} \frac{\#L_v}{\#H^0(G_{Q_S}, F_p(i))} = \frac{\#H^0(F_p(i))}{\#H^0(F_p(1 - i))} \frac{\#H^1(G_{Q_S}, F_p(i))}{\#H^1(G_{Q_S}, F_p(1 - i))} \frac{\#H^1(G_{R_S}, F_p(i))}{\#H^1(G_{R_S}, F_p(1 - i))} = \frac{1}{1} \cdot \frac{p^2}{1} \cdot \frac{1}{1} = p^2$$

where we know all of the local terms using the Local Euler Characteristic Formula and the parity of $i$. Since $H^1_{S}(F_p(1 - i))$ has the split condition at the primes of $S$ and the unramified condition everywhere else, it is contained in $H^1_{S}(F_p(i))$. This group is trivial by the regularity assumption, so we conclude that $\#H^1_{S}(F_p(i)) = p^2$, i.e. it is 2-dimensional. Part 6 follows from Parts 4 and 5 as

$$H^{1}_{S}(F_p(i)) \subseteq H^{1}_{N}(F_p(i)) \subseteq H^{1}_{S}(F_p(i)).$$

Theorem 2.3.2. Let $p \geq 3$ be prime. Then for odd $3 \leq i \leq p - 2$ we have

$$h_{21}^{1}(F_p(i)) = h_{21}^{1}(F_p(1 - i))$$

$$h_{21}^{1}(F_p(i)) = h_{21}^{1}(F_p(1 - i)) + 1$$

$$h_{21}^{1}(F_p(i)) \leq 1 + h_{21}^{1}(F_p(i)).$$

Proof. The first two statements are proved using Theorem 2.1.2 as in the proof of Part 4 of Theorem 2.3.1. The final statement follows from the exact sequence

$$0 \to H^1_{S}(F_p(i)) \to H^1_{N}(F_p(i)) \to H^1(G_{Q_p}, F_p(i)).$$

Corollary 2.3.3. Let $p \geq 3$ be a prime. Then for even $i \neq 0 \mod p - 1$,

$$h_{21}^{1}(F_p(i)) \neq 0 \implies h_{21}^{1}(F_p(1 - i)) \neq 0.$$ 

Proof. If $h_{21}^{1}(F_p(i)) \geq 1$, then by Theorem 2.3.2 we have $h_{21}^{1}(F_p(1 - i)) \geq 2$. Comparing via

$$h_{21}^{1}(F_p(1 - i)) \leq 1 + h_{21}^{1}(F_p(1 - i))$$

gives that $h_{21}^{1}(F_p(1 - i)) \geq 1$.

The purpose of the Selmer condition $\Sigma^*$ is to detect those classes whose cup product with $b$ is equal to 0, according to the following proposition.
**Proposition 2.3.4.** Assume that $p$ is regular. Given classes $a_i \in H^1_S(F_p(i))$ and $a_j \in H^1_S(F_p(j))$, the cup product $a_i \cup a_j \in H^2_S(G_{Q,N}, F_p(i+j))$ vanishes if and only if the restricted cup product $\text{res}_S(a_i) \cup \text{res}_S(a_j) \in H^2(G_{Q,N}, F_p(i+j))$ does.

**Proof.** We first claim that for any $k$, the restriction map $H^2_S(F_p(k)) \to H^2(G_{Q,N}, F_p(k))$ is injective. Both groups are 1-dimensional, as can be computed using the Global Euler Characteristic Formulas (Theorem 5.1 of [6]) and Local Tate Duality (Corollary of [6]); thus to prove injectivity it suffices to prove surjectivity. The end of the Poitou-Tate exact sequence (Theorem 4.10 of [6]) for $F_p(k)$ is

$$H^2_S(F_p(k)) \to H^2(G_{Q,N}, F_p(k)) \oplus H^2(G_{Q,N}, F_p(k)) \to H^0(G_{Q,S}, F_p(1-k)) \to 0.$$  

If $k \neq 1$ the surjectivity is immediate, as the final term in this sequence is 0. If $k = 1$, the definitions of the maps involved show that the image of $H^2_S(F_p(k))$ lands in $H^2(G_{Q,N}, F_p(k))$.

The non-vanishing of the cup product $a_i \cup a_j$ can thus be detected locally at $N$ due to the following commutative diagram:

$$
\begin{array}{c}
H^1_S(F_p(i)) \otimes H^1_S(F_p(j)) \\
\downarrow \\
H^1(G_{Q,N}, F_p(i)) \otimes H^1(G_{Q,N}, F_p(j)) \\
\downarrow \\
H^2(G_{Q,N}, F_p(i+j))
\end{array}
\cup
\begin{array}{c}
H^2(G_{Q,N}, F_p(i+j)) \\
\downarrow \\
H^2(G_{Q,N}, F_p(i+j))
\end{array}
$$

\[ \rlap{\Box} \]

**Corollary 2.3.5.** Assume $p$ is regular. If $a_i \in H^1_S(F_p(i))$ and $\text{res}_S(a_i) \neq 0$, and $a_j$ is any class in $H^1_S(F_p(j))$, then $a_i \cup a_j = 0$ if and only if $a_j \in H^1_S(F_p(j))$.

**Proof.** By Proposition 2.3.4 it suffices to show that $\text{res}_S(a_i) \cup \text{res}_S(a_j) = 0$ if and only if $a_j \in H^1_S(F_p(j))$. Since $\text{res}_S(a_i)$ is by assumption non-zero, we have that $\text{res}_S(a_i) = ub$ for some non-zero $u \in F_p$. We know by Proposition 2.2.2 $ub \cup \text{res}_S(a_j) = 0$ implies that $\text{res}_S(a_j)$ is a multiple of $b$ (possibly 0), which is the condition for $a_j$ to be an element of the Selmer group $H^1_S(F_p(j))$.

\[ \rlap{\Box} \]

**Remark 2.3.6.** Under the assumption that $p$ is regular, we know that any non-zero class in $H^1_S(F_p(i))$ (for $i \neq 0,1$) will be a non-zero multiple of $b$ when restricted to $G_{Q,N}$: being in the span of $b$ is the local condition at $N$ for these modules, and since this class is split at $p$ and unramified everywhere else, the regularity assumption on $p$ forces this class to be non-zero locally at $N$. Many classes we encounter will satisfy this condition; one in particular is the class of the extension $Q(^{(p)}_{S,N}) \in H^1_S(F_p)$.

**Lemma 2.3.7.** The completion of $Q(^{(p)}_{S,N})$ at the prime above $N$ is $K_N$.

**Proof.** We can see this by computing the norm subgroup in $Q^\times_N$ of both extensions and showing they are equal. We know that the norm subgroups will contain $(Q^\times_N)^p$ as an index $p$ subgroup; since this is index $p^2$ in $Q^\times_N$, it suffices to show that our two norm groups both contain the element $N$. One one hand we have that

$$\text{Norm}^{K_N}_{Q_N}(N^{1/p}) = \prod_{i=0}^{p-1} \zeta^i p N^{1/p} = N$$

but we also have

$$\text{Norm}_{Q_N}^{(\zeta_{N})^p}((\text{Norm}_{Q_N}^{(\zeta_N)}) (1 - \zeta_N)) = \text{Norm}_{Q_N}^{(\zeta_{N})^p} (1 - \zeta_N) = \prod_{j=1}^{N-1} (1 - \zeta_N^j) = N.$$  

Therefore we conclude that $Q_N^{(\zeta_{N})^p} = K_N$.  \[ \rlap{\Box} \]

9
Stated in the language of cohomology groups, this says exactly that the class \( c \in H^1_S(F_p) \) which represents \( \mathbb{Q}(\zeta^{(p)}_N) \) is trivial when restricted to \( K_N \). In the language of cup products, this is the statement that \( b \cup c = 0 \in H^2_S(F_p) \).

3 Selmer groups and \( \text{Cl}_K \)

The goal of this section is to relate the \( p \)-rank \( r_K \) of the class group of \( K \) to the rank of a certain Selmer subgroup of the Galois cohomology of a cyclotomic twist of \( \text{Sym}^{p-4}V \), which in turn is bounded by dimensions of Selmer subgroups in the Galois cohomology of characters.

For simplicity, we will state the main theorem of this section for regular primes. The arguments in Sections 3.1 and 3.2 do not require that \( p \) be regular. However, some of the arguments in Sections 3.3, 3.4, and 3.5 break down in the absence of regularity. See Section 5.4 for a discussion of what happens when \( p \) is irregular. The main theorem of this section is:

**Theorem 3.0.1.** Let \( p \) be regular. We have

\[
r_K = 1 + h^1_{\Lambda}(\text{Sym}^{p-4}V \otimes F_p(2)).
\]

The structure of \( \text{Sym}^{p-4}V \otimes F_p(2) \) induces the following lower and upper bounds on \( r_K \)

\[
1 + h^1_{\Sigma}(F_p(-1)) \leq r_K \leq 1 + \sum_{i=1}^{p-3} h^1_{\Sigma}(F_p(-i)).
\]

This is essentially Theorem 1.3.1. The lower bound in this theorem was first established by Wake–Wang-Erickson; we recover this as Proposition 3.5.2. Throughout this section, \( E \) will be an unramified \( F_p \)-extension of \( K \) and \( M \) will be its Galois closure over \( \mathbb{Q} \). The proof begins in Section 3.1 with some preliminary lemmas on the structure of \( \text{Gal}(M/K(\zeta_p)) \) as a \( \text{Gal}(K(\zeta_p)/\mathbb{Q}) \)-representation.

In Section 3.2, we introduce an auxiliary Selmer condition \( \Lambda \), which will encode the local conditions that cut out certain Galois cohomology classes corresponding to unramified \( F_p \)-extensions of \( K \). We will also define a filtration on \( H^1_\Lambda(\text{Sym}^{p-3}V \otimes F_p(2)) \) related to the filtration defined by Iimura in [3] on \( \text{Cl}_K(\zeta_p) \); see Remark 3.2.4. This filtration of Iimura is also used by Lecouturier in [4].

The next step in the proof of Theorem 3.0.1 is to relate the Selmer condition \( \Lambda \) to the Selmer condition \( \Sigma \) defined in Section 2.2. This is done in Section 3.3, which also contains some general lemmas that realize \( \Sigma^* \) as the “correct” Selmer condition for discussing a specific extension problem related to the vanishing of certain Massey products.

Finally, we descend the filtration on \( H^1_\Lambda(\text{Sym}^{p-3}V \otimes F_p(2)) \) to a filtration on \( H^1_{\Sigma}(\text{Sym}^{p-4}V \otimes F_p(2)) \). In Section 3.4, we use this filtration to bound the rank \( h^1_{\Sigma}(\text{Sym}^{p-4}V \otimes F_p(2)) \) in terms of the ranks \( h^1_{\Sigma}(F_p(-i)) \) of the \( \Sigma \)-Selmer groups of characters. This will complete the proof of Theorem 3.0.1.

The discussion in Section 3.4 will also suggest a framework which we can use to think about bounding \( h^1_{\Sigma}(\text{Sym}^{p-4}V \otimes F_p(2)) \) from below using the \( h^1_{\Sigma}(F_p(-i)) \), which we explore briefly in Section 3.5.
3.1 Indecomposability of some $\text{Gal}(K(\zeta_p)/\mathbb{Q})$-modules arising from $\text{Cl}_K$

Let $E/K$ be unramified and Galois of degree $p$ and let $M$ be the Galois closure of $E$ over $\mathbb{Q}$, as in the diagram below.

\[
\begin{array}{c}
\text{M} \\
\text{E(\zeta_p)} \rightarrow A \\
\text{E} \\
\text{K(\zeta_p)} \\
\text{K} \\
\text{Q(\zeta_p)} \rightarrow \text{G} \\
\text{Q} \\
\end{array}
\]

\[\textit{(*)}\]

$M$ is the compositum of the $G := \text{Gal}(K(\zeta_p)/\mathbb{Q})$-translates of $E(\zeta_p)/K(\zeta_p)$, which implies that $M$ is an unramified elementary abelian $p$-extension of $K(\zeta_p)$. Thus $A := \text{Gal}(M/K(\zeta_p)) \cong (\mathbb{Z}/p\mathbb{Z})^m$ for some $m \geq 1$. This prompts the following definition.

**Definition 3.1.1.** With the above notation, we say that the unramified $\mathbb{F}_p$-extension $E/K$ is type $m$ where $m = \dim_{\mathbb{F}_p}(\text{Gal}(M/K(\zeta_p)))$.

Our goal in this subsection is to prove the following theorem.

**Theorem 3.1.2.** $A = \text{Gal}(M/K(\zeta_p))$ is an $\mathbb{F}_p$-vector space, and is isomorphic to $\text{Sym}^{m-1} V \otimes \mathbb{F}_p(1-m)$ as a $G = \text{Gal}(K(\zeta_p)/\mathbb{Q})$-representation where $m$ is the type of $E/K$. Furthermore, we have $1 \leq m \leq p - 2$. In particular, $A$ is indecomposable as a representation of $G$.

Note that our fixed primitive $p$th root of unity $\zeta_p$ gives us a canonical generator of $\text{Gal}(K(\zeta_p)/\mathbb{Q}(\zeta_p))$, namely the particular $\sigma$ with $\sigma(N^{1/p}) = \zeta_p N^{1/p}$. We use this to fix an isomorphism $G \cong \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$.

**Lemma 3.1.3.** The following short exact sequence splits.

$$1 \rightarrow A \rightarrow \text{Gal}(M/\mathbb{Q}) \rightarrow G \rightarrow 1$$

**Proof.** We argue by means of group cohomology; consider the Hochschild-Serre spectral sequence. Since $H^1(\mathbb{Z}/p\mathbb{Z}, A)$ is an $\mathbb{F}_p$-vector space, its order is coprime to the order of $(\mathbb{Z}/p\mathbb{Z})^\times$ and thus

$$H^i((\mathbb{Z}/p\mathbb{Z})^\times, H^1(\mathbb{Z}/p\mathbb{Z}, A)) = 0$$

for all $i > 0$. Hence the only nonzero column on the $E_2$ page is the 0th one, which implies that the restriction map

$$H^2(G, A) \rightarrow H^2(\mathbb{Z}/p\mathbb{Z}, A)^{(\mathbb{Z}/p\mathbb{Z})^\times}$$

is an isomorphism.

We wish to show that the class $[\text{Gal}(M/\mathbb{Q})] \in H^2(G, A)$ is 0. Its image in $H^2(\mathbb{Z}/p\mathbb{Z}, A)$ under the restriction map is the class of $[\text{Gal}(M/\mathbb{Q}(\zeta_p))]$ coming from

$$1 \rightarrow A \rightarrow \text{Gal}(M/\mathbb{Q}(\zeta_p)) \rightarrow \text{Gal}(K(\zeta_p)/\mathbb{Q}(\zeta_p)) \rightarrow 1.$$

We can explicitly construct a splitting of this sequence. Let $\mathfrak{N}$ be a prime of $M$ lying above $N$. The total ramification degree of $\mathfrak{N}$ in $M/\mathbb{Q}(\zeta_p)$ is $p$, since $N$ is totally ramified in $K(\zeta_p)/\mathbb{Q}(\zeta_p)$ and unramified in $M/K(\zeta_p)$, so the inertia group at $\mathfrak{N}$ is a copy of $\mathbb{Z}/p\mathbb{Z}$ in $\text{Gal}(M/\mathbb{Q}(\zeta_p))$ that maps isomorphically onto $\text{Gal}(K(\zeta_p)/\mathbb{Q}(\zeta_p))$. This inertia group is the image of our desired splitting. \[\square\]

Before continuing, we record the following general fact that we make use of throughout the section.
Lemma 3.1.4. Suppose that $F$ and $F'$ are extensions of $Q_p(\zeta_p)$, each of degree dividing $p$ and Galois over $Q_p$. Suppose further that $\text{Gal}(F/Q_p(\zeta_p))$ and $\text{Gal}(F'/Q_p(\zeta_p))$ are not isomorphic as representations of $\text{Gal}(Q_p(\zeta_p)/Q_p) = (Z/pZ)^\times$, or that both extensions are trivial. If $FF'/F$ is unramified, then $F'/Q_p(\zeta_p)$ is also unramified.

This follows from the fact that any unramified extension of $Q_p(\zeta_p)$ must be cyclic and Galois over $Q_p$, and that $F_p(i) \oplus F_p(j)$ has exactly two $(Z/pZ)^\times$-fixed lines when $i \neq j$.

Our next goal is to show that $1 \leq m \leq p - 2$ where $m$, as above, is the type of $E/K$. The lower inequality is immediate. However, we can say slightly more about this edge case.

Proposition 3.1.5. $E/K$ is of type 1 (i.e. $m = 1$) if and only if $E = K(\zeta_N^{(p)})$ is the genus field of $K$, where $\zeta_N^{(p)}$ is any generator of the degree-$p$ subfield of $Q(\zeta_N)/Q$.

Proof. The backward direction is trivial: It is clearly unramified away from $N$, Lemma 2.3.7 shows that $K(\zeta_N^{(p)})/K$ is unramified at $N$ as well, and the Galois closure of $K(\zeta_N^{(p)})/Q$ is $K(\zeta_p, \zeta_N^{(p)})$.

If $m = 1$ then $E(\zeta_p) = M$ is Galois over $Q$ and $A = \text{Gal}(E(\zeta_p)/K(\zeta_p)) = Z/pZ$. Consider the action of $G$ on $A$ by conjugation and recall that $G = Z/pZ \times (Z/pZ)^\times$. The order-$p$ subgroup of $G$ acts trivially on $A$ as there are no non-trivial 1-dimensional $F_p$-representations of $Z/pZ$. Referencing [4], we see that $(Z/pZ)^\times \subseteq G$ is the image of $\text{Gal}(E(\zeta_p)/E) \subseteq \text{Gal}(E(\zeta_p)/Q)$ which acts trivially on $A = \text{Gal}(E(\zeta_p)/K(\zeta_p))$, as $E(\zeta_p)$ is the compositum of the Galois extensions $E/K$ and $K(\zeta_p)/K$.

Thus we conclude that $G$ acts trivially on $A$ and hence that $\text{Gal}(E(\zeta_p)/Q) = Z/pZ \times G$ by Lemma 3.1.3. Consider $L = E(\zeta_p)^2$, which is $Z/pZ$ extension of $Q$. As $\text{Gal}(E(\zeta_p)/E) = (Z/pZ)^\times \subseteq G$ we know that $L \subseteq E$. As $L \neq K$ this tells us that $E = LK$.

We claim that $L = Q(\zeta_N^{(p)})$. To see this, it suffices to notice that $L$ is unramified away from $N$. By choice of $E$, it is automatically unramified away from $p$ and $N$. At $p$, it suffices to check that $L(\zeta_p)/Q(\zeta_p)$ is unramified, as $[L : Q]$ is coprime to $[Q(\zeta_p) : Q]$. Consider the following diagram of fields.

```
\begin{center}
\begin{tikzcd}
& E(\zeta_p) \ar[dr] & \\
L(\zeta_p) \ar[ur] & & K(\zeta_p) \\
L \ar[ur] \ar[dr] & Q(\zeta_p) \ar[ur] & \\
& Q \ar[ur]
\end{tikzcd}
\end{center}
```

Consider the corresponding extensions of fields locally at $p$. Because the groups $\text{Gal}(L(\zeta_p)/Q(\zeta_p))$ and $\text{Gal}(K(\zeta_p)/Q(\zeta_p))$ carry different actions of $\text{Gal}(Q(\zeta_p)/Q) = \text{Gal}(Q_p(\zeta_p)/Q_p)$, Lemma 3.1.4 gives us the desired conclusion. 

To prove Theorem 3.1.2 we need to view $A$ as a $G$-representation coming from the conjugation action of $G$ on $A$. Our first goal is to show that $A$ is indecomposable as a $G$-representation. We briefly recall the classification of indecomposable representations of groups of this kind:

**Theorem 3.1.6.** Let $k \in Z/(p - 1)Z$ and let $\Gamma_k$ be the group $Z/pZ \times (Z/pZ)^\times$, where $u \in (Z/pZ)^\times$ acts on $Z/pZ$ by multiplication by $u^k$.

The indecomposable $F_p$-representations of $\Gamma_k$ are exactly

$$\text{Sym}^i V_k \otimes F_p(i)$$

for $0 \leq i \leq p - 2$ and $0 \leq j \leq p - 1$, where $F_p(i)$ is the 1-dimensional representation where $u \in (Z/pZ)^\times$ acts by $u^i$ and $V_k$ is the 2-dimensional representation of $\Gamma_k$ over $F_p$ given by the map

$$\Gamma_k \to \text{GL}_2(F_p)$$

$$(b, u) \mapsto \begin{pmatrix} u^k & b \\ 0 & 1 \end{pmatrix}.$$
Writing our $A$ as a sum of indecomposable representations of $G = \Gamma_1$, we know that the number of indecomposable factors is equal to the dimension of $A^{\mathbb{Z}/p\mathbb{Z}}$. Indeed, each indecomposable factor when considered as a representation of $\mathbb{Z}/p\mathbb{Z}$ corresponds to a Jordan block with eigenvalue 1. Thus we’ve reduced the indecomposability of $A$ to showing that $A^{\mathbb{Z}/p\mathbb{Z}}$ is 1-dimensional.

**Lemma 3.1.7.** $A^{\mathbb{Z}/p\mathbb{Z}}$ is 1-dimensional. Furthermore, it carries the trivial $(\mathbb{Z}/p\mathbb{Z})^\times = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$-action.

**Proof.** The first part of the claim follows once we have shown that $H = A^{\mathbb{Z}/p\mathbb{Z}} \cap \text{Gal}(M/E(\zeta_p))$ is trivial since $\text{Gal}(M/E(\zeta_p))$ is codimension 1 in $A$. We will demonstrate this by showing that $H$ is normal in $\text{Gal}(M/\mathbb{Q})$. Indeed, as $M$ is the Galois closure of $E(\zeta_p)/\mathbb{Q}$, any normal subgroup of $\text{Gal}(M/\mathbb{Q})$ contained in $\text{Gal}(M/E(\zeta_p))$ is necessarily trivial.

Because $A$ is abelian, to show that $H$ is normal in $\text{Gal}(M/\mathbb{Q}) = A \times G$ it suffices to show that it is fixed by conjugation by $G$. Again applying the classification of indecomposable representations of $G$ we see that $A^{\mathbb{Z}/p\mathbb{Z}}$ is a product of characters and is thus a $G$-subrepresentation of $A$.

Referring to Lemma 3.1, notice now that the action of $(\mathbb{Z}/p\mathbb{Z})^\times = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ on $A$ is the same as the action of $\text{Gal}(E(\zeta_p)/E)$ on $A$. But the action of $\text{Gal}(E(\zeta_p)/E)$ on $A$ clearly stabilizes $\text{Gal}(M/E(\zeta_p)) \subseteq A$.

This shows that $(\mathbb{Z}/p\mathbb{Z})^\times \subseteq G$ stabilizes both $A^{\mathbb{Z}/p\mathbb{Z}}$ and $\text{Gal}(M/E(\zeta_p))$ and thus it stabilizes their intersection $H$. As $H \subseteq A^{\mathbb{Z}/p\mathbb{Z}}$ is also fixed pointwise by $\mathbb{Z}/p\mathbb{Z}$, we conclude that $H$ is fixed by the action of $G$ and is thus normal in $\text{Gal}(M/\mathbb{Q})$.

To see the second part of the lemma, we first notice as above that $(\mathbb{Z}/p\mathbb{Z})^\times$ acts on $A$ as $\text{Gal}(K(\zeta_p)/K)$ and thus acts trivially on $\text{Gal}(E(\zeta_p)/K(\zeta_p)) = \text{Gal}(E/K)$.

The short exact sequence
\[
1 \rightarrow \text{Gal}(M/E(\zeta_p)) \rightarrow A \rightarrow \text{Gal}(E(\zeta_p)/K(\zeta_p)) \rightarrow 1
\]
is $\text{Gal}(K(\zeta_p)/K)$-equivariant. As $A^{\mathbb{Z}/p\mathbb{Z}}$ has trivial intersection with the above kernel, it maps isomorphically onto $\text{Gal}(E(\zeta_p)/K(\zeta_p))$, which we just established carries the trivial $(\mathbb{Z}/p\mathbb{Z})^\times$ action.

The first part of Lemma 3.1 gives $A \cong \text{Sym}^i V \otimes F_p(i)$ for some $0 \leq i \leq p - 2$ and $0 \leq j \leq p - 1$, and the second part establishes that $i = -j$. This also implies that $A$ is a faithful representation of $G$ whenever $m \geq 2$, i.e., whenever $j \geq 1$.

We now have that $A \cong \text{Sym}^{m-1} V \otimes F_p(1-m)$ as $G$-representations, but to complete the proof of Theorem 3.1.2 it remains to show that $m \leq p - 2$. In what follows, it will be useful to write $\text{Gal}(M/\mathbb{Q})$ as an explicit matrix group that we can view as the image of a representation of $G_{\mathbb{Q},S}$.

**Remark 3.1.8.** Suppose that $A$ is an $F_p$-vector space and that $G \rightarrow \text{Aut}(A) = \text{GL}_m(F_p)$ is an injective homomorphism. Then $A \times G$ is isomorphic to the $(m + 1) \times (m + 1)$ block-matrix group
\[
\begin{pmatrix}
G & A \\
0 & 1
\end{pmatrix}
\]
where $G$ is identified with its image in $\text{GL}_m(F_p)$ and elements of $A$ are expressed as column vectors in the corresponding basis.

Assuming that $E$ is not the genus field of $K$, $A$ is a faithful $G$-representation so the previous remark establishes that in a suitable basis of $\text{Sym}^{m-1} V \otimes F_p(1-m)$ (fixed for the remainder of this article), $\text{Gal}(M/\mathbb{Q})$ is isomorphic to the group of matrices
\[
\begin{pmatrix}
1 & \chi^{-1}b & \chi^{-2}b^2 & \cdots & \chi^{-(m-1)}b^{(m-1)} \\
\chi^{-1} & \chi^{-2} & \chi^{-3} & \cdots & \chi^{-(m-1)}b^{(m-2)} \\
\chi^{-2} & \cdots & \chi^{-(m-1)}b^{(m-2)} \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
\chi^{-(m-1)}b & \cdots & \chi^{-1}b & \chi^{-2} & \chi^{-1} \\
\chi^{-(m-1)} & \cdots & \chi^{-1} & \chi^{-2} & \chi^{-1} \\
0 & \cdots & 1 & \chi^{-1} & \chi^{-2} & \chi^{-3} & \cdots & \chi^{-(m-1)}b^{(m-1)} & a_0 \\
a_1 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & a_{m-1} & \cdots & \cdots & \cdots & \cdots & \cdots & a_m \\
\end{pmatrix}
\]
where the $i,j$-th entry in the top left block is $\chi^{-(j-1)}b^{(j-1)}$. This also defines a representation $G_{\mathbb{Q},S} \rightarrow \text{Gal}(M/\mathbb{Q}) \rightarrow \text{GL}_{m+1}(F_p)$ of dimension $m + 1$ that we will consider more carefully in Section 3.2.
Remark 3.1.9. For the 2-dimensional representation $V$ we are considering, let \( \{e, f\} \) be the basis for $V$ as in the discussion at the start of Section 2.2. The usual basis for $\text{Sym}^k V$ is then \( \{e^k, e^{k-1}f, \ldots, f^k\} \). In that basis, the $i,j$-th entry of the top left block is, ignoring powers of the cyclotomic character, \((\zeta_p^i)^{b_j^{-1}}\). The basis we use is a rescaling of the usual basis to make it “compatible” with the quotient maps $\text{Sym}^k V \rightarrow \text{Sym}^{k-1} V$.

Indeed, we can view the representation $G_{Q,S} \rightarrow \GL_{m+1}(\mathbb{F}_p)$ defined by the matrix \( \mathbf{**} \) as an extension of the trivial representation by the representation $\text{Sym}^{m-1} V \otimes \mathbb{F}_p(1-m)$. The quotient map $\text{Sym}^{m-1} V \otimes \mathbb{F}_p(1-m) \rightarrow \text{Sym}^{m-2} V \otimes \mathbb{F}_p(1-m)$ induces a map on Ext groups. Applying this to the extension above gives a new extension of the trivial representation by the representation $\text{Sym}^{m-2} V \otimes \mathbb{F}_p(1-m)$, which we can write explicitly as a map $G_{Q,S} \rightarrow \GL_m(\mathbb{F}_p)$. The bases of $\text{Sym}^k V$ are chosen so that the image of this representation is the exactly the matrix \( \mathbf{**} \) with the first row and column removed.

If $E = \mathbb{Q}(N^{1/p}, \zeta_N^{(p)})$ is the genus field, we instead consider the representation $G_{Q,S} \rightarrow \GL_2(\mathbb{F}_p)$ of the form
\[
\begin{pmatrix}
1 & c \\
0 & 1
\end{pmatrix}
\]
where $c \in \text{Hom}(G_{Q,S}, \mathbb{F}_p) = H^1(\mathbb{Z}_p, \mathbb{F}_p)$ is the class defining the extension $\mathbb{Q}(\zeta_N^{(p)})/\mathbb{Q}$.

Remark 3.1.10. As $M/K(\zeta_p)$ is unramified, we can view its Galois group $A$ as a quotient of the $p$-part of the class group $\text{Cl}_K(\zeta_p)$. The results above can then be viewed through the lens of decomposing this class group into a sum of indecomposable $\text{Gal}(K(\zeta_p)/\mathbb{Q})$-representations, similar to classical results on decomposing the $p$ part of $\text{Cl}_K(\zeta_p)$ into a sum of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$-representations. In Section 4 we will see that the numbers $M_i$ defined in Section 4 play a similar role to that of the Bernoulli numbers in the structure of $\text{Cl}_K(\zeta_p)$.

The structure of $\text{Cl}_K(\zeta_p)$ as a Galois module was also studied by Imura in [3]. We will discuss the connection between Imura’s work and our current approach is discussed in slightly more detail in Remark 3.2.3.

With the above matrix representation in hand, we can now prove that $m \leq p - 2$. Notice that we already have that $m \leq p$ since all indecomposable representations of $G$ have dimension $\leq p$. We will show directly that $m \neq p, p - 1$ using some of the Galois cohomology facts discussed at the beginning of Section 2.

Lemma 3.1.11. $m \neq p$.

Proof. Suppose that $m = p$. The lower $2 \times 2$ corner of the matrix \( \mathbf{**} \) will thus be
\[
\begin{pmatrix}
1 & a_{p-1} \\
0 & 1
\end{pmatrix}
\]
which we think of as a quotient of $\text{Gal}(M/\mathbb{Q})$ (alternatively, as a new $G_{Q,S}$-representation with $G_{M,S}$ in the kernel). This gives us a class $a_{p-1} \in H^1(\mathbb{Z}_p, \mathbb{F}_p)$, and it cuts out a $\mathbb{Z}/p\mathbb{Z}$ extension $L$ of $\mathbb{Q}$ contained in $M$ and hence unramified outside of $S$. We will show that this extension is necessarily unramified at $N$ and $p$ as well, contradicting its existence. For $p$, consider the diagram of fields
\[
\begin{array}{ccc}
L \text{K}(\zeta_p) & & L(\zeta_p) \\
\downarrow & & \downarrow \\
K(\zeta_p) & & L(\zeta_p) \\
\downarrow & & \downarrow \\
\mathbb{Q}(\zeta_p) & & L \\
\downarrow & & \downarrow \\
\mathbb{Q} & & \mathbb{Q}
\end{array}
\]
locally at $p$. As $L \subseteq M$ we know that $L \text{K}(\zeta_p)/K(\zeta_p)$ is unramified at $p$. Applying Lemma 3.1.4 we conclude that $L(\zeta_p)/\mathbb{Q}(\zeta_p)$, and hence $L/\mathbb{Q}$, is also unramified at $p$.

Suppose independently that $L/\mathbb{Q}$ is (tamely) ramified at $N$. The inertia group(s) above $N$ in $\text{Gal}(M/\mathbb{Q})$ are cyclic of order $p$ as $M/K(\zeta_p)$ is unramified. If $\tau$ is a generator of the tame inertia group of $\mathbb{Q}_N$ we know
by the functoriality of inertia groups that \( b(\tau) \) and \( a_{p-1}(\tau) \) are both non-zero, as the extensions \( K(\zeta_p) \) and \( L \) defined by these classes are tamely ramified at \( N \). Under the quotient map \( G_{\mathbb{Q},S} \to \text{Gal}(M/\mathbb{Q}) \) we have

\[
\tau \mapsto \begin{pmatrix}
1 & b(\tau) & \cdots & b(\tau)^{p-1} \left( \frac{p-1}{(p-2)!} \right) & a_0(\tau) \\
1 & b(\tau) & \cdots & b(\tau)^{p-2} \left( \frac{p-2}{(p-2)!} \right) & a_1(\tau) \\
& & \ddots & \vdots & \vdots \\
& & & b(\tau) & a_{p-2}(\tau) \\
& & & 1 & a_{p-1}(\tau)
\end{pmatrix}.
\]

Raising this to the \( p \)th power, we get

\[
\tau^p \mapsto \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & b(\tau)^{p-1}a_{p-1}(\tau) \\
1 & 0 & \cdots & 0 & 0 & 0 \\
& & \ddots & \vdots & \vdots & \vdots \\
& & & 1 & 0 & 0 \\
& & & & 1 & 1
\end{pmatrix}
\]

which is non-zero, contradicting the fact that the generator of the inertia group at \( N \) has order \( p \).

**Lemma 3.1.12.** \( m \neq p - 1 \).

**Proof.** The lower \( 2 \times 2 \) corner of the matrix \( \boxed{**} \) will thus be

\[
\chi \begin{pmatrix}
a_{p-2} \\
0
\end{pmatrix}
\]

where \( a_{p-2} \in H_1^S(\mathbb{F}_p(1)) \). As in the previous lemma, we deduce the existence of an extension \( L/\mathbb{Q}(\zeta_p) \) contained in \( M \) which is Galois over \( \mathbb{Q} \), with Galois group isomorphic to \( G \). The extension \( L \) is not equal to \( K(\zeta_p) \) however; we have that \( A \) surjects onto \( \text{Gal}(L/\mathbb{Q}(\zeta_p)) \) but not \( \text{Gal}(K(\zeta_p)/\mathbb{Q}(\zeta_p)) \) as \( A \) is equal to the kernel of \( \text{Gal}(M/\mathbb{Q}) \to \text{Gal}(K(\zeta_p)/\mathbb{Q}) \). Thus we must have that \( a_{p-2} \) is not a nonzero multiple of the class \( b \in H_1^S(\mathbb{F}_p(1)) \). However, we know that \( a_{p-2} \cup b = 0 \) since there is a 3-dimensional representation of \( G_{\mathbb{Q},S} \) coming from the lower \( 3 \times 3 \) quotient

\[
\chi^2 \begin{pmatrix}
\chi b & a_{p-3} \\
0 & \chi \\
0 & 0 & 1
\end{pmatrix}
\]

of the matrix \( \boxed{**} \), so \( a_{p-2} \) must be a multiple of \( b \) by Corollary 2.3.5. This gives that \( a_{p-2} = 0 \), but then \( \dim_{\mathbb{F}_p}(A) \leq p - 2 \) so \( E/K \) is not in fact type \( p - 1 \).

### 3.2 An Auxiliary Selmer Group

In the previous section, we obtained from an unramified \( \mathbb{F}_p \)-extension \( E/K \) of type \( m \) a representation \( G_{\mathbb{Q},S} \to \text{GL}_{m+1}(\mathbb{F}_p) \) of the form \( \boxed{**} \). As a representation, it is an extension of the trivial representation by \( \text{Sym}^{m-1}V \otimes \mathbb{F}_p(1-m) \) considered as a \( G_{\mathbb{Q},S} \)-representation via the quotient \( G_{\mathbb{Q},S} \to G \), so it gives a class

\[
a_E = [a_0] \in H_1^S(\text{Sym}^{m-1}V \otimes \mathbb{F}_p(1-m))
\]

as discussed in Section 2.1.

Let \( \Lambda \) be the Selmer condition defined by

- \( L_\ell = H_{\text{ur}}^1(G_{\mathbb{Q},\ell}, A) \) for \( \ell \neq N, p \)
Remark 3.2.1. In the case of the Galois module $F_p$, the containment $H^1_{\Lambda}(F_p) \subseteq H^1_{\Lambda}(F_p)$ is an equality. This is to say that any $F_p$-extension $L/Q$ unramified away from $S$ and unramified at $p$ after base change to $K(\zeta_p)$ was necessarily unramified at $p$ over $Q$. This is essentially a corollary of the proof of Lemma 3.1.5.

Although we don’t need the following fact, it is true that for all of the modules $A$ listed in Theorem 3.1.2 which can arise as $\text{Gal}(M/K(\zeta_p))$, one has $H^1_{\Lambda}(A) = H^1_{\Lambda}(A)$; this follows from Lemma 3.3.4. However, if one wants to use the methods of this section to study $Cl_{K(\zeta_p)}$ or the case of composite $N$, it is necessary to use modules $A$ for which $H^1_{\Lambda}(A) \neq H^1_{\Lambda}(A)$.

In this subsection we prove

**Theorem 3.2.2.** $r_K = h^1_{\Lambda}(\text{Sym}^{p-3}V \otimes F_p(2))$.

The main step in the proof of this theorem is to show that the class $a_E$ lies in the $\Lambda$-Selmer subgroup $H^1_{\Lambda}(\text{Sym}^{m-1}V \otimes F_p(1-m))$ and conversely that any such Selmer class arises from an unramified $F_p$-extension $E/K$. The forward direction is trivial: the only thing to check is that it satisfies the correct condition at $p$, which follows from the fact that $M/K(\zeta_p)$ is unramified above $p$.

Note that there is some ambiguity in the choice of $a_E$ as any constant multiple of it defines the same field extension. In the end, the proof of Theorem 3.2.2 comes down to establishing a bijection between the projectivized space $\text{PH}^1_{\Lambda}(\text{Sym}^{p-3}V \otimes F_p(2))$ and the set of unramified $F_p$-extensions $E/K$, which can itself be thought of as the projectivization of the $p$-part of $Cl_K$.

In order to promote $a_E$ to a class in $H^1_{\Lambda}(\text{Sym}^{p-3}V \otimes F_p(2))$, consider the natural filtration on $\text{Sym}^{p-3}V \otimes F_p(2) = \text{Sym}^{p-3}V \otimes F_p(3-p)$ given by

$$0 \subseteq F_p = \text{Sym}^0V \otimes F_p(0) \subseteq \text{Sym}^1V \otimes F_p(-1) \subseteq \text{Sym}^2V \otimes F_p(-2) \subseteq \cdots \subseteq \text{Sym}^{p-3}V \otimes F_p(3-p).$$

where the $k$th subspace is the span of the first $k$ basis vectors in the basis used above in the matrix (16). The successive quotients are

$$\frac{\text{Sym}^kV \otimes F_p(-k)}{\text{Sym}^{k-1}V \otimes F_p(1-k)} \cong F_p(-k).$$

Since these have no $G_{Q,S}$-fixed points, as $1 \leq k \leq p-3$, we get a corresponding filtration in cohomology

$$0 \subseteq H^1_{\Lambda}(F_p) \subseteq H^1_{\Lambda}(\text{Sym}^1V \otimes F_p(-1)) \subseteq H^1_{\Lambda}(\text{Sym}^2V \otimes F_p(-2)) \subseteq \cdots \subseteq H^1_{\Lambda}(\text{Sym}^{p-3}V \otimes F_p(3-p))$$

where each inclusion can be realized concretely via

$$\begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} \mapsto \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \\ 0 \end{pmatrix}.$$

This filtration restricts to a filtration on the Selmer subgroups $H^1_{\Lambda}(-)$. Thus, given our $E/K$ of type $m$, we get an element (defined up to a scalar) in $H^1_{\Lambda}(\text{Sym}^{p-3}V \otimes F_p(2))$, as desired.
Conversely, given a nonzero class \( a \in H^1_\Lambda(\text{Sym}^{p-3}V \otimes F_p(2)) \), we can restrict it to a class in \( G_{K,S} \)-cohomology to get a representation of \( G_{K,S} \) of the form

\[
\begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & a_0 \\
\chi^{-1} & 0 & 0 & \cdots & 0 & a_1 \\
\chi^{-2} & \vdots & \ddots & \vdots \\
\vdots & \ddots & \ddots & 0 & a_{p-4} \\
\chi^2 & a_{p-3} & & & 1
\end{pmatrix}
\]

From this we see that \( a_0|_{G_{K,S}} \) is a homomorphism \( G_{K,S} \rightarrow F_p \). Note that some of the \( a_i \) might be 0 if \( a \) comes from some smaller piece of the filtration above, but \( a_0|_{G_{K,S}} \neq 0 \) by the following lemma. Thus, it cuts out an \( F_p \)-extension \( E_a = K^{\ker(a_0|_{G_{K,S}})} \) of \( K \).

**Lemma 3.2.3.** If \( a \in H^1_\Lambda(\text{Sym}^{p-3}V \otimes F_p(2)) \) is nonzero then \( a_0|_{G_{K,S}} : G_{K,S} \rightarrow F_p \) is nonzero as well.

**Proof.** We show the equivalent statement that \( a_0 \) is nonzero when restricted to \( G_{K(\zeta_p),S} \). Let \( A = \text{Sym}^{p-3}V \otimes F_p(2) \) and consider the inflation-restriction sequence

\[
0 \rightarrow H^1(G,A) \rightarrow H^1(G_{\mathbb{Q},S},A) \rightarrow H^1(G_{K(\zeta_p),S},A)^G.
\]

We claim that \( H^1(G,A) = 0 \). Using inflation-restriction again, we get that

\[
H^1(G,A) \cong H^1(\mathbb{Z}/p\mathbb{Z},A)^{\mathbb{Z}/p\mathbb{Z}}.
\]

It can be explicitly seen that \( H^1(\mathbb{Z}/p\mathbb{Z},A) = F_p(2) \) as a \( (\mathbb{Z}/p\mathbb{Z})^\times \)-module, implying that

\[
H^1(\mathbb{Z}/p\mathbb{Z},A)^{\mathbb{Z}/p\mathbb{Z}} = 0.
\]

Therefore, a nonzero \( a \in H^1(G_{\mathbb{Q},S},A) \) restricts to a nonzero homomorphism \( G_{K(\zeta_p),S} \rightarrow A = F_p^{p-2} \) that is invariant under \( G \). In particular, its image is fixed by the action of \( G \) on \( A \) so its image is a nonzero \( G \)-subrepresentation. However, the only nontrivial \( G \)-subrepresentations of \( A \) are the spans of the first \( k \geq 1 \) basis vectors, all of which contain some element whose first coordinate is nonzero.

The Selmer condition \( A \) guarantees that this extension \( E_a/K \) is unramified everywhere. This is obvious for all \( \ell \neq N,p \).

At \( N \), recall from the proof of Proposition 2.2.2 that \( H^1(G_{\mathbb{Q},S},\text{Sym}^kV \otimes F_p(-k)) \) is 2-dimensional, spanned by an unramified class and the class corresponding to \( K_N \), so the image of any class here in \( H^1(G_{K_S},\text{Sym}^kV \otimes F_p(-k)) \) is unramified. At \( p \), it suffices to remark that \( [E_a : K] \) is prime to \( [K(\zeta_p) : K] \), and thus \( E_a/K \) is unramified exactly when \( E(\zeta_p)/K(\zeta_p) \) is.

Finally, to finish the proof of Theorem 3.2.2, we remark that the assignments \( E \mapsto a_E \) and \( a \mapsto E_a \) are mutually inverse. Indeed, given an unramified \( E/K \), Theorem 3.1.2 along with the above discussion implies that \( M/K \) has a unique \( F_p \)-subextension which is stabilized by the action of \( \text{Gal}(K(\zeta_p)/K) = (\mathbb{Z}/p\mathbb{Z})^\times \) (the one defined by \( a_{E,0} \)) which must be \( E \).

Conversely, take any two cohomology classes \( a,a' \in H^1_\Lambda(\text{Sym}^{p-3}V \otimes F_p(2)) \) and assume \( E_a = E_{a'} \), which implies that \( a_0|_{G_{K,S}} \) is a constant multiple of \( a_0'|_{G_{K,S}} \). Scaling \( a' \) so that these are equal and applying Lemma 3.2.3 to \( a-a' \), we conclude that \( a-a' = 0 \) and hence \( a = a' \).

**Remark 3.2.4.** We can now think of the filtration on \( H^1_\Lambda(\text{Sym}^{p-3}V \otimes F_p(2)) \) from the perspective of the types \( m \) of the extensions \( E/K \). Under the correspondence used to prove Theorem 3.2.2 the subspace \( H^1_\Lambda(\text{Sym}^{k}V \otimes F_p(-k)) \) contains the \( E \) of type \( m \leq k+1 \), and the quotient

\[
\frac{H^1_\Lambda(\text{Sym}^{k}V \otimes F_p(-k))}{H^1_\Lambda(\text{Sym}^{k-1}V \otimes F_p(1-k))}
\]

is nonzero exactly when there is an \( E/K \) of type \( k+1 \).
In [3], Iimura defines a descending filtration on the $p$-part of $A = \mathrm{Cl}_{K(G)}$ by considering it as a $\mathbb{F}_p[G]$-module. Let $\sigma \in G$ be order $p$. The $i$th piece $J_i$ of the filtration is the image of $(\sigma - 1)^i A$. Comparing his construction with the one given in this section, one sees that quotients of the $(\mathbb{Z}/p\mathbb{Z})^k$-coinvariants of $J_0/J_k$ give extensions $E/K$ of type $m \leq k$, and that quotients of the $(\mathbb{Z}/p\mathbb{Z})^\infty$-coinvariants of $J_{m-1}/J_m$ give extensions $E/K$ of type exactly $m$.

In [9], Sharifi connects Iimura’s filtration to the vanishing of Massey products (see Theorem A of [9]). In this theorem, the $4$th graded piece of the filtration is shown to be related to a $(k + 1)$-fold Massey product with $k$ copies of a Kummer generator; our matrix [***] witnesses the vanishing of such a Massey product.

### 3.3 An Exact Sequence of Selmer Groups

Starting here, we assume that $p$ is regular. The goal of this subsection is to provide some motivation for the definitions of the Selmer conditions $\Sigma$ and $\Sigma^*$ and to prove the following proposition:

**Proposition 3.3.1.** Let $p$ be regular. Let $1 \leq k \leq p - 3$. There is an exact sequence

$$0 \to H^1_{\Lambda}(\mathbb{F}_p) \to H^1_{\Lambda}(\text{Sym}^k V \otimes \mathbb{F}_p(-k)) \to H^1_{\Sigma^1}(\text{Sym}^{k-1} V \otimes \mathbb{F}_p(k)) \to 0.$$ 

In particular,

$$h^1_{\Lambda}(\text{Sym}^{p-3} V \otimes \mathbb{F}_p(2)) = 1 + h^1_{\Lambda}(\text{Sym}^{p-4} V \otimes \mathbb{F}_p(2)).$$

The last equality follows from the $k = p - 3$ case of the first part of the proposition combined with part 2 of Theorem 2.3.1, which gives that $h^1_{\Lambda}(\mathbb{F}_p) = 1$.

Let $1 \leq k \leq p - 3$ and consider the short exact sequence of $G_{\mathbb{Q}, \sigma}$-representations

$$0 \to \mathbb{F}_p \to \text{Sym}^k V \otimes \mathbb{F}_p(-k) \to \text{Sym}^{k-1} V \otimes \mathbb{F}_p(-k) \to 0.$$ 

Sym$^{k-1} V \otimes \mathbb{F}_p(-k)$ has no $G_{\mathbb{Q}, \sigma}$-fixed points, so taking $G_{\mathbb{Q}, \sigma}$-cohomology gives that the top row of the following commutative diagram is exact; Proposition 3.3.1 is the statement that the bottom row of this diagram is exact as well.

$$\begin{array}{cccccc}
0 & \longrightarrow & H^1_{\Lambda}(\mathbb{F}_p) & \longrightarrow & H^1_{\Lambda}(\text{Sym}^k V \otimes \mathbb{F}_p(-k)) & \longrightarrow & H^1_{\Sigma^1}(\text{Sym}^{k-1} V \otimes \mathbb{F}_p(-k)) \\
& & \ | & & \ | & & \\
0 & \longrightarrow & H^1_{\Lambda}(\mathbb{F}_p) & \longrightarrow & H^1_{\Lambda}(\text{Sym}^k V \otimes \mathbb{F}_p(-k)) & \longrightarrow & H^1_{\Sigma^1}(\text{Sym}^{k-1} V \otimes \mathbb{F}_p(-k)) & \longrightarrow & 0.
\end{array}$$

To show this exactness of the bottom row, we need to show:

1. The image of $H^1_{\Lambda}(\text{Sym}^k V \otimes \mathbb{F}_p(-k))$ in $H^1_{\Sigma^1}(\text{Sym}^{k-1} V \otimes \mathbb{F}_p(-k))$ is contained in the Selmer subgroup $H^1_{\Lambda}(\text{Sym}^{k-1} V \otimes \mathbb{F}_p(-k))$.

2. The induced map $H^1_{\Lambda}(\text{Sym}^k V \otimes \mathbb{F}_p(-k)) \to H^1_{\Sigma^1}(\text{Sym}^{k-1} V \otimes \mathbb{F}_p(-k))$ is surjective.

3. The kernel of this induced map is precisely $H^1_{\Lambda}(\mathbb{F}_p) \subseteq H^1_{\Sigma^1}(\mathbb{F}_p)$.

The third item is the easiest; we just need that the intersection of image of $H^1_{\Lambda}(\mathbb{F}_p)$ with $H^1_{\Lambda}(\text{Sym}^{k-1} V \otimes \mathbb{F}_p(-k))$ in $H^1_{\Sigma^1}(\text{Sym}^k V \otimes \mathbb{F}_p(-k))$ is $H^1_{\Lambda}(\mathbb{F}_p)$, which follows from Remark 3.2.1 that $H^1_{\Lambda}(\mathbb{F}_p) = H^1_{\Lambda}(\mathbb{F}_p)$.

The proof of the remainder of the proposition is broken up into two parts. Lemma 3.3.2 establishes Parts 1 and 2 above with $\Lambda$ replaced by $S$ and $\Sigma$ replaced by $\Sigma^*$ by considering the local condition at $N$. To get the corresponding statements for $\Lambda$ and $\Sigma$, we need to consider the local conditions at $p$, which is done in Lemmas 3.3.3 and 3.3.4.

Lemma 3.3.2 is stated in slightly more generality than we presently need. To establish Theorem 3.3.1 we only need the case $i = j$. The full strength of this lemma is used in Sections 3.5 and 5 when we discuss issues of extending Galois representations of this kind.
Theorem 3.3.2. For any $1 \leq i \leq p - 3$, $0 \leq j \leq i$, the image of $H^1_S(\text{Sym}^j V \otimes F_p(-i))$ in $H^1_S(\text{Sym}^{j-1} V \otimes F_p(-i))$ is precisely $H^1_S(\text{Sym}^{j-1} V \otimes F_p(-i))$.

Equivalently, a $G_{Q_S}$-representation of dimension $j + 1$ coming from an element $a \in H^1_S(\text{Sym}^{j-1} V \otimes F_p(-i))$ of the form

$$
\begin{pmatrix}
\chi^j \cdot \chi^j \cdot \vdots \cdot \chi^i \cdot a_j \\
\chi^j \cdot \chi^i \cdot \vdots \cdot \chi^i \cdot a_{j-1}
\end{pmatrix}
$$

extends to a $G_{Q_S}$-representation of dimension $j + 2$ of the form

$$
\begin{pmatrix}
\chi^j \cdot \chi^i \cdot \vdots \cdot \chi^i \cdot a_j \\
\chi^j \cdot \chi^i \cdot \vdots \cdot \chi^i \cdot a_{j-1}
\end{pmatrix}
$$

if and only if $a \in H^1_S(\text{Sym}^{j-1} V \otimes F_p(-i))$.

Proof. Consider the following commutative diagram of cohomology groups.

$$
\begin{array}{cccc}
H^1_S(\text{Sym}^j V \otimes F_p(-i)) & \rightarrow & H^1_S(\text{Sym}^{j-1} V \otimes F_p(-i)) & \rightarrow & H^1_S(\text{Sym}^{j-1} V \otimes F_p(-i)) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(G_{Q_S}, F_p) & \rightarrow & H^1(G_{Q_S}, \text{Sym}^j V) & \rightarrow & H^1(G_{Q_S}, \text{Sym}^{j-1} V) & \rightarrow & H^2(G_{Q_S}, F_p).
\end{array}
$$

We are concerned with the image of the middle map in the top row, which is the kernel of the following boundary map. Let $a \in H^1_S(\text{Sym}^{j-1} V \otimes F_p(i))$. Its image under the boundary map is the cup product of $a$ with the class in

$$
H^1_S(\text{Sym}^{j-1} V \otimes F_p(-i))
$$

that realizes $\text{Sym}^j V \otimes F_p(-i)$ as an extension of $\text{Sym}^{j-1} V \otimes F_p(-i)$ by $F_p(j - i)$. By Proposition 2.3.4, we can look locally at $N$ to determine if cup products are 0. Locally at $N$, all of the modules are self-dual by Lemma 2.2.1 and thus we might as well think of $\text{Sym}^j V$ as an extension of $F_p$ by $\text{Sym}^{j-1} V$. The corresponding class in $H^1(G_{Q_S}, \text{Sym}^{j-1} V)$ giving this extension is the column vector $b = [\chi^j, \chi^i, \chi^i, \chi^i, \chi^i, \chi^i, \chi^i, \chi^i, \chi^i]^T$ in the notation of Proposition 2.2.2.

This is in the kernel of the map to $H^1(G_{K_N}, \text{Sym}^{j-1} V)$. As we established in Proposition 2.2.2, $a \cup b = 0$ is then equivalent to $a|_{G_{K_N}} = 0$, i.e., $a \in H^1_S(\text{Sym}^{j-1} V \otimes F_p(i))$.

Lemma 3.3.3. Let $1 \leq k \leq p - 3$. Any class $a \in H^1_S(\text{Sym}^k V \otimes F_p(-k))$ has a lift to $H^1_A(\text{Sym}^k V \otimes F_p(-k))$.

Proof. Write $a = [a_1, \cdots, a_k]^T$. Choose any $a_0$ giving us a lift to $H^1_A(\text{Sym}^k V \otimes F_p(-k))$, which is possible by the previous lemma. By assumption, $a_i|_{G_{Q_S}} = 0$ for all $1 \leq i \leq k$. We need to show that $a_0$ can be modified so that it is unramified when restricted to $K(\zeta_{p^2})$.

It can in fact be chosen to be unramified over $Q_p$. $H^1_A(G_{Q_p}, F_p)$ is 2-dimensional, spanned by an unramified class and the class corresponding to $Q_p(\zeta_{p^2})$. But this class is in the image of the global classes, so by adding an appropriate multiple of this class to $a_0$ we get the desired conclusion.
Lemma 3.3.4. Let $1 \leq k \leq p-3$. Let $a$ be any class

$$a = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{bmatrix} \in H^1_A(Sym^k V \otimes F_p(-k)).$$

Then $a_i|_{G_{Q_p}} = 0$ for all $i \neq 0$. Furthermore, $a_0$ restricts to an unramified homomorphism $G_{Q_p} \to F_p$.

Proof. The proof is by strong induction on $i$, starting with $a_k$. Let $M$ be the Galois extension of $Q$ defined by the kernel of the representation associated to $a$. We begin by examining the $G_{Q,S}$-representation associated to the image of $a$ in $H^1_S(Sym^{k-1} V \otimes F_p(-k))$:

$$
\begin{pmatrix}
\chi^{-1} & \chi^{-2}b & \chi^{-3}b^2 & \cdots & \chi^{-k} \frac{b^{k-1}}{(k-1)!} \\
\chi^{-2} & \chi^{-3}b & \cdots & \chi^{-k} \frac{b^{k-2}}{(k-2)!} \\
\vdots & \vdots & \ddots & \vdots \\
\chi^{1-k} & \chi^{-k}b & a_{k-1} \\
\chi^{-k} & a_k & 1
\end{pmatrix} = 0.
$$

Restrict this representation to $G_{Q_p}$. Looking at the bottom $2 \times 2$ quotient, we notice that $a_k|_{G_{Q_p}}$ gives an extension $L_k/Q_p(\zeta_p)$ contained in $M_p$. If it is nontrivial, its Galois group is $F_p(-k)$ as a Gal($Q_p(\zeta_p)/Q_p$)-module. Since $a$ satisfies the Selmer condition $\Lambda$, $L_kK(\zeta_p)_{p}/K(\zeta_p)_{p}$ is unramified. As $-k \neq 1 \mod p - 1$, Lemma 3.1.4 then applies to conclude that $L_k/Q_p(\zeta_p)$ is unramified. Equivalently, $a_k|_{G_{Q_p}}$ lies in $H^1_{ur}(G_{Q_p}, F_p(-k))$ which is trivial as $k \neq 0 \mod p - 1$.

Still restricting to $G_{Q_p}$, we now have that the bottom $3 \times 3$ quotient of the representation given by the matrix above is

$$
\begin{pmatrix}
\chi^{1-k} & \chi^{-k}b & a_{k-1} \\
\chi^{-k} & a_k & 1
\end{pmatrix}.
$$

Thus $a_{k-1} \in H^1(G_{Q_p}, F_p(1-k))$ and so defines an extension $L_{k-1}/Q_p(\zeta_p)$. If it’s non trivial, it has an action of Gal($Q_p(\zeta_p)/Q_p$) by $\chi^{1-k}$. Again, as above, $L_{k-1}K(\zeta_p)_{p}/K(\zeta_p)_{p}$ is unramified, so we conclude that $a_{k-1} \in H^1_{ur}(G_{Q_p}, F_p(1-k)) = 0$.

We can continue inductively in the same manner to show that $a_{k-i} = 0$ for $0 \leq i \leq k-1$. The two facts we need are that $\chi^{1-k} \neq \chi$ so that Lemma 3.1.4 applies, and that $\chi^{-k}$ is nontrivial so that $H^1_{ur}(G_{Q_p}, F_p(i)) = 0$.

To get the final claim about $a_0$, carry out one more step of the induction. Lemma 3.1.4 applies in this case, but the second fact above does not.

3.4 $Cl_K$ and Selmer Groups of Characters

Recall the filtration on $H^1_A(Sym^{p-3} V \otimes F_p(2))$ by types considered in Remark 3.2.4. As a corollary to Proposition 3.3.1, we conclude that this filtration descends to a filtration

$$0 \subseteq H^1_L(F_p(-1)) \subseteq H^1_L(Sym^1 V \otimes F_p(-2)) \subseteq H^1_L(Sym^2 V \otimes F_p(-3)) \subseteq \cdots \subseteq H^1_L(Sym^{p-4} V \otimes F_p(2)).$$

In the spirit of Remark 3.2.4, we can think of the $k$th piece $H^1_L(Sym^{k-1} V \otimes F_p(-k))$ in the above filtration as corresponding to those $E/K$ of type $2 \leq m \leq k + 1$, and the quotient

$$
\frac{H^1_L(Sym^{k-1} V \otimes F_p(-k))}{H^1_L(Sym^{k-2} V \otimes F_p(1-k))}
$$
corresponds to the extensions of type exactly $k+1$, in the sense that its dimension is the number of equivalent extensions $E/K$ of type $k+1$, where two such extensions are equivalent if they become the same after taking the compositum with an extension of strictly smaller type.

With this in mind, we offer the following proposition.

**Proposition 3.4.1.** The following are true:

1. $h^1_\Sigma(F_p(-1)) \leq h_\Sigma(Sym^{p-4}V \otimes F_p(2))$.

2. If there is an $E/K$ of type $m \geq 2$, then $H^1_\Sigma(F_p(1-m))$ is nontrivial.

3. $h^1_\Sigma(Sym^{p-4}V \otimes F_p(2)) \leq \sum_{i=1}^{p-3} h^1_\Sigma(F_p(-i))$.

**Proof.** The first part of the proposition follows from the fact that the smallest piece in the above filtration is $H^1_\Sigma(F_p(-1)) \subseteq H^1_\Sigma(Sym^{p-4}V \otimes F_p(2))$.

Now, from the exact sequence

$$0 \to \text{Sym}^{k-2}V \otimes F_p(1-k) \to \text{Sym}^{k-1}V \otimes F_p(-k) \to F_p(-k) \to 0$$

we can look at the $\Sigma$-Selmer subgroups of the long exact sequence in $G_{Q,S}$-cohomology to get the exact sequence

$$0 \to H^1_\Sigma(\text{Sym}^{k-2}V \otimes F_p(1-k)) \to H^1_\Sigma(\text{Sym}^{k-1}V \otimes F_p(-k)) \to H^1_\Sigma(F_p(-k)).$$

Thus

$$\frac{H^1_\Sigma(\text{Sym}^{k-2}V \otimes F_p(1-k))}{H^1_\Sigma(\text{Sym}^{k-2}V \otimes F_p(-k))} \subseteq H^1_\Sigma(F_p(-k))$$

which establishes the second part of the proposition: if there is an $E/K$ of type $m$ then $H^1_\Sigma(F_p(1-m)) \neq 0$, and furthermore that the size of this group is related to the number of inequivalent extensions of type $m$ as discussed above.

The associated graded space of $H^1_\Sigma(\text{Sym}^{p-4}V \otimes F_p(2))$ equipped with this filtration is

$$\text{gr}(H^1_\Sigma(\text{Sym}^{p-4}V \otimes F_p(2))) = \bigoplus_{k=1}^{p-3} \frac{H^1_\Sigma(\text{Sym}^{k-1}V \otimes F_p(-k))}{H^1_\Sigma(\text{Sym}^{k-2}V \otimes F_p(1-k))} \subseteq \bigoplus_{k=1}^{p-3} H^1_\Sigma(F_p(-k))$$

which proves the final part of the proposition. \qed

### 3.5 Climbing The Ladder

One might ask if the inequality of Theorem 3.0.1 is ever an equality:

$$h^1_\Sigma(\text{Sym}^{p-4}V \otimes F_p(2)) = \sum_{k=1}^{p-3} h^1_\Sigma(F_p(-k)).$$

In Section 5.2, we show that this is true when $p = 5$. However, it is not true in general. In particular, see Section 5.3 for a detailed analysis of the possible cases when $p = 7$.

To summarize the results of Section 3 thus far: Given an extension $E/K$ of type $m$, we get a $G_{Q,S}$-representation of dimension $m+1$ whose image is isomorphic to the Galois group $\text{Gal}(M/Q)$ where $M$ is the Galois closure of $E/Q$. This gives a class in $H^1_\Sigma(\text{Sym}^{m-2}V \otimes F_p(1-m))$ whose image in the quotient $H^1_\Sigma(F_p(1-m))$ is nonzero.

Conversely, given a nonzero class $a_i$ in $H^1_\Sigma(F_p(-i))$, we want to determine if it lifts to an element in $H^1_\Sigma(\text{Sym}^{i-1}V \otimes F_p(-i))$, as such classes give representations of the form $(**)$ by Theorem 3.3.1 which correspond to extensions $E/K$ of type $i+1$.  

21
Equivalently, we want to extend the representation

$$\begin{pmatrix} \chi^{-i} & a_i \\ 1 & 1 \end{pmatrix}$$

to a representation of the form $\ast \ast$.

Lemma 3.3.2 tells us that $a_i$ lifts to a class in $H^1_S(V(-i)) = H^1_S(\text{Sym}^1 V \otimes F_p(-i))$, which is well-defined up to an element of $H^1_S(F_p(1-i))$. Choosing a particular lift gives rise to a 3-dimensional $G_{\mathbb{Q}, S}$-representation of the form

$$\begin{pmatrix} \chi^{1-i} & \chi^{-i}b & a_{i-1} \\ \chi^{-i} & a_i \\ 1 & 1 \end{pmatrix}$$

We want to know when we can extend one of these lifts to a 4-dimensional $G_{\mathbb{Q}, S}$-representation of the correct form, that is, whether or not one of these lifts actually lies in $H^1_S(V(-i)) \subseteq H^1_S(V(-i))$. This involves checking two independent conditions – that our given class can be made to satisfy the conditions of $\Sigma$ at $N$ and at $p$.

This is the beginning of an increasing sequence of obstruction problems. At each step $1 \leq k \leq i-1$, we have a class in $H^1_S(\text{Sym}^k V \otimes F_p(-i))$ defined up to an element of

$$H^1_S(F_p(k-i)) = \ker(H^1_S(\text{Sym}^k V \otimes F_p(-i)) \to H^1_S(\text{Sym}^{k-1} V \otimes F_p(-i))).$$

We want to know if this coset has nontrivial intersection with the $\Sigma$-Selmer subgroup so that the corresponding representation can be extended to one of dimension 1 larger. The top rung of this ladder is $H^1_S(\text{Sym}^{i+1} V \otimes F_p(-i))$, as classes in here lift directly to classes in $H^1_H(\text{Sym}^i V \otimes F_p(-i))$ corresponding to extensions $E/K$ of type $i+1$.

In general, the dimension of this kernel will be positive, so we have room to move as we attempt to solve these lifting problems. Given a particular lift of our class to $a \in H^1_S(\text{Sym}^i V \otimes F_p(-i))$, we can try to “fix” it at each of $N$ and $p$ by modifying it by an appropriate class $c \in H^1_S(F_p(k-i))$.

There are some cases in which this is always possible. To fix $a$ at $N$, we can modify $a$ by any element in

$$\frac{H^1_S(F_p(k-i))}{H^1_S(F_p(k-i))},$$

as the classes in $H^1_S(F_p(k-i))$ already have the correct behavior at $N$. Then to fix it at $p$ without changing it at $N$, we can modify $a$ by any element in

$$\frac{H^1_S(F_p(k-i))}{H^1_S(F_p(k-i))}.$$

This proves the following lemma.

**Lemma 3.5.1.** Assume that

$$h^1_S(F_p(k-i)) < h^1_S(F_p(k-i)) < h^1_S(F_p(k-i))$$

then we can lift our class $a$ one more step up the ladder in the sense of the above discussion.

As $p$ is assumed regular, this can only occur when $k-i$ is odd, $h^1_S(F_p(k-i)) = 0$, and $h^1_S(F_p(k-i)) = 1$.

It is worth remarking that in the special case of $i = 1$, there are no obstructions to worry about: The class $a_1 \in H^1_S(F_p(-1))$ lifts directly to a class in $H^1_H(\text{Sym}^1 V \otimes F_p(-1))$ which gives an extension $E/K$ of type 2. This is the method that Wake–Wang–Erickson to prove the lower bound in Theorem 3.0.1 as the following proposition.

**Proposition 3.5.2.** (*) Proposition 11.1.1. If $h^1_S(F_p(-1)) \neq 0$ then $r_K \geq 2$.

**Remark 3.5.3.** This question of extending representations is related to the vanishing of higher Massey products $(b, \ldots, b, a_i)$ in $G_{\mathbb{Q}, S}$-cohomology. In $\mathbb{Q}$, Sharifi has shown that certain higher Massey products of the type we are considering vanish in $G_{\mathbb{Q}}$-cohomology. One way of interpreting our results of Section 5.2 is in terms of the vanishing of certain triple Massey products in $G_{\mathbb{Q}, S}$-cohomology for $p = 5$. 

22
4 Effective Criteria for $H^1_{\Sigma}(\mathbb{F}_p(-i)) \neq 0$

Our goal in this section is to find an effective method for determining whether the various $H^1_{\Sigma}(\mathbb{F}_p(-i))$, $1 \leq i \leq p - 3$ are zero or not. The cases $i$ even and $i$ odd are treated separately. For each $i$, we relate the question of whether or not $H^1_{\Sigma}(\mathbb{F}_p(-i)) = 0$ to whether or not certain quantities in $\mathbb{F}_N^\times$ are $p$th powers. Throughout this section we assume that $p$ is regular. See Section 5.4 for a discussion of the case of irregular primes.

4.1 A Criterion for $H^1_{\Sigma}(\mathbb{F}_p(-i)) \neq 0$, $i$ Odd

Let $M = \frac{N-1}{p}$, and for any positive integer $i$ define

$$S_i = \prod_{k=1}^{p-1} ((Mk)!)^{k^i}.$$ 

**Theorem 4.1.1.** Assume that $p$ is regular. Let $i \neq -1 \mod p - 1$ be odd. Then $H^1_{\Sigma}(\mathbb{F}_p(-i)) \neq 0$ if and only if $S_i$ is a $p$th power in $\mathbb{F}_N^\times$.

See Section 5.4 for a discussion of the case of irregular $p$.

**Remark 4.1.2.** The proof of Theorem 4.1.1 will come down to producing a certain element of $\mathbb{Q}(\zeta_p)^\times$ satisfying some list of local conditions (see Lemma 4.1.4 for these conditions). The existence of such an element in a slightly different formulation is shown by Lecouturier in $[4]$. Lecouturier computes the image of this element in $\mathbb{Q}_N^\times/\mathbb{Q}_N^{xp}$ using the Gross-Koblitz formula and $N$-adic Gamma function, and the quantity $M_i = \prod_{k=1}^{N-1} \prod_{a=1}^{k^i} k^a$ arises as the image of this element in the factor $\mathbb{Z}_N^\times/\mathbb{Z}_N^{xp}$ of $\mathbb{Q}_N^\times/\mathbb{Q}_N^{xp}$. His results are not stated in terms of the Selmer groups $H^1_{\Sigma}(\mathbb{F}_p(-i))$; instead he relates the vanishing of $M_i$ directly to Imura’s filtration on the class group of $K(\zeta_p)$ in order to deduce bounds on the rank of the class group of $K$.

We include a proof of Theorem 4.1.1 that is better suited to our formulation using Selmer groups. The quantities $M_i$ of Lecouturier play the same role as the $S_i$ in our statement of Theorem 4.1.1; we show in Lemma 4.2.1 that $M_i = S_i^{-1}$ as elements of $\mathbb{F}_N^\times/\mathbb{F}_N^{xp}$.

**Remark 4.1.3.** One can compare the role of $S_i$ in Theorem 4.1.1 to the role of classical Bernoulli numbers in the theorems of Herbrand and Ribet on class groups of cyclotomic fields. The question of Bernoulli numbers being divisible by $p$ is replaced by the question of whether or not the invariants $S_i$ are $p$th powers. Similar to the fact that Bernoulli numbers $B_i$ for odd $i$ are all 0, the invariant $S_i$ for even $i$ is always a $p$th power, as the following computation in $\mathbb{F}_N^\times/\mathbb{F}_N^{xp}$ shows. If $i = 2j$ is even, then

$$S_{2j}^2 = \prod_{k=1}^{p-1} (((Mk)!)^{k^j})^{(M(p-k))!}^{(p-k)^{2j}}$$

$$= \prod_{k=1}^{p-1} ((Mk)!)(M(p-k))^{k^j}$$

$$= 1$$

where the last step follows from the fact that $a!(N-1-a)! \equiv \pm 1 \in \mathbb{F}_N^\times$ for any $a \neq 0$. Since $p$ is odd, the fact that $S_{2j}^2$ is a $p$th power means that $S_i$ itself must be a $p$th power.

For any prime $\lambda|N$ of $\mathbb{Q}(\zeta_p)$, define

$$\iota_\lambda : \mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p)_\lambda = \mathbb{Q}_N.$$ 

Note that if $\lambda' = [a]\lambda$ for $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, then

$$\iota_{\lambda'} = \iota_{[a]\lambda} = \iota_\lambda \circ [a^{-1}].$$

Fix a prime $\lambda|N$, and set $\iota = \iota_\lambda$, and $\iota_a = \iota_{[a]\lambda}$ for $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

The strategy for proving Theorem 4.1.1 is encompassed in the following lemma.
Lemma 4.1.4. Assume that \( p \) is regular. Let \( i \not\equiv -1 \mod p - 1 \) be odd. Suppose that there exists an element \( \mathcal{G}_{-i} \in \mathbb{Z}[[\zeta_p]] \) which satisfies the following properties:

(a) \( \mathcal{G}_{-i} \) lies in the \( \chi^{-i} \)-eigenspace of \( \mathbb{Q}(\zeta_p)^\times/\mathbb{Q}(\zeta_p)^{\times p} \);

(b) The ideal \( (\mathcal{G}_{-i}) \) of \( \mathbb{Z}[[\zeta_p]] \) is divisible only by prime ideals dividing \( N \).

(c) \( i(\mathcal{G}_{-i}) \) is not a \( p \)-th power in \( \mathbb{Q}_N^\times \).

Then \( H^1_{\Sigma}(\mathbb{F}_p(-i)) \) is non-zero if and only if \( i(\mathcal{G}_{-i}) \) and \( N \) generate the same subgroup of \( \mathbb{Q}_N^\times/\mathbb{Q}_N^{\times p} \).

Proof. Under the regularity assumption on \( p \), we know that \( H^1_{\Sigma}(\mathbb{F}_p(-i)) \) is one-dimensional, and contains \( H^1_{\Sigma}(\mathbb{F}_p(-i)) \). If \( c \not\equiv 0 \) is a class in \( H^1_{\Sigma}(\mathbb{F}_p(-i)) \), we want to determine whether or not \( c \) satisfies the condition at \( N \) to lie in \( H^1_{\Sigma}(\mathbb{F}_p(-i)) \). Such a class \( c \) defines an extension \( L/\mathbb{Q}(\zeta_p) \) which is Galois over \( \mathbb{Q} \) with Galois group \( \Gamma_{-i} \). The extension \( L/\mathbb{Q}(\zeta_p) \) is determined, through local class field theory, by the map which includes \( \chi \) in \( \psi \). This map necessarily factors through \( \mathbb{Q}(\zeta_p) \), by property (a), we have that the projection \( \psi : \mathbb{A}_p^\times \to \mathbb{F}_p \)

which factors through the \( \chi^{-i} \) eigenspace of the \( p \)-coinvariants of the quotient

\[ \mathbb{Q}(\zeta_p)^\times/\mathbb{A}_p^{\times} \]

where \( U \) is the subgroup

\[ U = \prod_{\lambda \mid N} (1 + \lambda \mathcal{O}_{\mathbb{Q}(\zeta_p)_\lambda}) \times \prod_{q \mid N} \mathcal{O}^\times_{\mathbb{Q}(\zeta_p)_q} \times (\mathbb{Q}(\zeta_p) \otimes \mathbb{R})^\times. \]

Identifying \( \mathbb{Q}(\zeta_p)_\lambda \) with \( \mathbb{Q}_N \), we have that the ramified extension of \( \mathbb{Q}_N \) given by localizing \( L \) at a prime above \( \lambda \) is determined, through local class field theory, by the map which includes \( \mathbb{Q}_N \) as \( \mathbb{Q}(\zeta_p)_\lambda \) composed with \( \psi \),

\[ \psi_N : \mathbb{Q}_N^\times \to \mathbb{A}^\times_{\mathbb{Q}(\zeta_p)} \to \mathbb{F}_p. \]

This map necessarily factors through \( \mathbb{Q}_N^\times/\mathbb{Q}_N^{\times p} \) (which is 2-dimensional as an \( \mathbb{F}_p \)-vector space), and the (1-dimensional) kernel of this map is the norm subgroup of the corresponding extension of \( \mathbb{Q}_N \) coming from \( L \). In particular this extension is \( K_N \) if and only if \( N \) is in the kernel of \( \psi_N \).

Suppose that we are given an element \( \mathcal{G}_{-i} \in \mathbb{Z}[[\zeta_p]] \) that satisfies properties (a), (b), (c) as in the statement of the lemma. We claim that \( i(\mathcal{G}_{-i}) \) is a generator of the kernel of \( \psi_N : \mathbb{Q}_N^\times/\mathbb{Q}_N^{\times p} \to \mathbb{F}_p \). Clearly by property (c) \( i(\mathcal{G}_{-i}) \) does indeed generate a 1-dimensional subspace of \( \mathbb{Q}_N^\times/\mathbb{Q}_N^{\times p} \). Let \( C \) be the \( \chi^{-i} \)-eigenspace of the \( p \)-coinvariants of \( \mathbb{A}_p^{\times} \). We show that, in \( C \), the inclusion of \( i(\mathcal{G}_{-i}) \) in the \( \lambda \) coordinate is equal to the diagonal inclusion of the globally-defined \( \mathcal{G}_{-i} \) in the ideles. Thus, since the diagonal inclusion of \( \mathcal{G}_{-i} \) is certainly in the kernel of \( \psi \), we have that \( i(\mathcal{G}_{-i}) \) is in the kernel of \( \psi_N \). Since \( \mathcal{G}_{-i} \) is a unit at all primes not above \( N \) by property (b), it suffices to work only in the factors of the ideles corresponding to primes above \( N \). By property (a), we have that the projection \( P_{\chi^{-i}} \) to the \( \chi^{-i} \)-eigenspace fixes the diagonal embedding of \( \mathcal{G}_{-i} \), i.e.

\[ P_{\chi^{-i}}((\psi(\mathcal{G}_{-i}), 1, \ldots, 1)) = (\psi(\mathcal{G}_{-i}), \mathbb{Z}/p\mathbb{Z}) \times \]

in \( C \). On the other hand, the image of \( i(\mathcal{G}_{-i}) \) in \( C \) is

\[ P_{\chi^{-i}}((\psi(\mathcal{G}_{-i}), 1, \ldots, 1)) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi^{-i}(a^{-1}) [\psi(\mathcal{G}_{-i}), 1, \ldots, 1] \]

\[ = (\chi^{-i}(a^{-1}) \psi(\mathcal{G}_{-i}), \mathbb{Z}/p\mathbb{Z}) \times \]

\[ = (\psi(\mathcal{G}_{-i}^{-1}(a^{-1})), \mathbb{Z}/p\mathbb{Z}) \times \]

\[ = (\psi(\mathcal{G}_{-i}^{-1}(a^{-1})), \mathbb{Z}/p\mathbb{Z}) \times \]
\[ \mu(a) = (\iota_a(G_{-i}))_{a \in \mathbb{Z}/p\mathbb{Z}}. \]

Therefore since \( \iota(G_{-i}) \) is in the kernel of \( \psi_N \) and is non-zero, we conclude that it generates this kernel and hence \( H^1_k(F_p(-i)) = H^1_k(F_p(-i)) \) if and only if \( \iota(G_{-i}) \) generates the same subgroup of \( \mathbb{Q}_N^\times /\mathbb{Q}_N^{\times, p} \) as \( N \). 

To prove Theorem 4.1.1 it suffices to produce an element \( G_{-i} \) which satisfies the conditions of Lemma 4.1.4. We will show in Lemma 4.1.6 that the image of \( G_{-i} \) under \( \iota \) is equal to \( N^u S_i^{-1} \) as an element of \( \mathbb{Q}_N^\times /\mathbb{Q}_N^{\times, p} \) for some \( u \neq 0 \mod p \), hence \( \iota(G_{-i}) \) will generate the same subgroup as \( N \) if and only if \( S_i \) is trivial in \( \mathbb{Q}_N^\times /\mathbb{Q}_N^{\times, p} \), as \( S_i \) is an \( N \)-adic unit. Determining whether or not \( S_i \) is a \( p \)th power can be done in \( \mathbb{F}_N^\times \), and Theorem 4.1.1 follows.

Let \( A = \mathbb{Q}(\zeta_p, \zeta_N) \) and let \( B = \mathbb{Q}(\zeta_p, \zeta_N) \). For any character \( \eta \)

\[ \eta : \text{Gal}(B/\mathbb{Q}(\zeta_p)) \cong (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mu_p \]

of order \( p \), define the Gauss sum

\[ g_\eta = \sum_{k=1}^{N-1} \eta(k) \zeta_N^k. \]

Let \( \lambda \) be the prime above \( \lambda \) in \( A \), and \( \mathcal{L} \) the prime above \( \ell \) in \( B \) (so we have \( \mathcal{L}^{N-1} = \mathcal{P} = \lambda \)). The Gauss sums \( g_\eta \) satisfy the following properties

- \( g_\eta \) is an element of the ring of integers of \( A \), and is divisible only by primes above \( N \).
- Since \( \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \) acts on \( \mathcal{O}_A \), we have that for \( a \in (\mathbb{Z}/p\mathbb{Z})^\times \)

\[ [a]g_\eta = g_{\eta^a}. \]

- If \( [b] \in \text{Gal}(B/\mathbb{Q}(\zeta_p)) = (\mathbb{Z}/N\mathbb{Z})^\times \), then

\[ [b]g_\eta = \eta(b^{-1})g_\eta. \]

- \( g_\eta^p \in \mathbb{Q}(\zeta_p). \)

Fix the choice of \( \eta \) so that the composite map

\[ (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\eta} \mu_p \rightarrow (\mathbb{Z}/[\mu_p]/\lambda)^\times = (\mathbb{Z}/N\mathbb{Z})^\times \]

is the map \( k \mapsto k^{-N^{-1}/p} \), and let \( \tau : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{Z} \setminus \{0\} \) be a set map which satisfies that the composite

\[ (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\tau} \mathbb{Z} \setminus \{0\} \rightarrow (\mathbb{Z}/p^2\mathbb{Z})^\times \]

is the map \( x \mapsto x^p \). In particular, \( \tau(xy) \equiv \tau(x)\tau(y) \mod p^2 \). Define

\[ G_{-i} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} ([a]g_\eta)^{\tau(a^i)} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} (g_{\eta^a})^{\tau(a^i)}. \]

To establish the desired properties of the element of \( G_{-i} \), we will need to examine the expansion of \( \iota(G_{-i}) \) in terms of the uniformizer of \( \mathbb{Q}(\zeta_p)_\lambda = \mathbb{Q}_N \), and to do this we will need to examine the expansion of a Gauss sum in terms of a uniformizer. This latter expansion is computed in the following lemma.

**Lemma 4.1.5.** Let \( 1 \leq r < p \), \( M = (N-1)/p \), and \( m = rM \). Let \( I : B \rightarrow B_\mathcal{L} = \mathbb{Q}_N(\zeta_N) \) be the embedding extending \( I \). Note that \( \pi = 1 - \zeta_N \) is a uniformizer in \( \mathbb{Q}_N(\zeta_N) \). We have that

\[ I(g_{\eta^r}) = (-1)^{m+1} \frac{\pi^m}{m!} + O(\pi^{m+1}). \]
Proof. By definition, we have that

\[
I(g_\eta^r) = \sum_{k=1}^{N-1} \eta(k)^r (1 - \pi)^k
\]

\[
= \sum_{k=1}^{N-1} \eta(k)^r - \pi \sum_{k=1}^{N-1} \binom{k}{1} \eta(k)^r + \pi^2 \sum_{k=2}^{N-1} \binom{k}{2} \eta(k)^r - \ldots + \pi^{N-1}
\]

\[
= \sum_{j=0}^{N-1} (-1)^j \pi^j \sum_{k=j}^{N-1} \binom{k}{j} \sum_{k=1}^{N-1} \eta(k)^r
\]

where we take \(\binom{k}{j} = 0\) when \(k < j\). If we expand the binomial coefficients as polynomials in \(k\), each term in this last sum will be of the form

\[
(-1)^j \pi^j \sum_{k=j}^{N-1} \binom{k}{j} \eta(k)^r
\]

for some \(l < j\) and integer \(a\). Note that

\[
\pi^m \sum_{k=j}^{N-1} \binom{k}{j} \eta(k)^r = \begin{cases} O(\pi^{N-1}) & j \neq m \\ -1 + O(\pi^{N-1}) & j = m \end{cases}
\]

since \(\lambda = \mathcal{L}^{N-1}\) and we have that

\[
\sum_{k=1}^{N-1} k^l \eta(k)^r = \sum_{k=1}^{N-1} k^l \mod \lambda
\]

using that \(\eta^r\) is the map \(k \mapsto k^{-m}\) modulo \(\lambda\).

Therefore every term in the sum for \(I(g_\eta^r)\) will be \(O(\pi^{N-1})\) until the first term involving \(\sum_{k=1}^{N-1} k^m \eta(k)^r\).

This term is

\[
(-1)^m \pi^m \frac{1}{m!} \sum_{k=1}^{N-1} k^m \eta(k)^r
\]

All other terms in the sum are \(O(\pi^{m+1})\), so we conclude that

\[
I(g_\eta^r) = (-1)^m \pi^m \frac{1}{m!} + O(\pi^{m+1}).
\]

Lemma 4.1.6. The element \(G_{-i}\) is in \(\mathbb{Q}(\zeta_p)^\times\), and satisfies properties (a), (b), and (c) of Lemma 4.1.4. Furthermore, as elements of \(\mathbb{Q}_N^\times/\mathbb{Q}_N^{\times p}\), we have

\[
\iota(G_{-i}) = N^u S_i^{-1}
\]

for some \(u \equiv 0 \mod p\).

Proof. For \(b \in \text{Gal}(B/\mathbb{Q}(\zeta_p)) = (\mathbb{Z}/NP)^\times\), we have working mod \(p\)th powers that

\[
[b]G_{-i} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} [b](g_{\eta^a})^{\tau(a^i)}
\]

\[
= \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} (\eta^a (b^{-1})g_{\eta^a})^{\tau(a^i)}
\]

\[
= G_{-i} \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \eta^{a^{-1} + 1} (b^{-1})
\]

26
where we have used that \( \tau(a^i) \equiv a^i \mod p \) and that \( \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} a^{i+1} \equiv 0 \mod p \) when \( i \neq -1 \mod p - 1 \). This establishes that \( G_{-i} \in \mathbb{Z}[\mathbb{Z}_p] \). Along with the properties of the Gauss sums \( g_\eta \), we conclude that \( G_{-i} \) is only divisible by the primes above \( N \), which is to say it satisfies property (b) of Lemma \ref{lemma:11.4}

To show that it satisfies property (a), we recall that \( \tau \) is a \( \eta \)-adic unit. Using Lemma \ref{lemma:4.15}, we can write

\[
\left( \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} a^i \right)^{\tau(a^i)} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left( \left[ a \right] \left[ a \right] \right)^{\tau(a^i)}
\]

where all equalities are taken to be in \( \mathbb{Q}(\zeta_p)^\times/\mathbb{Q}(\zeta_p)^{xp} \). Note that we have used that \( g_\eta^p \in \mathbb{Q}(\zeta_p)^\times \), so \( g_\eta^{xp} \in \mathbb{Q}(\zeta_p)^{xp} \) which means we can work mod \( p^2 \) in the exponent.

Once we show that \( i(G_{-i}) = N^u S_i^{-1} \) in \( \mathbb{Q}_N^\times/\mathbb{Q}_N^{xp} \) for some \( u \neq 0 \mod p \) it will follow that \( G_{-i} \) is not a \( p \)-th power in \( \mathbb{Q}_N^\times \), which was property (c) of Lemma \ref{lemma:11.4} as \( S_i \) is a \( N \)-adic unit.

Using Lemma \ref{lemma:4.13} we can write

\[
i(G_{-i}) = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} I(g_\eta^a)^{\tau(a^i)}
\]

\[
= \prod_{r=1}^{p-1} \left( \frac{(-1)^{rM+1}}{(rM)!} \right)^{\tau(r^i)} + O(\pi)
\]

\[
= \prod_{r=1}^{p-1} \left( \frac{(-1)^{rM+1}}{(rM)!} \right)^{\tau(r^i)} + O(\pi) \pi \sum_{r=1}^{p-1} rM \tau(r^i)
\]

in \( \mathbb{Q}_N(\zeta_N)^\times \). Notice that the first term in this product lies in \( \mathbb{Q}_N^\times \) and is equal to \( S_i^{-1} \) in \( \mathbb{Q}_N^\times/\mathbb{Q}_N^{xp} \).

To understand the final term, we first write

\[
\frac{\pi^{N-1}}{N} = \frac{1}{N} (1 - \zeta_N)^{N-1}
\]

\[
= \frac{1}{N} \text{Norm}_{\mathbb{Q}_N}^{\mathbb{Q}_N(\zeta_N)} (1 - \zeta_N) \prod_{i=1}^{N-1} \frac{1 - \zeta_i^i}{1 - \zeta_N}
\]

\[
= \prod_{i=1}^{N-1} (1 + \zeta_N + \cdots + \zeta_N^{i-1})
\]

\[
= \prod_{i=1}^{N-1} i \mod \pi
\]

\[
= -1 \mod \pi
\]

as \( \mathbb{Z}_N[\zeta_N]/(\pi) = \mathbb{F}_N \). Thus \( \pi^{N-1} = N(-1 + O(\pi)) \) and we can use this to write

\[
\pi \sum_{r=1}^{p-1} rM \tau(r^i) = \pi(N-1) \frac{1}{2} \sum_{r=1}^{p-1} r \tau(r^i)
\]
\[\pm N^{\frac{1}{p}} \sum_{r=1}^{p-1} r\tau(r') \left(1 + O(\pi)\right).\]

Working modulo \(p\) in the exponent, we can substitute \(\frac{1}{p} \sum_{r=1}^{p-1} r\tau(r')\) with \(\frac{1}{p} \sum_{r=1}^{p-1} r\chi(r')\). This is just the generalized Bernoulli number \(B_{1,\chi}\), which is a \(p\)-adic unit as \(p\) is regular.

Combining the previous calculations, we have now shown that in \(\mathbb{Q}^\times_N/\mathbb{Q}^\times_N\),

\[\iota(G_{-i}) = S^{-1}_i N^u w\]

where \(u \not\equiv 0 \mod p\), and where \(w\) is a unit in \(\mathbb{Z}_N\) that, considered as an element of \(\mathbb{Z}_N[\zeta_N]\), is congruent to 1 modulo \(\pi\). The isomorphism \(\mathbb{Z}_N[\zeta_N]/(\pi) = \mathbb{Z}_N/(N)\) tells us that \(w \equiv 1 \mod N\) and is thus a \(p\)th power in \(\mathbb{Q}_N^\times\). Thus

\[\iota(G_{-i}) = N^u S^{-1}_i\]

in \(\mathbb{Q}_N^\times/\mathbb{Q}_N^{\times p}\), as desired.

### 4.2 Relationship with Lecouturier’s Results

We begin by showing that \(S_i\) is a \(p\)th power in \(\mathbb{F}_N^\times\) if and only if Lecouturier’s \(M_i\) is.

**Lemma 4.2.1.** As elements of \(\mathbb{F}_N^\times/\mathbb{F}_N^{\times p}\), \(S^{-1}_i = M_i\). 

**Proof.** All equalities in this proof take place in \(\mathbb{F}_N^\times/\mathbb{F}_N^{\times p}\). In Lemma 4.3 of [4], Lecouturier proves that

\[M_i = \prod_{k=1}^{p-1} \Gamma_N(k/p)^{k^i}\]

Using that \(\frac{k}{p} \equiv M(p - k) + 1 \mod N\), the Gamma functions can be replaced by factorials

\[M_i = \prod_{k=1}^{p-1} \left(\left(M(p - k)\right)!\right)^{k^i}\]

\[= \prod_{k=1}^{p-1} \left(\left(Mk\right)!\right)^{-k^i}\]

\[= S^{-1}_i\]

where the second step follows by changing variables from \(k\) to \(p - k\) and discarding \(p\)-th powers.

Recall the definition of Lecouturier’s \(\mu\), the number of odd \(1 \leq i \leq p - 4\) for which \(M_i\) (equivalently, \(S_i\)) is not a \(p\)th power in \(\mathbb{F}_N^\times\). Combining this with our results in Section 3, we get the following corollary, which establishes Theorem 1.2.1 for regular \(p\).

**Corollary 4.2.2.** Assume \(p\) is regular. Then

\[r_K \leq 1 + \sum_{i=1}^{p-3} h_{\Sigma}(F_p(-i)) \leq p - 2 - 2\mu.\]

**Proof.** The first inequality is Theorem 3.0.1. There are \(p - 3\) terms in the sum, each of which is 0 or 1 by Part 6 of Theorem 2.3.1. This gives \(r_K \leq p - 2\).

For any odd \(i\), Theorem 4.1.1 gives that if \(S_i\) is not a \(p\)th power mod \(N\), \(h_{\Sigma}(F_p(-i)) = 0\). As this also implies \(h_{\Sigma}(F_p(1 + i)) = 0\) by Corollary 2.3.3, we conclude that two terms of the above sum must be 0. Putting this together for all \(i\), we get the desired bound.
4.3 Relationships with Known Criteria for \( H_{\Sigma}^1(F_p(-i)) \neq 0 \)

Theorem 4.1.1 establishes that \( H_{\Sigma}^1(F_p(-i)) \) is non-zero if and only if \( S_i \) is a \( p \)-th power, for regular \( p \) and odd \( i \neq -1 \mod p - 1 \). A similar relationship was known to Wake–Wang-Erickson in the case \( i \equiv 1 \mod p - 1 \); see Theorem 12.5.1 of [10].

However, these results are not stated in terms of \( S_1 \), but rather in terms of Merel’s number

\[
C = \prod_{k=1}^{(N-1)/2} k^b.
\]

Theorem 1.3, (ii) of [1] states that if \( r_K = 1 \) then \( C \) is not a \( p \)-th power mod \( N \). Similarly, Proposition 3.5.2 and Theorem 4.1.1 together imply that if \( r_K = 1 \) then \( S_1 \) is not a \( p \)-th power mod \( N \). Thus one might expect that the quantities \( C \) and \( S_1 \) can be related in \( F^\times_N / F^\times_p \). The goal of this section is to prove this statement; to do so we will introduce another family of quantities related to both \( C \) and the \( S_i \).

Let

\[
A_m = \prod_{k=1}^{N-1} k^{bm}.
\]

In Proposition 1.2 of [4], Lecouturier proves that \( C = A_{-3/4} \) in \( F^\times_N / F^\times_p \).

To relate the \( A_m \) to the \( S_i \) we will use the \( N \)-adic Gamma function, the relevant properties of which are:

- \( \Gamma_N : \mathbb{Z}_N \to \mathbb{Z}^\times_N \) is a continuous function, constructed by extending the function
  \[
  \Gamma_N(x) = (-1)^x \prod_{0 < j < x, j \not| N} j
  \]
  defined for positive integers \( x \) by continuity to all of \( \mathbb{Z}_N \).

- For an integer \( 0 < x < N \), we have \( \Gamma_N(x) = (-1)^x (x - 1)! \).

- If \( x \equiv y \mod N \), then \( \Gamma_N(x) \equiv \Gamma_N(y) \) mod \( N \).

- If \( x + r \) is not divisible by \( N \) for \( 0 \leq r \leq M - 1 \) where \( M = \frac{N-1}{p} \), then
  \[
  \prod_{r=0}^{M-1} (x + r) = (-1)^M \frac{\Gamma_N(M + x)}{\Gamma_N(x)}.
  \]

**Theorem 4.3.1.** Suppose that \( 0 < m < p - 1 \). Then

\[
A_m = \prod_{j=1}^{m-1} S_j^{\binom{m}{j}} \text{ in } F^\times_N / F^\times_p.
\]

**Proof.** All equalities in this proof are in \( F^\times_N / F^\times_p \). We start by reindexing the product in the definition of \( A_m \)

\[
A_m = \prod_{k=1}^{p-1} \prod_{r=0}^{M-1} (k + pr)^{(k+pr)m}.
\]

After removing \( p \)-th powers from the exponent and factoring out a \( p \)-th power of \( p \) we have that

\[
A_m = \prod_{k=1}^{p-1} \prod_{r=0}^{M-1} \left( \frac{k}{p} + r \right)^{km}
\]
\[
= \prod_{k=1}^{p-1} \left( (-1)^M \frac{\Gamma_N(M + k/p)}{\Gamma_N(k/p)} \right)^{km}
\]

where the second step follows from the last listed property of the \(N\)-adic Gamma function. Aligning terms using by a “telescoping series” argument gives that

\[
A_m = \prod_{k=1}^{p-1} \Gamma_N(k/p)^{(k+1)m - km}.
\]

Using that \(k \equiv M(p - k) + 1 \mod N\), the Gamma functions can be replaced by factorials

\[
A_m = \prod_{k=1}^{p-1} ((M(p - k)!)^{(k+1)m - km}
\]

where the second step follows by changing variables from \(k\) to \(p - k\). Simplifying the exponent and combining terms appropriately into the \(S_i\), this yields that

\[
A_m = \prod_{j=0}^{m-1} S_j^{-(m)}.
\]

Note that this theorem implies that

\[
A_2 = S_1^{-2} \text{ in } \mathbb{F}_N^\times / \mathbb{F}_N^{\times p}
\]

so combining this with the relationship between \(C\) and \(A_2\), we see that one of \(C, A_2, S_1,\) and \(M_1\) is a \(p\)th power \(\text{mod } N\) if and only if all of them are.

Theorem 4.3.1 also shows that the \(S_i\) can be recovered from the \(A_m\), at least as elements of \(\mathbb{F}_N^\times / \mathbb{F}_N^{\times p}\), using inductively that \(S_1 = A_2^2\) and that

\[
S_i = \left( A_{i+1} \prod_{j=1}^{i-1} S_j^{-(i+j)} \right)^{i+1}
\]

for all \(i\).

4.4 A Criterion for \(H_1^\Sigma(\mathbb{F}_p(-i)) \neq 0, i \text{ even}\)

We wish to find invariants that will let us compute whether or not \(H_1^\Sigma(\mathbb{F}_p(-i))\) is trivial for even \(i \neq 0 \text{ mod } p - 1\).

**Proposition 4.4.1.** Let \(p\) be regular, and \(i\) even. We have that \(H_1^\Sigma(\mathbb{F}_p(-i))\) is non-trivial if and only if \(H_1^\Sigma(\mathbb{F}_p(1 + i))\) is non-trivial and \(H_1^p(\mathbb{F}_p(1 + i)) \subseteq H_1^\Sigma(\mathbb{F}_p(1 + i))\).

**Proof.** We see by Theorems 2.3.1 and 2.3.2 that \(H_1^\Sigma(\mathbb{F}_p(-i))\) is non-trivial if and only if \(H_1^\Sigma(\mathbb{F}_p(1 + i))\) is 2-dimensional and thus equal to \(H_1^\Sigma(\mathbb{F}_p(1 + i))\). Since \(H_1^\Sigma(\mathbb{F}_p(1 + i))\) is spanned by its \(H_1^N\) and \(H_1^p\) subspaces, this second condition happens if only if both \(H_1^N(\mathbb{F}_p(1 + i)) = H_1^\Sigma(\mathbb{F}_p(1 + i))\) and \(H_1^p(\mathbb{F}_p(1 + i)) \subseteq H_1^\Sigma(\mathbb{F}_p(1 + i))\). \(\square\)
Since we know how to test for \( H^1_{\Sigma}(\mathbf{F}_p(1+i)) \) being non-trivial, we simply need to find a way of testing whether or not \( H^1_{\Sigma}(\mathbf{F}_p(1+i)) \subseteq H^1_{\Sigma}(\mathbf{F}_p(1+i)) \).

The class in \( H^1_{\Sigma}(\mathbf{F}_p(1+i)) \) is unramified at \( N \), so it will land in \( H^1_{\Sigma}(\mathbf{F}_p(1+i)) \) if and only if it is split at \( N \). We may think of such a class as being given by a Kummer generator over \( \mathbb{Q}(\zeta_p) \), which will necessarily be a unit locally at primes not equal to \( p \). Thus it suffices to find this generator, and then use that the class is split at \( N \) if and only if the Kummer generator is a \( p \)-th power mod \( N \). Note that such a generator is independent of \( N \). Such a Kummer generator is a choice of non-zero element in

\[
\left( \frac{\mathbb{Z}[\zeta_p, p^{-1}]}{\mathbb{Z}[\zeta_p, p^{-1} \times p]} \right)^{\chi^{-i}}.
\]

Note that given such an element, all of its Galois conjugates are also Kummer generators of the same extension.

The minimal polynomials of such elements can be computed using a computer algebra system. We did this using SageMath [8] for \( p = 5 \) and \( p = 7 \).

**Theorem 4.4.2.** We have:

1. Suppose \( p = 5 \). Then \( H^1_{\Sigma}(\mathbf{F}_p(2)) \) is non-zero if and only both \( S_1 \) and the roots of \( x^2 + x - 1 \) are 5th powers in \( \mathbb{F}_N^\times \).

2. Suppose \( p = 7 \). Then
   
   (a) \( H^1_{\Sigma}(\mathbf{F}_p(2)) \) is non-zero if and only both \( S_3 \) and the roots of \( x^3 + 41x^2 + 54x + 1 \) are 7th powers in \( \mathbb{F}_N^\times \).
   
   (b) \( H^1_{\Sigma}(\mathbf{F}_p(4)) \) is non-zero if and only if both \( S_1 \) and the roots of \( x^3 - 25x^2 + 31x + 1 \) are 7th powers in \( \mathbb{F}_N^\times \).

**Remark 4.4.3.** The polynomials in the theorem above are not unique. One could use any other polynomial whose roots generate the same 1-dimensional subspace of

\[
\left( \frac{\mathbb{Z}[\zeta_p, p^{-1}]}{\mathbb{Z}[\zeta_p, p^{-1} \times p]} \right)^{\chi^{-i}}.
\]

### 5 Specific Primes

We now apply the results of Section 3 to the specific cases \( p = 3, 5, \) and \( 7 \). For \( p = 3 \) the situation is quite straightforward, as the results of Section 3 imply that \( r_K = 1 \). For \( p = 5 \) we show that the inequality of Theorem 3.0.1 is always an equality, which then determines \( r_K \) solely in terms of the dimensions \( h^1_{\Sigma}(\mathbf{F}_p(-1)) \) and \( h^1_{\Sigma}(\mathbf{F}_p(-2)) \). A similar argument applied to the case \( p = 7 \) proves the converse to Theorem 1.2.2.

Throughout this section we will often use without reference the results of Section 2.3 on the dimensions of various Selmer subgroups of \( H^1_{\Sigma}(\mathbf{F}_p(-1)) \).

#### 5.1 \( p = 3 \)

If \( p = 3 \), Theorem 4.5 of [2] implies that \( r_K = 1 \). In other words, if \( N \equiv 1 \mod 3 \), the only degree 3 unramified extension of \( K = \mathbb{Q}(N^{1/3}) \) is the genus field.

The results of Section 3.1 recover this result in the following way. Lemmas 3.1.11 and 3.1.12 imply that the type \( m \) of any unramified extension \( E/K \) must satisfy \( m \leq p - 2 = 1 \). Lemma 3.1.9 shows that the only extension of type 1 is the genus field \( K(\zeta_N^p) \). This proves the following theorem.

**Theorem 5.1.1.** Let \( p = 3 \). Then \( r_K = 1 \).
5.2 $p = 5$

In the case $p = 5$, we prove the following refined version of Theorem 3.0.1

**Theorem 5.2.1.** Let $p = 5$. Then $r_K = 1 + h^1_2(F_p(-1)) + h^1_2(F_p(-2))$.

Combining this theorem with the results of Section 4 proves Theorem 1.2.3

**Proof of Theorem 1.2.3** Since each $h^1_2(F_p(-i))$ is at most 1, we obtain the bound $r_K \leq 3$. We know that $r_K$ is $\geq 2$ if and only if $S_1 = \prod_{k=1}^{p-1}((Mk)!)$ is a 5th power in $F_N^\times$, as Theorem 4.1.1 proves that $h^1_2(F_p(-1)) = 1$ if and only if $S_1$ is a 5th power, and further, $r_K = 3$ if and only if $h^1_2(F_p(-1)) = h^1_2(F_p(-2)) = 1$, which by Theorems 4.1.1 and 4.4.2 happens if and only if both $S_1$ and $\sqrt{\frac{S_1}{2}}$ are 5th powers. $\blacksquare$

See Appendix A.1 for data on how often each of the three possible cases $r_K = 1$, 2, or 3 occurs.

For the rest of Section 5.2 we assume that

$$h^1_2(F_p(-2)) = 1$$

as we know by Corollary 3.5.2 and Theorem 3.0.1 that

$$1 + h^1_2(F_p(-1)) \leq r_K \leq 1 + h^1_2(F_p(-1)) + h^1_2(F_p(-2)).$$

We already know by Theorem 3.0.1 that $r_K = 1 + h^1_2(V(-2))$. The content of Theorem 5.2.1 is thus that we can compute $h^1_2(V(-2))$ simply with the dimensions of Selmer groups of one dimensional representations. This statement about dimensions will follow from showing that the following sequence (see the proof of Proposition 3.4.1 in Section 3.4) is short exact:

$$0 \to H^1_2(F_p(-1)) \to H^1_2(V(-2)) \to H^1_2(F_p(-2)).$$

To rephrase slightly, what we want to establish is that every class in $H^1_2(F_p(-2))$ lifts not only to a class in $H^1_2(V(-2))$, but to a class in the subspace $H^1_2(V(-2))$.

**Lemma 5.2.2.** A class $a_2 \in H^1_2(F_p(-2))$ lifts to $H^1_2(V(-2))$ if and only if it lifts to $H^1_2.(V(-2))$

**Proof.** One direction is clear, as $H^1_2(V(-2)) \subseteq H^1_2(V(-2))$. Since $h^1_2(F_p(-1)) = 2$ and $h^1_2(F_p(-1)) = 1$ in the present situation, any lift of $a_2$ to $H^1_2.(V(-2))$ may be modified so that it is split at $p$ without changing it locally at $N$, i.e. any such lift may be translated to one which is in $H^1_2(V(-2))$. $\blacksquare$

Theorem 5.2.1 will be proven if we show that $H^1_2(V(-2)) = H^1_2.(V(-2))$. This is the statement of Theorem 5.2.1, the proof of which occupies the remainder of this section.

We will prove Theorem 5.2.1 with the use of a new representation of $G_{Q,S}$, which we introduce now. Let $a_2$ denote the class that spans $H^1_2(F_p(-2))$. Choose a lift $a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \in H^1_2(V(-2))$. The extension $L$ of $Q$ defined by $a$ has Galois group isomorphic to the image of the $G_{Q,S}$-representation

$$\begin{pmatrix} \chi^{-1} & \chi^{-2}a_1 \\ 0 & \chi^{-2} \\ 0 & 0 & 1 \end{pmatrix}.$$  \(\dagger\)

Consider the contragredient of this representation twisted by the character $\chi^{-1}$; in a choice of basis to make it upper-triangular this new $G_{Q,S}$-representation has the form

$$\begin{pmatrix} \chi^{-1} & a_2b - a_1 \\ 0 & \chi \\ 0 & 0 & 1 \end{pmatrix}.$$  \(\dagger\)

This representation has image again isomorphic to the Galois group of $L$ over $Q$, as taking duals and twisting by $\chi^{-1}$ will not change the kernel of this representation, which is $G_L$. 32
We define $W$ to be the 2-dimensional $\mathbb{F}_p$-vector space where $G_{\mathbb{Q}, S}$ acts by
\[
\begin{pmatrix}
\chi^{-2} & a_2 \\
0 & 1
\end{pmatrix}.
\]
Thus the two 3-dimensional $G_{\mathbb{Q}, S}$-representations (†) and (‡) of the preceding paragraph yield cohomology classes
\[
\left[\begin{array}{c}
a_1 \\
a_2
\end{array}\right] \in H^1_S(V(2)), \left[\begin{array}{c}
a_2 b - a_1 \\
-b
\end{array}\right] \in H^1_S(W(1)).
\]

**Remark 5.2.3.** Consider the diagram of fields

$$
\begin{array}{ccc}
L & \rightarrow & L_2 \\
\downarrow & & \downarrow \\
K(\zeta_p) & \rightarrow & L_2 \\
\downarrow & & \downarrow \\
\mathbb{Q}(\zeta_p) & \rightarrow & \mathbb{Q}
\end{array}
$$

where $L_2$ is the field defined by the class $a_2$, which is Galois over $\mathbb{Q}$ with Galois group $\Gamma_{-2}$, the semi-direct product $\mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$ with action given by $\chi^{-2}$.

The representation (†) above is found by considering the action of $\text{Gal}(K(\zeta_p)/\mathbb{Q})$ on $\text{Gal}(L/K(\zeta_p)) \cong V(2)$, and the representation (‡) is found by considering the action of $\text{Gal}(L_2/\mathbb{Q})$ on $\text{Gal}(L_2/\mathbb{Q}) \cong W(1)$.

We now relate the local properties of the cohomology classes $\left[\begin{array}{c}
a_1 \\
a_2
\end{array}\right]$ and $\left[\begin{array}{c}
b a_2 - a_1 \\
-b
\end{array}\right]$.

**Lemma 5.2.4.** The class $a = \left[\begin{array}{c}
a_1 \\
a_2
\end{array}\right] \in H^1_S(V(2))$ is in $H^1_{\Sigma^*}(V(2))$ if and only if the class $a' = \left[\begin{array}{c}
a_2 b - a_1 \\
-b
\end{array}\right] \in H^1_S(W(1))$ is in $H^1_{\Sigma^*}(W(1))$.

**Proof.** Noting that $a_2$ is necessarily a non-zero multiple of $b$ locally at $N$ by Remark 2.3.6, we see that $W(1)$ and $V(2)$ are isomorphic representations locally at $N$. In particular the results of Section 2.2 still apply to the twists of $W$.

In the case of both $V(2)$ and $W(1)$, the $\Sigma^*$ condition is just that classes vanish when restricted to $K_N$. Interpreting this in terms of the Galois extension $L/\mathbb{Q}$ cut out by both $a$ and $a'$, we see that either class satisfies the $\Sigma^*$ condition if and only if $N$ is split in $L/L_2 K(\zeta_p)$, as we know that locally at $N$ the extension $L_2 K(\zeta_p)$ is $K_N$.

We will prove that $H^1_{\Sigma^*}(W(1)) = H^1_S(W(1))$, hence the equivalent statements of the previous lemma always hold. Note that $W(1)^* = W(-2)$.

**Lemma 5.2.5.** The classes generating $H^1_S(W(1))$ and $H^1_S(W(-2))$ are as follows.

1. The dimension of $H^1_S(W(1))$ is bounded by $3 \leq h^1_S(W(1)) \leq 4$. The classes $\left[\begin{array}{c}
a \\
b
\end{array}\right]$ for $a \in H^1_S(\mathbb{F}_p(-1))$ always span a 3-dimensional subspace. Let $b'$ be the class of $p$ in $H^1_S(\mathbb{F}_p(1))$. The dimension $h^1_S(W(-2))$ is equal to 4 if and only if $p$ is a $p$th power mod $N$, in which case the final dimension is spanned by some lift of $b'$, $\left[\begin{array}{c}
* \\
b'
\end{array}\right]$. 

33
2. \( H^1_S(W(-2)) \) is 3-dimensional, and is spanned by the classes

\[
\begin{bmatrix} a \\ 0 \\ a_2^2/2 \\ a_2 \end{bmatrix}.
\]

Proof. For \( a \in H^1_S(F_p) \). For the first part of this lemma, consider the following piece of the long exact sequence in \( G_{Q,S} \)-cohomology:

\[
0 \to H^1_S(F_p(-1)) \to H^1_S(W(1)) \to H^1_S(F_p(1)) \xrightarrow{a_2^2/2} H^2_S(F_p(-1)).
\]

The 2 dimensions of \( H^1_S(F_p(-1)) \) give classes in \( H^1_S(W(1)) \) immediately. The classes \( b, b' \), which span \( H^1_S(F_p(1)) \) lift to \( H^1_S(W(1)) \) if and only if \( a_2 \) vanishes.

For the class \( b \), we know that \( a_2 \cup b = 0 \) by Proposition 2.3.5 as \( a_2 \in H^1_S(F_p(-2)) \). Since \( a_2 = b \) when viewed as a class for \( G_{Q,N} \), we have that \( a_2 \cup b' = 0 \) if and only if \( b' \) is a multiple of \( b \) locally at \( N \), again by Proposition 2.3.5. As \( b' \) is unramified at \( N \), the only way for it to be a multiple of \( b \) locally at \( N \) if \( N \) is split in the extension defined by \( b' \), which is \( Q(p^{1/p}) \). \( N \) splits in this extension if and only if \( p \) is a \( p \)th power in \( Q_N^\times \), which happens if and only if \( p \) is a \( p \)th power in \( F_N^\times \). Thus the class \( b' \) lifts to \( H^1_S(W(1)) \) if and only if \( p \) is a \( p \)th power mod \( N \).

The proof for the second part of the lemma is similar, using the long exact sequence for \( W(-2) \):

\[
0 \to H^1_S(F_p) \to H^1_S(W(-2)) \to H^1_S(F_p(-2)) \xrightarrow{a_2^2/2} H^2_S(F_p).
\]

Note that in this case the boundary map \( a_2 \cup - \) vanishes because \( a_2 \) spans \( H^1_S(F_p(-2)) \), and \( a_2 \) certainly cups to 0 with itself. \( \square \)

**Lemma 5.2.6.** \( H^1_S(W(1)) = H^1_S(W(1)) \).

Proof. Applying Theorem 2.1.2 to \( H^1_S(W(1)) \) produces the relation:

\[
h^1_S(W(1)) = 2 + h^1_S(W(-2)),
\]

where we have used that \( W \cong V \) as \( G_{Q,N} \)-representations so Proposition 2.2.2 applies to the twists of \( W \).

We determine \( h^1_S(W(-2)) \) explicitly based on our knowledge of the classes of \( H^1_S(W(-2)) \). Let \( c, c' \) be the classes spanning \( H^1_S(F_p) \), which correspond respectively to \( Q(\zeta^{(p)}_N) \) and \( Q(\zeta^{(p)}_{p^2}) \).

- the class \( \begin{bmatrix} a_2^2/2 \\ a_2 \end{bmatrix} \) is always in \( H^1_S(W(-2)) \), since \( a_2 \) itself is in \( H^1_S(F_p(-2)) \).
- the class \( \begin{bmatrix} c' \\ 0 \end{bmatrix} \) is never in \( H^1_S(W(-2)) \) as it is ramified at \( p \).
- the class \( \begin{bmatrix} c \\ 0 \end{bmatrix} \) is in \( H^1_S(W(-2)) \) if and only if \( p \) is split in \( Q(\zeta^{(p)}_N) \), which happens if and only if \( p \) is a \( p \)th power mod \( N \), since \( \text{Gal}(Q(\zeta^{(p)}_N)/Q) \) is canonically \( (\mathbb{Z}/N\mathbb{Z})^\times / (\mathbb{Z}/N\mathbb{Z})^{\times p} \).

Putting this description together with the previous lemma we have that:

\[
p \text{ a \( p \)th power mod } N \implies h^1_S(W(-2)) = 2 \text{ and } h^1_S(W(1)) = 4
\]

\[
\implies h^1_S(W(1)) = 2 + 2 = 4 = h^1_S(W(1))
\]

\[
p \text{ not a \( p \)th power mod } N \implies h^1_S(W(-2)) = 1 \text{ and } h^1_S(W(1)) = 3
\]

\[
\implies h^1_S(W(1)) = 1 + 2 = 3 = h^1_S(W(1)).
\]

Thus in all cases we have \( h^1_S(W(1)) = h^1_S(W(1)) \); since \( h^1_S(W(1)) \subseteq H^1_S(W(1)) \) we conclude that these groups are equal. \( \square \)

The necessary information is now in place to prove the following theorem, promised earlier in this section.
Theorem 5.2.7. \( H^1_S(V(-2)) = H^1_S(V(-2)) \).

Proof. The classes spanning \( H^1_S(V(-2)) \) are

\[
\begin{bmatrix} a \\ \emptyset \\ a_1 \\ a_2 \end{bmatrix}
\]

for \( a \in H^1_S(F_p(-1)) \). The standing assumption of this section is that \( H^1_S(F_p(-2)) \neq 0 \), which forces \( H^1_S(F_p(-1)) = H^1_S(F_p(-1)) \). Combining Lemma 5.2.4 and Lemma 5.2.6 shows that \( \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \) is always in \( H^1_S(V(-2)) \). This proves that \( H^1_S(V(-2)) \supseteq H^1_S(V(-2)) \), which proves equality as the other containment is immediate.

Remark 5.2.8. The result of Theorem 5.2.7 holds in more generality than just the case \( p = 5 \) with our assumptions on \( H^1_S(F_p(-2)) \). In general for any regular \( p \) note that \( F_p(\mathbb{Z}_p^{-1}/2) \) and \( F_p(\mathbb{Z}_p^+2) \) are dual Galois modules, and the character \( \chi^{(p-1)/2} \) is its own inverse. The general statement is that for these characters that are the dual pair in the “middle” of the possible range of powers of \( \chi \), it holds that

\[
H^1_S(F_p(\mathbb{Z}_p^{-1}/2)) \neq 0 \implies H^1_S(V(\mathbb{Z}_p^+2)) = H^1_S(V(\mathbb{Z}_p^{-1}/2)).
\]

5.3 \( p = 7 \)

When \( p = 7 \) it is not the case that \( r_K \) can be determined completely by the dimensions \( h^1_S(F_p(-i)) \). Note that when \( p = 7 \) the possible groups \( H^1_S(F_p(-i)) \) that may arise are those for \( i \in \{-1, -2, -3, -4\} \). When discussing the possible cases we will indicate the dimensions of these \( H^1_S(F_p(-i)) \) by a binary string of length 4; so for example 1000 is used to indicate \( h^1_S(F_p(-1)) = 1 \) and all others 0.

Theorem 5.3.1. Let \( p = 7 \). Then \( r_K \geq 2 \) if and only if at least one of \( H^1_S(F_p(-1)) \) or \( H^1_S(F_p(-3)) \) is non-zero.

Proof. Corollary 2.3.3 and Proposition 3.4.1 combine to show the only if direction, that \( r_K \geq 2 \) implies that one of \( H^1_S(F_p(-1)) \) and \( H^1_S(F_p(-3)) \) is non-zero.

We also have established in Proposition 3.5.1 that \( h^1_S(F_p(-1)) = 1 \implies r_K \geq 2 \). Thus it remains to show that when \( h^1_S(F_p(-3)) = 1 \) and \( h^1_S(F_p(-1)) = 0 \), we still have that \( r_K \geq 2 \). There are two possible cases.

Case 1: the dimensions of the \( H^1_S(F_p(-i)) \) are 0010. In this case the same argument as employed for \( p = 5 \) (Theorem 5.2.7) see Remark 5.2.8 shows that the class in \( H^1_S(F_p(-3)) \) always has a lift to \( H^1_S(V(-3)) \). The one dimension of \( H^1_S(F_p(-2)) \), which is by assumption not split at \( p \), can be used to modify this lift so that it is in \( H^1_S(V(-3)) \), as in Section 3.5. This class in \( H^1_S(V(-3)) \) then lifts to a class in \( H^1_S(Sym^2V \otimes F_p(-3)) \) by Lemma 3.5.1.

Case 2: the dimensions are 0110. In this case the class in \( H^1_S(F_p(-2)) \) always has a lift to \( H^1_S(V(-2)) \) by Lemma 3.5.1.

Theorem 1.2.4 follows by combining this result and Theorem 4.1.1 the dimensions \( h^1_S(F_p(-1)) \) and \( h^1_S(F_p(-3)) \) are non-zero if and only if, respectively, \( S_1 \) and \( S_3 \) are \( p \)th powers in \( F_N^\times \).

Note that not all binary strings of length 4 arise as dimensions of the \( H^1_S(F_p(-i)) \); Corollary 2.3.3 implies that only 9 out of 16 possible binary strings of length 4 may arise, and in fact each of these 9 possibilities do occur. For a given binary string of dimensions, Theorem 3.0.1 gives a list of at most four possible ranks which can occur given those dimensions of the \( H^1_S(F_p(-1)) \). Apart from the cases \( r_K = 1 \) and the \( h^1_S(F_p(-i)) \) are 0010 or 0110 which are ruled out in Theorem 5.3.1 all such possibilities do actually occur. For data on the distribution of \( N \) among the possible cases of the \( h^1_S(F_p(-i)) \) and \( r_K \), see Appendix 3.2.

Note that in the cases 1011, 1110, and 1111, there is potentially some ambiguity as to which classes \( a_i \in H^1_S(F_p(-i)) \) are contributing to \( r_K \). It does not appear to the authors that the methods of this article can address this ambiguity in general. For example, when the dimensions are 1011 and the rank is 3 it could be the case that either the class in \( H^1_S(F_p(-3)) \) or \( H^1_S(F_p(-4)) \) is contributing to the rank (the \( H^1_S(F_p(-1)) \) class always contributes to the rank, as does the genus field).

35
There is another level of ambiguity that our methods do not seem capable of handling. If a class \( a_i \in H_1^N(F_p(-i)) \) does not contribute to \( r_K \), it must be because \( a_i \) fails to lift from \( a \in H_1^N(Sym^k V \otimes F_p(-i)) \) to \( a' \in H_1^N(Sym^{k+1} V \otimes F_p(-i)) \) for some \( k \). We know that the class \( a \in H_1^N(Sym^k V \otimes F_p(-i)) \) always has a lift to \( a'' \in H_3^N(Sym^{k+1} V \otimes F_p(-i)) \) (well-defined up to addition of classes in \( H_3^N(F_p(k+1-i)) \)), as this lifting up one dimension only requires that \( a \) satisfy the \( \Sigma \) condition locally at \( N \). These classes \( a'' \) may fail to satisfy the local conditions of \( \Sigma \) in a number of ways. It could be the case that

1. no lift \( a' \) is split at \( p \),
2. no lift \( a' \) vanishes when restricted to \( K_N \),
3. there are lifts that satisfy the local condition at \( p \) or at \( N \), but no lift satisfies both local conditions simultaneously.

In general when a class \( a_i \) fails to contribute to \( r_K \) we cannot determine for which \( k \) the lifting of representations fails, and if it is failing at \( p \), \( N \), or both. In some cases, an analysis of the local behaviour of the classes in \( H_3^N(F_p(k+1-i)) \) can be done to show that a class fails to lift for a specific reason. We collect here several examples of cases where a specific type of failure can be shown to occur. In each of the following examples, a non-zero class \( a_3 \in H_1^N(F_p(-3)) \) is shown to have a specific type of failure. Note that by the Remark 5.2.8 the class \( a_3 \) always lifts to a class in \( H_1^N(V(-3)) \).

**Example 5.3.1.** Suppose that the dimensions are 0110 and the rank is 2. The proof of Theorem 5.3.1 showed that the class in \( H_1^N(F_p(-2)) \) always contributed to the class group, so the class \( a_3 \in H_1^N(F_p(-3)) \) must be failing to lift to \( H^3_1(Sym^2 V \otimes F_p(-3)) \). By Lemma 5.3.1 any lift to \( H_3^N(Sym^2 V \otimes F_p(-3)) \) can be modified to satisfy the Selmer condition \( \Sigma \), so it must be the case that \( a_3 \) does not even lift \( H_1^N(V(-3)) \). Since \( a_3 \) lifts to \( H_1^N(V(-3)) \) it must be the case that all such lifts are ramified at \( p \), meaning that a failure occurs at \( p \).

**Example 5.3.2.** Consider the case where the dimensions are 1011 and the rank is 2. As in the proof of Theorem 5.3.1, \( a_3 \) lifts to \( H_1^N(V(-3)) \) and then \( H_3^N(Sym^2 V \otimes F_p(-3)) \). Every class we can use to modify such a lift vanishes when restricted to \( K_N \), but there is a class in \( H_2^N(F_p(-1)) \) which is ramified at \( p \), so can be used to modify a lift so that it is split at \( p \), without changing it locally at \( N \). Since none of these lifts are contributing to the class group (the rank 2 comes from the non-zero class in \( H_2^N(F_p(-1)) \)), it must be the case that they do not vanish when restricted to \( K_N \), so they cannot extend one step further.

**Example 5.3.3.** Suppose that the dimensions are 1011 and the rank is 2. Again, \( a_3 \) lifts to \( H_1^N(V(-3)) \) and then \( H_3^N(Sym^2 V \otimes F_p(-3)) \). In this case the local behaviour of such a lift can then be corrected at \( p \) or at \( N \) individually using the 1 dimension of \( H_2^N(F_p(-1))/H_2^N(F_p(-1)) \), but since a failure is occurring it must be the case that no lift satisfies the local conditions at \( p \) and \( N \) simultaneously.

### 5.4 Irregular \( p \)

The methods of Sections 3 and 4 can still be used to obtain bounds on \( r_K \) in the case that \( p \) is irregular, but some of the statements of the results in those sections need to be altered to account for the irregularity. In this section, we discuss some of these alterations and the proofs of Theorems 1.2.1 and 1.3.1 in the irregular case.

Recall that the bound \( r_K \leq r_{Q(\zeta_p))} + p - 2 - \mu \) is a theorem of Lecouturier [4].

When \( p \) is not regular, the computations of Theorem 2.3.1 change. One particular difference we have is that now, when \( 1 \leq i \leq p - 4 \) is odd, one can deduce using Theorem 2.1.2 twice that

\[
\begin{align*}
\hat{h}_N(F_p(-i)) &= 1 + h_{N,1}(F_p(1+i)) \\
&\leq 1 + h_{p,1}(F_p(1+i)) \\
&= 1 + h_{p,1}(F_p(-i)) \\
&\leq 1 + h_{1}(F_p(1-i)) \\
&= 1 + r_{Q(\zeta_p)}^N
\end{align*}
\]
where \( r_{Q(\zeta_p)}^{\chi^{-i}} \) is the \( p \)-rank of the \( \chi^{-i} \)-eigenspace of \( \text{Cl}_{Q(\zeta_p)} \). This argument produces the same bound for even \( 2 \leq i \leq p - 3 \), though via a slightly different sequence of inequalities.

Similarly, Theorem 2.3.4 fails in general, as \( h^2(G_{Q,S}, F_p(i)) \) can be strictly larger than 1 in the absence of regularity. This propagates into Section 3.3, where the full statements of Lemmas 3.3.2 and 3.3.3 need not hold.

The issues arise from the fact that the vanishing of global cup products (which are needed to guarantee that certain representations extend to representations of larger dimension) can’t be checked locally anymore. However, the vanishing of a global cup product does guarantee the vanishing of the local cup product. Thus Lemma 3.3.4 still holds and Lemma 3.3.2 should be replaced by

**Lemma.** For any \( i \leq p - 3 \), 0 \( \leq j \leq i \), the image of \( H^1(Sym^j V \otimes F_p(-i)) \) in \( H^1(Sym^{j-1} V \otimes F_p(-i)) \) is contained in \( H^1(Sym^{j-1} V \otimes F_p(-i)) \).

Fortunately, this is still enough to conclude that Proposition 3.4.1 holds, as the full statements of Lemma 3.3.2 and Lemma 3.3.3 are only needed for the discussion in Section 3.5. This retrieves Theorem 3.0.1 and the statement that \( r_K \geq 2 \) implies at least one \( h^1(F_p(-i)) \neq 0 \) in the case that \( p \) is irregular.

We also note that Proposition 3.5.2 is still true when \( p \) is irregular. That is, we still have \( 1 + h^1(F_p(-1)) \leq r_K \). Even for irregular \( p \), it is still true that \( h^2(G_{Q,S}, F_p) = 1 \), so Lemmas 3.3.2 and 3.3.4 still hold.

Combining this discussion with the bound \( h^1_X(F_p(-i)) \leq 1 + r_{Q(\zeta_p)}^{\chi^{-i}} \), we conclude

\[
 r_K \leq 1 + \sum_{i=1}^{p-3} h^1(Y(F_p(-i)) \leq 1 + \sum_{i=1}^{p-3} h^1_X(F_p(-i)) \leq 1 + \sum_{i=1}^{p-3} (1 + r_{Q(\zeta_p)}^{\chi^{-i}}) = r_{Q(\zeta_p)} + p - 2.
\]

Suppose now that for some odd \( 1 \leq i \leq p - 4 \), \( M_i \) (equivalently, \( S_i \)) is not a \( p \)-th power mod \( N \). As \( p \) is not regular, this can’t be used to conclude that \( H^1_Y(F_p(-i)) = 0 \). However, the argument of Lemma 4.1.4 applies to show that the extension of \( Q(\zeta_p) \) defined by \( G_{-i} \) (via class field theory) gives a cohomology class that lies in \( H^1_X(F_p(-i)) \) but not \( H^1_Y(F_p(-i)) \). Thus, in this case, one has

\[
 h^1_Y(F_p(-i)) \leq h^1_X(F_p(-i)) - 1.
\]

Combining this for all odd \( i \), one sees

\[
 1 + \sum_{i=1}^{p-3} h^1_Y(F_p(-i)) \leq r_{Q(\zeta_p)} + p - 2 - \mu.
\]

### Appendix A Data for \( p = 5, 7 \)

All computations in this section were performed using PARI/GP \[7\] and SageMath \[8\]. Note that the computation of ranks of class groups when \( p = 7 \) used PARI/GP’s algorithms for computing class groups of number fields, which assume the GRH to optimize computation. Thus the ranks computed when \( p = 7 \) in all cases other than 0000, 1000, and 0010 are conditional on GRH.

#### A.1 \( p = 5 \)

For primes \( N \equiv 1 \mod 5 \), \( N \leq 20,000,000 \) we computed the dimensions \( h^1_Y(F_p(-1)) \) and \( h^1_Y(F_p(-2)) \) using the results of Section 4. For each \( N \) there are three possible sets of dimensions: both are 0, \( h^1_Y(F_p(-1)) = 1 \) and \( h^1_Y(F_p(-2)) = 0 \), and both are 1; as in Section 5.3 these are notated by a binary string of length 2 (00,
10, and 11). Note that by Theorem 5.2.1 the dimensions \( h_1^\Sigma(F_p(-i)) \) completely determine the rank \( r_K \). There are 317,587 such primes \( N \), and their distribution among the three possible cases is given in Table 1 below.

| Dimensions | \( r_K \) | Number of \( N \) |
|------------|----------|------------------|
| 00         | 1        | 253,234          |
| 10         | 2        | 51,613           |
| 11         | 3        | 12,740           |
| Total      |          | 317,587          |

Table 1: Data for \( p = 5 \).

From this we see that 20.26\% of \( N \) in this range have \( r_K \geq 2 \), and of those \( N \), 19.80\% of \( N \) have \( r_K \geq 3 \). We expect that the quantities \( M_1 \) and \( \sqrt{\frac{5}{2}} - 1 \) should be “uniformly distributed” in \( \mathbb{Z}/5\mathbb{Z} \cong F_5^N/F_5^N \), meaning that they are 5th powers for a set of primes of density \( \frac{1}{5} \) in the primes \( N \equiv 1 \text{ mod } 5 \). This would imply that \( r_K \geq 2 \) for \( \frac{1}{5} \) of primes and that \( r_K = 3 \) for \( \frac{1}{25} \) of primes \( N \equiv 1 \text{ mod } 5 \), which is suggested by the data.

**A.2 \( p = 7 \)**

For primes \( N \equiv 1 \text{ mod } 7 \), \( N \leq 100,000,000 \), we computed the dimensions \( h_1^\Sigma(F_p(-i)) \) for \( i = 1, 2, 3, 4 \) using the results of Section 4. There are 960,023 such primes \( N \), and their distribution among the possible cases is given in Table 2 below.

| Dimensions | Number of \( N \) |
|------------|------------------|
| 0000       | 705,575          |
| 1000       | 99,649           |
| 0010       | 101,126          |
| 1010       | 15,057           |
| 1001       | 16,610           |
| 0110       | 16,580           |
| 1011       | 2,249            |
| 1110       | 2,546            |
| 1111       | 631              |
| Total      | 960,023          |

Table 2: Dimensions of the \( H_1^\Sigma(F_p(-i)) \), \( p = 7 \) and \( N \leq 100,000,000 \).

For primes \( N \equiv 1 \text{ mod } 7 \) and \( N \leq 20,000,000 \), we computed the rank \( r_K \) (which is not determined completely by the \( h_1^\Sigma(F_p(-i)) \) in this case). There are 211,766 such primes \( N \), and their distribution between possible ranks \( 1 \leq r_K \leq 5 \) and dimensions \( h_1^\Sigma(F_p(-i)) \) are given in Table 3 below. The empty cells in Table 3 are cases that are shown to never occur in Section 5.3 in particular every possible case does actually occur.

Similar to the case \( p = 5 \), one might expect that \( H_1^\Sigma(F_p(-1)) \) and \( H_1^\Sigma(F_p(-3)) \) are each non-zero for \( \frac{1}{7} \) of primes \( N \equiv 1 \text{ mod } 7 \). Indeed, the data supports this guess, with 14.24\% of the \( N \) tested having \( H_1^\Sigma(F_p(-1)) \) non-zero, and 14.39\% of the \( N \) tested having \( H_1^\Sigma(F_p(-3)) \) non-zero.

One might also expect that \( \frac{1}{7} \) of primes with \( H_1^\Sigma(F_p(-1)) \) non-zero have \( H_1^\Sigma(F_p(-4)) \) non-zero, as this just rests on whether or not the roots of a fixed polynomial are 7th powers mod \( N \); this holds for 14.25\% of the \( N \) tested. Similarly \( H_1^\Sigma(F_p(-2)) \) is non-zero for 14.30\% of the primes tested for which \( H_1^\Sigma(F_p(-3)) \) is non-zero.
| Dimensions | \#r\_K = 1 | \#r\_K = 2 | \#r\_K = 3 | \#r\_K = 4 | \#r\_K = 5 | Total |
|------------|-------------|-------------|-------------|-------------|-------------|-------|
| 0000       | 155,691     |             |             |             |             | 155,691|
| 1000       |             | 21,975      |             |             |             | 21,975|
| 0010       |             | 22,201      |             |             |             | 22,201|
| 1010       |             | 2,925       | 478         |             |             | 3,403|
| 1001       |             | 3,110       | 487         |             |             | 3,597|
| 0110       |             | 3,133       | 499         |             |             | 3,632|
| 1011       |             | 444         | 50          | 10          |             | 504   |
| 1110       |             | 407         | 170         | 2           |             | 579   |
| 1111       |             | 130         | 46          | 6           | 2           | 184   |
| Total      | 155,691     | 54,325      | 1,730       | 18          |             | 211,766|

Table 3: Ranks r\_K and dimensions of the H^{1}_{\Sigma}(F\_p(-i)), p = 7 and N \leq 20,000,000.

References

[1] Frank Calegari and Matthew Emerton. “On the ramification of Hecke algebras at Eisenstein primes”. In: Invent. Math. 160.1 (2005), pp. 97–144. ISSN: 0020-9910. URL: https://doi.org/10.1007/s00222-004-0406-z

[2] Frank Gerth III. “On 3-class groups of pure cubic fields”. In: J. Reine Angew. Math. 278/279 (1975), pp. 52–62. ISSN: 0075-4102. URL: https://doi.org/10.1515/crll.1975.278-279.52

[3] Kiyoaki Imura. “On the l-rank of ideal class groups of certain number fields”. In: Acta Arith. 47.2 (1986), pp. 153–166. ISSN: 0065-1036. URL: https://doi.org/10.4064/aa-47-2-153-166

[4] Emmanuel Lecouturier. “On the Galois structure of the class group of certain Kummer extensions”. In: Journal of the London Mathematical Society 0.0 (). DOI: 10.1112/jlms.12123 eprint: https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/jlms.12123 URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms.12123

[5] Loïc Merel. “L’accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de J_0(p)”. In: J. Reine Angew. Math. 477 (1996), pp. 71–115. ISSN: 0075-4102. URL: https://doi.org/10.1515/crll.1996.477.71

[6] J.S. Milne. Arithmetic Duality Theorems. Second. BookSurge, LLC, 2006, pp. viii+339. ISBN: 1-4196-4274-X.

[7] PARI/GP version 2.7.5. available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2015.

[8] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 7.5.1). http://www.sagemath.org 2017.

[9] Romyar T. Sharifi. “Massey products and ideal class groups”. In: J. Reine Angew. Math. 603 (2007), pp. 1–33. ISSN: 0075-4102. URL: https://doi.org/10.1515/CRELLE.2007.010

[10] Preston Wake and Carl Wang-Erickson. “The Rank of Mazur’s Eisenstein Ideal”. Preprint available at http://arxiv.org/abs/1707.01894

[11] Lawrence C. Washington. “Galois Cohomology”. In: Modular Forms and Fermat’s Last Theorem. Ed. by Gary Cornell, Joseph H. Silverman, and Glenn Stevens. Springer-Verlag, 1997. Chap. IV.