CLASS GROUPS OF KUMMER EXTENSIONS VIA CUP PRODUCTS IN GALOIS COHOMOLOGY

KARL SCHAEFER AND ERIC STUBLEY

Abstract. We use Galois cohomology to study the p-rank of the class group of $\mathbf{Q}(N^{1/p})$, where $N \equiv 1 \bmod p$ 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 $\mathbf{Q}(N^{1/5})$ in terms of whether or not $\prod_{k=1}^{(N-1)/2} k^k$ and $\frac{\sqrt{5}-1}{2}$ are 5th powers mod N.

Contents

2010 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R34.

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

1. Introduction

Let N and $p \geq 3$ be prime numbers with $p|(N-1)$. Fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ and a choice of $N^{1/p} \in \overline{\mathbf{Q}}$, and let K denote the field $\mathbf{Q}(N^{1/p})$. The goal of this article is to study the class group Cl_K of K, and in particular its p-rank $r_K = \dim_{\mathbf{F}_p}(\mathrm{Cl}_K \otimes \mathbf{F}_p)$. We access r_K by class field theory, as r_K is equal to the maximal r such that K admits an unramified-everywhere $(\mathbf{Z}/p\mathbf{Z})^r$-extension. By genus theory, $r_K \geq 1$, since the degree-p subfield of $K(\zeta_N)/K$ is unramified everywhere; this is a corollary of Lemma 2.2.4. Our starting point is the following theorem of Calegari–Emerton.

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

This theorem is proven using deformation theory of Galois representations. Previous work of Merel [7] showed that whether or not the number C is a pth power determines whether the $\mathbf{Z}_p$-rank of a certain Hecke algebra is at least 2. Calegari–Emerton identify this Hecke algebra with a deformation space of Galois representations, and construct an unramified $\mathbf{F}_p$-extension of K in the case that the deformation space has $\mathbf{Z}_p$-rank at least 2. More recently, this theorem was given another proof by Wake–Wang-Erickson (see Proposition 11.1.1 of [12], restated in this article as Proposition 4.0.1) using cup products in Galois cohomology.

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 [6] that the converse fails in the case $p = 7$, $N = 337$.

1.1. 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 [6], and let $r_{\mathbf{Q}(\zeta_p)}$ be the p-rank of $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}$. Let χ be the mod-p cyclotomic character and say that $(p, -i)$ is a regular pair if the χ^{-i}-eigenspace of $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}$ is trivial.

Lecouturier proves that

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

where μ is the number of odd i such that $1 \leq i \leq p-4$, $(p, -i)$ is a regular pair, and M_i is not a pth power in $\mathbf{F}_N^\times$.

Using a new method, we improve the previous bound on r_K:

Theorem 1.1.1.

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

This follows from the stronger inequality of Theorem 1.2.1 combined with Theorems 1.2.2 and 1.2.3. An immediate corollary of Theorem 1.1.1 in the case of regular p is the following partial converse to the theorem of Calegari–Emerton:

Theorem 1.1.2. *Suppose that p is regular, and that $r_K \geq 2$. Then at least one of the M_i is a pth power in $\mathbf{F}_N^\times$.*

Proof. If $r_K \geq 2$, then the inequality of Theorem 1.1.1 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 pth power in $\mathbf{F}_N^\times$. □

The quantity M_1 is a pth power in $\mathbf{F}_N^\times$ if and only if $C = \prod_{k=1}^{(N-1)/2} k^k$ is (see Section 5.2 for this comparison).

When $p = 5$, Theorem 1.1.2 is the full converse to the theorem of Calegari–Emerton, as the only M_i is M_1. Furthermore, we give in Section 6.2 an effective method for completely determining r_K in this case:

Theorem 1.1.3. *Let $p = 5$. 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 5th power in $\mathbf{F}_N^\times$.*
(2) *$r_K = 3$ if and only if both M_1 and $\frac{\sqrt{5}-1}{2}$ are 5th powers in $\mathbf{F}_N^\times$.*

The converse to Theorem 1.1.2 is not true in general: in the case $p = 11$, $N = 353$ one has that both $r_K = 1$ and M_3 is an 11th power in $\mathbf{F}_{353}^\times$. However, the converse to Theorem 1.1.2 is true in the case $p = 7$, which we prove in Section 6.3:

Theorem 1.1.4. *Let $p = 7$. Then $r_K \geq 2$ if and only if one of M_1 or M_3 is a 7th power in $\mathbf{F}_N^\times$.*

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 7th power in $\mathbf{F}_{337}^\times$, but M_3 is.

1.2. Strategy.

Put $S = \{p, N, \infty\}$ and let $G_{\mathbf{Q},S}$ be the Galois group over $\mathbf{Q}$ of the maximal extension of $\mathbf{Q}$ unramified outside of S.

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 pth power in $\mathbf{F}_N^\times$ 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 $G_{\mathbf{Q},S} \to \mathrm{GL}_3(\mathbf{F}_p)$, from which an unramified $\mathbf{F}_p$-extension of K is constructed.

Let $\mathbf{F}_p(i)$ denote the module $\mathbf{F}_p$ on which $G_{\mathbf{Q},S}$ acts by χ^i. Choose an isomorphism $\mu_p \to \mathbf{F}_p(1)$ and let $b : G_{\mathbf{Q},S} \to \mathbf{F}_p(1)$ be the cocycle defined by $b(\sigma) = \sigma(N^{1/p})/N^{1/p}$. Let $V \cong \mathbf{F}_p^2$ be the vector space on which $G_{\mathbf{Q},S}$ acts by the representation

$$\begin{aligned} G_{\mathbf{Q},S} &\to \mathrm{GL}_2(\mathbf{F}_p) \\ \sigma &\mapsto \begin{pmatrix} \chi(\sigma) & b(\sigma) \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

In an abuse of notation, we will also use b to refer to the class of this cocycle in $H^1(G_{\mathbf{Q},S}, \mathbf{F}_p(1))$, which is just the Kummer class of N. Starting with an unramified $\mathbf{F}_p$-extension of K, we use the classification of indecomposable $\mathbf{F}_p$-representations of $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q}) \cong \mathbf{Z}/p\mathbf{Z} \rtimes (\mathbf{Z}/p\mathbf{Z})^\times$ to show the existence of an upper-triangular

Galois representation $G_{\mathbf{Q},S} \to \mathrm{GL}_{m+2}(\mathbf{F}_p)$ of the form

$$\left(\begin{array}{c|c} \mathrm{Sym}^m V \otimes \mathbf{F}_p(-m) & * \\ \hline & 1 \end{array}\right) = \left(\begin{array}{ccccc|c} 1 & \chi^{-1}b & \chi^{-2}\frac{b^2}{2} & \cdots & \chi^{-m}\frac{b^m}{m!} & * \\ & \chi^{-1} & \chi^{-2}b & \cdots & \chi^{-m}\frac{b^{m-1}}{(m-1)!} & * \\ & & \chi^{-2} & & \vdots & \vdots \\ & & & \ddots & \chi^{-m}b & * \\ & & & & \chi^{-m} & * \\ \hline & & & & & 1 \end{array}\right).$$

Note that this symmetric power is written using a slightly non-standard basis, see Remark 3.1.8 for an explanation as to why we use this basis.

The representations arising in this fashion give rise to classes in the $G_{\mathbf{Q},S}$-cohomology of the high-dimensional Galois representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(i)$. We study the local properties of these cohomology classes and show that they satisfy a Selmer condition Σ, first considered by Wake–Wang-Erickson for the Galois module $\mathbf{F}_p(-1)$ (see Section 2.2 for the definition of Σ in general). This Selmer condition Σ is chosen to detect exactly 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 1.2.1. *Let $h^1_\Sigma(\mathbf{F}_p(-i))$ denote the $\mathbf{F}_p$-dimension of $H^1_\Sigma(\mathbf{F}_p(-i))$. We have*

$$1 + h^1_\Sigma(\mathbf{F}_p(-1)) \le r_K \le 1 + \sum_{i=1}^{p-3} h^1_\Sigma(\mathbf{F}_p(-i)).$$

Section 3 is dedicated to the proof of this theorem. Note that this theorem has as a corollary the statement that if $r_K \ge 2$, then at least one of the $H^1_\Sigma(\mathbf{F}_p(-i))$ is nonzero. By a computation using Gauss sums, we relate the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ to the quantities M_i introduced earlier.

Theorem 1.2.2. *Assume that i is odd and $(p, -i)$ is a regular pair. Then we have $h^1_\Sigma(\mathbf{F}_p(-i)) = 1$ if and only if M_i is a pth power in $\mathbf{F}_N^\times$, and $h^1_\Sigma(\mathbf{F}_p(-i)) = 0$ otherwise.*

The proof of this theorem can be found in Sections 5.1 and 5.2.

While not needed to establish Theorem 1.1.1, in order to prove Theorem 1.1.3 we need to find a computable criterion for determining when $h^1_\Sigma(\mathbf{F}_p(-i)) = 1$ for even i. This is done for $(p, 1+i)$ a regular pair in Section 5.3.

Finally, to establish Theorem 1.1.1, we need the following theorem, which comes from duality theorems in Galois cohomology.

Theorem 1.2.3. *For any $1 \le i \le p-3$*

$$h^1_\Sigma(\mathbf{F}_p(-i)) \le 1 + r^{\chi^{-i}}_{\mathbf{Q}(\zeta_p)},$$

where $r^{\chi^{-i}}_{\mathbf{Q}(\zeta_p)}$ is the p-rank of the χ^{-i}-eigenspace of $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}$.

Furthermore, if p is odd and $h^1_\Sigma(\mathbf{F}_p(-i)) = 0$, then $h^1_\Sigma(\mathbf{F}_p(-(p-2-i))) = h^1_\Sigma(\mathbf{F}_p(1+i)) = 0$ as well.

This theorem is a combination of Theorem 2.3.4 and Corollary 2.3.7.

The outline of this article is as follows. In Section 2, we recall some facts about Selmer groups, define the Selmer condition Σ, and prove several lemmas about the relationship between the condition Σ and the vanishing of cup products. In Section 3, we relate the p-part of Cl_K to Selmer groups of higher-dimensional representations of $G_{\mathbf{Q},S}$ and prove Theorem 1.2.1. In Section 4, we prove results about when classes in $H^1_\Sigma(\mathbf{F}_p(-i))$ can be lifted to classes in the Σ-Selmer group of the higher-dimensional representations arising in Section 3. In Section 5, 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_{1-i} and another quantity arising from the units of the cyclotomic field $\mathbf{Q}(\zeta_p)$. Finally, in Section 6, we analyze the cases $p = 5$ and $p = 7$ in more detail. Appendix A contains computer calculations of r_K and the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ 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.

1.3. **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. We also thank the anonymous referee for their suggestions which greatly improved the clarity of the paper.

2. Cohomology Computations

Throughout this article we will work with Selmer groups in the cohomology of various mod-p representations of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In fact all representations we consider will be unramified outside of $S = \{p, N, \infty\}$, so will be representations of $G_{\mathbf{Q},S}$, the Galois group over $\mathbf{Q}$ of the maximal extension of $\mathbf{Q}$ unramified outside of 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 $\mathbf{F}_p$-vector space with an action of $G_{\mathbf{Q}}$ via $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_n(\mathbf{F}_p)$.

- Let $\mathbf{F}_p$ and $\mathbf{F}_p(1)$ be the 1-dimensional $\mathbf{F}_p$-vector spaces on which $G_{\mathbf{Q}}$ acts trivially and by the mod-p cyclotomic character χ, respectively. Let $A(i) = A \otimes_{\mathbf{F}_p} \mathbf{F}_p(1)^{\otimes i}$. Throughout, fix a primitive pth root of unity ζ_p, which determines an isomorphism $\mu_p \cong \mathbf{F}_p(1)$.
- Let $b : G_{\mathbf{Q},S} \to \mathbf{F}_p(1)$ be the cocycle defined by $\sigma \mapsto \sigma(N^{1/p})/N^{1/p}$. By Kummer Theory,
$$H^1(G_{\mathbf{Q},S}, \mathbf{F}_p(1)) = \frac{\mathbf{Z}[1/pN]^\times}{\mathbf{Z}[1/pN]^{\times p}}.$$
The class of b in $H^1(G_{\mathbf{Q},S}, \mathbf{F}_p(1))$, which we also denote by b, is the class of N under this isomorphism.
- We denote by $A^\vee$ and A^* the $G_{\mathbf{Q}}$-modules
$$A^\vee = \mathrm{Hom}(A, \mathbf{F}_p) \quad \text{and} \quad A^* = A^\vee(1) = \mathrm{Hom}(A, \mathbf{F}_p(1)).$$

- Given a class $a \in H^1(G_{\mathbf{Q}}, A)$ represented by a cocyle $a : G_{\mathbf{Q}} \to A \cong \mathbf{F}_p^n$, we can write
$$a(\sigma) = \begin{bmatrix} a_0(\sigma) \\ \vdots \\ a_{n-1}(\sigma) \end{bmatrix}$$
for $\sigma \in G_{\mathbf{Q}}$. This defines a new $(n+1)$-dimensional $G_{\mathbf{Q}}$-representation which is an extension of $\mathbf{F}_p$ by A via the map
$$\sigma \mapsto \left(\begin{array}{c|c} & a_0(\sigma) \\ \rho(\sigma) & \vdots \\ & a_{n-1}(\sigma) \\ \hline 0 & 1 \end{array}\right) \in \mathrm{GL}_{n+1}(\mathbf{F}_p)$$
whose kernel cuts out a Galois extension of $\mathbf{Q}$. Conversely, given a $G_{\mathbf{Q}}$-representation which is an extension of $\mathbf{F}_p$ by A of the above form, we get a cohomology class which we denote by
$$a = \begin{bmatrix} a_0 \\ \vdots \\ a_{n-1} \end{bmatrix} \in H^1(G_{\mathbf{Q}}, A).$$
- Given any characters $\chi, \chi' : G_{\mathbf{Q}} \to \mathbf{F}_p^\times$, let $\mathbf{F}_p(\chi)$ and $\mathbf{F}_p(\chi')$ be the lines on which $G_{\mathbf{Q}}$ acts by χ and χ', respectively. Classes $a \in H^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi))$ and $a' \in H^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi'))$ correspond to 2-dimensional $G_{\mathbf{Q}}$-representations of the forms
$$\begin{pmatrix} \chi & a \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \chi' & a' \\ 0 & 1 \end{pmatrix},$$
respectively. These patch together to form a 3-dimensional representation
$$\begin{pmatrix} \chi\chi' & \chi' a & c \\ 0 & \chi' & a' \\ 0 & 0 & 1 \end{pmatrix}$$
if and only if $a \cup a' = 0$ as cohomology classes, in which case the coboundary of $-c$ is the cochain $a \cup a'$.

For a $G_{\mathbf{Q}}$-module A, recall that a Selmer condition is a collection $\mathcal{L} = \{L_v\}$ of subspaces $L_v \subseteq H^1(G_{\mathbf{Q}_v}, A)$ where v runs over all places of $\mathbf{Q}$, such that L_v is the unramified subspace
$$H^1_{\mathrm{ur}}(G_{\mathbf{Q}_v}, A) := H^1(G_{\mathbf{F}_v}, A^{I_v})$$
for almost all places v, where $I_v \subseteq G_{\mathbf{Q}_v} = \mathrm{Gal}(\overline{\mathbf{Q}_v}/\mathbf{Q}_v)$ is the inertia subgroup and $G_{\mathbf{F}_v} = G_{\mathbf{Q}_v}/I_v$ is the absolute Galois group of the residue field at v. The Selmer group associated to a set of conditions $\mathcal{L}$ is then
$$H^1_{\mathcal{L}}(G_{\mathbf{Q}}, A) = \ker\left(H^1(G_{\mathbf{Q}}, A) \to \prod_v \frac{H^1(G_{\mathbf{Q}_v}, A)}{L_v}\right).$$

We will use the following conventions in describing Selmer groups.

- To simplify notation, we will denote a Selmer group $H^1_{\mathcal{L}}(G_{\mathbf{Q}}, A)$ by $H^1_{\mathcal{L}}(A)$.
- As every module A we will consider will be an $\mathbf{F}_p$-vector space, we will use the following notation for dimensions:
$$h^1_{\mathcal{L}}(A) = \dim_{\mathbf{F}_p}(H^1_{\mathcal{L}}(A)).$$

- 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 $H^1(G_{\mathbf{R}}, A) = 0$, removing the need to specify a local condition at the infinite place.
- Given a subset $T \subset S = \{p, N, \infty\}$, 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 behavior allowed at the places of T.

Remark 2.1.1. If A is a module for $G_{\mathbf{Q},S}$ then the Selmer group $H^1_S(A)$ is equal to the $G_{\mathbf{Q},S}$-cohomology $H^1(G_{\mathbf{Q},S}, A)$. Every $G_{\mathbf{Q}}$-module we consider will in fact be a $G_{\mathbf{Q},S}$-module.

Given a Selmer condition $\mathcal{L} = \{L_v\}$ for A, $\mathcal{L}^* := \{L_v^\perp\}$ is a Selmer condition for A^*, where the orthogonal complements are taken with respect to the Tate pairing on local cohomology groups. Note that when v does not divide $\#A$ and the action of $G_{\mathbf{Q}_v}$ on A is unramified, we have that $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_v}, A)^\perp = H^1_{\mathrm{ur}}(G_{\mathbf{Q}_v}, A^*)$ (see Theorem 2.6 of [8]). 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 A be a finite $G_{\mathbf{Q}}$-module, and let $\mathcal{L} = \{L_v\}$ be a Selmer condition for A. Then $H^1_{\mathcal{L}}(A)$ and $H^1_{\mathcal{L}^*}(A^*)$ are finite and*

$$\frac{\#H^1_{\mathcal{L}}(A)}{\#H^1_{\mathcal{L}^*}(A^*)} = \frac{\#H^0(G_{\mathbf{Q}}, A)}{\#H^0(G_{\mathbf{Q}}, A^*)} \prod_v \frac{\#L_v}{\#H^0(G_{\mathbf{Q}_v}, A)}$$

where the product is over all places v of $\mathbf{Q}$.

See [13] 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 $\#L_v = \#H^0(G_{\mathbf{Q}_v}, A)$. 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 $\mathbf{F}_p$-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 ∞.

We will often want to compare sizes of Selmer groups when we change the Selmer conditions. The following lemma gives a way to do such a comparison.

Lemma 2.1.3. *Suppose that $\mathcal{L} = \{L_v\}$ and $\mathcal{L}' = \{L'_v\}$ are two Selmer conditions for A where $\mathcal{L} \subset \mathcal{L}'$ in the sense that $L_v \subseteq L'_v$ for all v. Then we have*

$$\#H^1_{\mathcal{L}'}(A) \leq \#H^1_{\mathcal{L}}(A) \prod_v \frac{\#L'_v}{\#L_v}$$

where the product is over all places v of $\mathbf{Q}$.

Proof. By the definitions of the Selmer groups in question there is an exact sequence

$$0 \to H^1_{\mathcal{L}}(A) \to H^1_{\mathcal{L}'}(A) \to \bigoplus_v \frac{L'_v}{L_v}.$$

The lemma follows by considering the sizes of the terms in this sequence. □

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

- $L_p = 0$.

- $L_N = \ker\big(\mathrm{res}: H^1(G_{\mathbf{Q}_N}, A) \to H^1(G_{K_N}, A)\big)$ where $K_N = \mathbf{Q}_N(N^{1/p})$ 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 $\Sigma^* = \{L_v^\perp\}$, where $L_v^\perp$ is the annihilator of L_v under the local cup product pairing. Applied to a $G_{\mathbf{Q},S}$-module A, it is clear that $L_p^\perp = H^1(G_{\mathbf{Q}_p}, A)$, and $L_v^\perp = H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p}, A)$ for places v outside S. See Proposition 2.2.3 for the determination of the condition $L_N^\perp$.

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

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

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

We establish in the following lemma and propositions the statements about $\mathrm{Sym}^n V$ and its cohomology as a $G_{\mathbf{Q}_N}$-module which will be relevant for applying Theorem 2.1.2.

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

Proof. Note that the action of $G_{\mathbf{Q}}$ on $\mathrm{Sym}^n V$ factors through $G = \mathrm{Gal}(K(\zeta_p)/\mathbf{Q})$. The range of n considered are in fact those symmetric powers of V which are indecomposable as $\mathbf{F}_p$-representations of G (see Theorem 3.1.6). The only indecomposable representation of G of dimension n are the twists by χ of $\mathrm{Sym}^n V$; since the dual of an indecomposable representation will certainly also be indecomposable and of the same dimension, we must have that $(\mathrm{Sym}^n V)^\vee \cong \mathrm{Sym}^n V \otimes \mathbf{F}_p(m)$ for some m. We consider the evaluation pairing

$$\mathrm{Sym}^n V \otimes (\mathrm{Sym}^n V)^\vee \to \mathbf{F}_p$$

restricted to the 1-dimensional subrepresentation $\mathbf{F}_p(n)$ of $\mathrm{Sym}^n V$. Since the above pairing is a perfect $G_{\mathbf{Q}}$-module pairing, the annihilator of $\mathbf{F}_p(n)$ must be an n-dimensional subrepresentation of $(\mathrm{Sym}^n V)^\vee$. Since $(\mathrm{Sym}^n V)^\vee \cong \mathrm{Sym}^n V \otimes \mathbf{F}_p(m)$ has a unique n-dimensional subrepresentation, this means that the pairing descends to a perfect pairing between $\mathbf{F}_p(n)$ and the (unique) 1-dimensional quotient of $(\mathrm{Sym}^n V)^\vee$. As this 1-dimensional quotient is $\mathbf{F}_p(m)$, we conclude that $m = -n$, as a perfect $G_{\mathbf{Q}}$-module pairing

$$\mathbf{F}_p(n) \otimes \mathbf{F}_p(m) \to \mathbf{F}_p$$

exists if and only if $m = -n$. □

Proposition 2.2.2. *For all n in the range $0 \leq n \leq p-2$, $H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V)$ is 2-dimensional, being spanned by*

$$\mathbf{a} = \begin{bmatrix} a \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad \textit{and} \quad \mathbf{b} = \begin{bmatrix} \frac{b^{n+1}}{(n+1)!} \\ \frac{b^n}{n!} \\ \vdots \\ b \end{bmatrix},$$

where a is a class spanning the 1-dimensional unramified subspace of $H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p)$, and $\mathbf{b}$ is the class corresponding to $\mathrm{Sym}^{n+1}V$, which is an extension of $\mathbf{F}_p$ by $\mathrm{Sym}^n V$ as $G_{\mathbf{Q}_N}$-modules.

Further, the subgroup $L_N \subset H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V)$ is 1-dimensional and spanned by $\mathbf{b}$.

Proof. It follows from the Local Euler Characteristic Formula (Theorem 2.8 of [8]) that $H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V)$ is 2-dimensional. Consider the short exact sequence

$$0 \to \mathbf{F}_p \to \mathrm{Sym}^n V \to \mathrm{Sym}^{n-1} V \to 0$$

of $G_{\mathbf{Q}_N}$-modules. The first terms of the associated long exact sequence in $G_{\mathbf{Q}_N}$-cohomology give us

$$0 \to \mathbf{F}_p \to \mathbf{F}_p \to \mathbf{F}_p \xrightarrow{b\cup -} H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p) \to H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V).$$

Since a and b form a basis for $H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p)$, and the image of $\mathbf{F}_p \xrightarrow{b\cup -} H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p)$ is the span of b, we conclude that the image of

$$H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p) \to H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V)$$

is spanned by the image of a; this is the class $\mathbf{a}$ defined above. To see that the class $\mathbf{b}$ is nonzero, consider the map

$$H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V) \to H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p)$$

coming from the long exact sequence in $G_{\mathbf{Q}_N}$-cohomology associated to the short exact sequence

$$0 \to \mathrm{Sym}^{n-1} V \to \mathrm{Sym}^n V \to \mathbf{F}_p \to 0.$$

The image of $\mathbf{b}$ under this map is the class $b \in H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p)$, which is nonzero, hence we conclude that $\mathbf{b}$ itself is nonzero.

Finally we see that $\mathbf{a}$ and $\mathbf{b}$ are linearly independent in $H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V)$ (and therefore constitute a basis), as $\mathbf{b}$ is trivial when restricted to G_{K_N} (even as a cocycle) and $\mathbf{a}$ is not. This also establishes that

$$L_N = \ker(H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V) \to H^1(G_{K_N}, \mathrm{Sym}^n V))$$

is 1-dimensional and is spanned by $\mathbf{b}$. □

Proposition 2.2.3. *Suppose that $A \cong \mathrm{Sym}^n V$ as a $G_{\mathbf{Q}_N}$-representation for some $n \leq p-2$. Under the local Tate pairing*

$$H^1(G_{\mathbf{Q}_N}, A) \otimes H^1(G_{\mathbf{Q}_N}, A^*) \to H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p(1))$$

the annihilator of $L_N \subseteq H^1(G_{\mathbf{Q}_N}, A)$ is

$$L_N^{\perp} = \ker\left(\mathrm{res} : H^1(G_{\mathbf{Q}_N}, A^*) \to H^1(G_{K_N}, A^*)\right).$$

That is, the dual condition $L_N^{\perp}$ is again the condition L_N (applied to the module A^*).

Proof. We first note that if suffices to prove this proposition only for $\mathrm{Sym}^n V$, as if $f : \mathrm{Sym}^n V \to A$ is an isomorphism of $G_{\mathbf{Q}_N}$-modules, we have that f induces an isomorphism between first cohomology groups which restricts to an isomorphism between the L_N subgroup on each side. The same also holds for the L_N subgroups in the first cohomology of $(\mathrm{Sym}^n V)^*$ and A^*.

Choose an isomorphism of $G_{\mathbf{Q}_N}$-modules $\phi : \mathrm{Sym}^n V \to (\mathrm{Sym}^n V)^*$ (this is possible as globally $\mathrm{Sym}^n V$ is self-dual up to a twist by some power of χ by Lemma 2.2.1, and χ is trivial as a character of $G_{\mathbf{Q}_N}$). We have as before that the isomorphism on first cohomology induced by ϕ restricts to an isomorphism of L_N subgroups; we write henceforth $\phi(L_N)$ for the L_N condition subgroup of $H^1(G_{\mathbf{Q}_N}, (\mathrm{Sym}^n V)^*)$. We know that the local Tate pairing in question is a perfect pairing, hence the annihilator $L_N^{\perp}$ of L_N must also be 1-dimensional. Therefore it suffices to prove that $\phi(L_N)$ is contained in $L_N^{\perp}$, i.e. $L_N \cup \phi(L_N) = 0$.

The cup product map

$$H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V) \otimes H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V) \to H^2(G_{\mathbf{Q}_N}, (\mathrm{Sym}^n V)^{\otimes 2})$$

is alternating, as it is in an odd degree of cohomology. In particular under this cup product map $L_N \cup L_N = 0$. Applying the isomorphism ϕ to the second coordinate gives that under the cup product

$$H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V) \otimes H^1(G_{\mathbf{Q}_N}, (\mathrm{Sym}^n V)^*) \to H^2(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V \otimes (\mathrm{Sym}^n V)^*)$$

we have that $L_N \cup \phi(L_N) = 0$. The local Tate pairing is the composition of the above cup product map with the map

$$H^2(G_{\mathbf{Q}_N}, \mathrm{Sym}^n V \otimes (\mathrm{Sym}^n V)^*) \to H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p(1))$$

induced by the evaluation pairing $\mathrm{Sym}^n V \otimes (\mathrm{Sym}^n V)^* \to \mathbf{F}_p(1)$, so we conclude that $\phi(L_N) = L_N^{\perp}$. □

We finish this section with a lemma regarding the Selmer group $H^1_{\Sigma^*}(\mathbf{F}_p)$.

Lemma 2.2.4. *The completion of $\mathbf{Q}(\zeta_N^{(p)})$ at the prime above N is K_N. That is, the class $c \in H^1_S(\mathbf{F}_p)$ which represents $\mathbf{Q}(\zeta_N^{(p)})$ lies in the Selmer subgroup $H^1_{\Sigma^*}(\mathbf{F}_p)$.*

Proof. The two extensions of $\mathbf{Q}_N$ in question are $\mathbf{Q}_N(\zeta_N^{(p)})$ and $\mathbf{Q}_N(N^{1/p})$, both of which are totally ramified $\mathbf{F}_p$-extensions of $\mathbf{Q}_N$.

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

$$\begin{aligned}\mathrm{Norm}_{\mathbf{Q}_N}^{K_N}(N^{1/p}) &= \prod_{i=0}^{p-1} \zeta_p^i N^{1/p} \\ &= N\end{aligned}$$

but we also have

$$\begin{aligned}\mathrm{Norm}_{\mathbf{Q}_N}^{\mathbf{Q}_N(\zeta_N^{(p)})}(\mathrm{Norm}_{\mathbf{Q}_N(\zeta_N^{(p)})}^{\mathbf{Q}_N(\zeta_N)}(1-\zeta_N)) &= \mathrm{Norm}_{\mathbf{Q}_N}^{\mathbf{Q}_N(\zeta_N)}(1-\zeta_N) \\ &= \prod_{j=1}^{N-1}(1-\zeta_N^j) \\ &= N.\end{aligned}$$

Therefore we conclude that $\mathbf{Q}_N(\zeta_N^{(p)}) = K_N$. □

2.3. **Selmer Groups in the Cohomology of the Cyclotomic Character.** This section contains a collection of statements about the dimensions of various Selmer groups in the cohomology of $\mathbf{F}_p(i)$.

Definition 2.3.1. Let p be an odd prime and $0 \leq i \leq p-2$. Let $r^{\chi^i}_{\mathbf{Q}(\zeta_p)}$ denote the p-rank of the χ^i-eigenspace of the class group of $\mathbf{Q}(\zeta_p)$. We say that (p,i) is a *regular pair* if $r^{\chi^i}_{\mathbf{Q}(\zeta_p)} = 0$.

Remark 2.3.2. It is always true that $(p,0)$ and $(p,1)$ are regular pairs. If i is odd, the theorems of Herbrand and Ribet give the following characterization: (p,i) is a regular pair if and only if the generalized Bernoulli number $B_{1,\chi^{-i}}$ (equivalently, the Bernoulli number B_{p-i}) is not divisible by p. See Section 6.3 of [14] for a more detailed discussion of these facts.

Theorem 2.3.3. *Let p be an odd prime. The following statements are true.*

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

(2) *The group $H^1_S(\mathbf{F}_p(1))$ is 2-dimensional, and spanned by the classes of N and p under the Kummer isomorphism*

$$H^1_S(\mathbf{F}_p(1)) = \frac{\mathbf{Z}[1/pN]^\times}{(\mathbf{Z}[1/pN]^\times)^p}.$$

(3) *For any i, we have that*

$$h^1_\emptyset(\mathbf{F}_p(i)) = r^{\chi^i}_{\mathbf{Q}(\zeta_p)}.$$

(4) *For any odd $i \not\equiv 1 \bmod p-1$ we have that*

$$h^1_\emptyset(\mathbf{F}_p(1-i)) \leq h^1_\emptyset(\mathbf{F}_p(i)) \leq 1 + h^1_\emptyset(\mathbf{F}_p(1-i)).$$

This is equivalent to Theorem 10.9 of [14].

Proof. Parts 1 and 2 follow from the Kronecker-Weber theorem and Kummer theory, respectively.

For part 3, note that the restriction map

$$H^1(G_{\mathbf{Q},S}, \mathbf{F}_p(i)) \to H^1(G_{\mathbf{Q}(\zeta_p),S}, \mathbf{F}_p(i))^{\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})}$$

is an isomorphism by the inflation-restriction sequence. This latter group can be interpreted as the $\mathbf{F}_p$-extensions of $\mathbf{Q}(\zeta_p)$ which are unramified away from S and whose Galois group is $\mathbf{F}_p(i)$ as a $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$-module through the equality

$$H^1(G_{\mathbf{Q}(\zeta_p),S}, \mathbf{F}_p(i)) = \mathrm{Hom}(G_{\mathbf{Q}(\zeta_p),S}, \mathbf{F}_p(i)).$$

The subgroup $H^1_\emptyset(\mathbf{F}_p(i))$ is those classes which are unramified everywhere. Global class field theory gives that $r^{\chi^i}_{\mathbf{Q}(\zeta_p)}$ is the number of independent $\mathbf{F}_p$-extensions of $\mathbf{Q}(\zeta_p)$ which are unramified everywhere and whose Galois group is $\mathbf{F}_p(i)$ as a $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$-module. Thus we conclude that the dimension $h^1_\emptyset(\mathbf{F}_p(i))$ is equal to $r^{\chi^i}_{\mathbf{Q}(\zeta_p)}$, as both count the same set of extensions.

The inequalities in part 4 both follow from applying Theorem 2.1.2 and estimating dimensions in a change of Selmer conditions as in Lemma 2.1.3. For instance, by Theorem 2.1.2 applied to $H^1_\emptyset(\mathbf{F}_p(i))$ we have

$$\begin{aligned}&\frac{\#H^1_\emptyset(\mathbf{F}_p(i))}{\#H^1_{\emptyset^*}(\mathbf{F}_p(1-i))}\\ &= \frac{\#H^0(\mathbf{F}_p(i))}{\#H^0(\mathbf{F}_p(1-i))}\prod_v \frac{\#L_v}{\#H^0(G_{\mathbf{Q}_v},\mathbf{F}_p(i))}\\ &= \frac{\#H^0(\mathbf{F}_p(i))}{\#H^0(\mathbf{F}_p(1-i))}\cdot\frac{\#H^1_{\mathrm{ur}}(G_{\mathbf{Q}_N},\mathbf{F}_p(i))}{\#H^0(G_{\mathbf{Q}_N},\mathbf{F}_p(i))}\cdot\frac{\#H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p},\mathbf{F}_p(i))}{\#H^0(G_{\mathbf{Q}_p},\mathbf{F}_p(i))}\cdot\frac{\#H^1(G_{\mathbf{R}},\mathbf{F}_p(i))}{\#H^0(G_{\mathbf{R}},\mathbf{F}_p(i))}\\ &= \frac{1}{1}\cdot\frac{p}{p}\cdot\frac{1}{1}\cdot\frac{1}{1}\\ &= 1\end{aligned}$$

where we know all of the local terms using the Local Euler Characteristic Formula and the parity of i. Stated in terms of dimensions, this relation is

$$h^1_\emptyset(\mathbf{F}_p(i)) = h^1_{\emptyset^*}(\mathbf{F}_p(1-i)).$$

Since we have that the Selmer condition $\emptyset^*$ contains the Selmer condition $\emptyset$, we may apply Lemma 2.1.3 to get

$$\begin{aligned}\#H^1_{\emptyset^*}(\mathbf{F}_p(1-i)) &\leq \#H^1_\emptyset(\mathbf{F}_p(1-i))\frac{\#H^1(G_{\mathbf{Q}_p},\mathbf{F}_p(1-i))}{\#H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p},\mathbf{F}_p(1-i))}\\ &= \#H^1_\emptyset(\mathbf{F}_p(1-i))\cdot p\end{aligned}$$

where we have again used the Local Euler Characteristic Formula to determine the local terms. Stated in terms of dimensions, this relation is

$$h^1_{\emptyset^*}(\mathbf{F}_p(1-i)) \leq h^1_\emptyset(\mathbf{F}_p(1-i)) + 1.$$

Thus we conclude that

$$h^1_\emptyset(\mathbf{F}_p(i)) \leq h^1_\emptyset(\mathbf{F}_p(1-i)) + 1.$$

The other inequality of part 4 follows from a similar argument, starting with $H^1_\emptyset(\mathbf{F}_p(1-i))$. □

Corollary 2.3.4. *For any i, $h^1_\Sigma(\mathbf{F}_p(i)) \leq 1 + r^{\chi^i}_{\mathbf{Q}(\zeta_p)}$.*

Proof. This follows from the fact that $H^1_\Sigma(\mathbf{F}_p(i)) \subseteq H^1_N(\mathbf{F}_p(i))$ and Lemma 2.1.3 applied to the Selmer conditions $\emptyset$ and N along with part 3 of the previous Theorem. □

Theorem 2.3.5. *Let p be an odd prime, let $i \not\equiv 1 \bmod p-1$ be odd, and assume that (p,i) is a regular pair. Then we have the following*

1. *$h^1_\emptyset(\mathbf{F}_p(i)) = h^1_\emptyset(\mathbf{F}_p(1-i)) = 0$.*
2. *$h^1_S(\mathbf{F}_p(i)) = 2$, $h^1_p(\mathbf{F}_p(i)) = 1$, and $h^1_N(\mathbf{F}_p(i)) = 1$.*
3. *$h^1_S(\mathbf{F}_p(1-i)) = 1$.*
4. *$h^1_\Sigma(\mathbf{F}_p(i))$ and $h^1_\Sigma(\mathbf{F}_p(1-i))$ are both at most 1.*

Proof. The first statement follows from parts 3 and 4 of Theorem 2.3.3 under the assumption that (p, i) is a regular pair.

Parts 2 and 3 each follow from applying Theorem 2.1.2 and then estimating changes in Selmer conditions. For instance, Theorem 2.1.2 for $H^1_N(\mathbf{F}_p(i))$ yields

$$h^1_N(\mathbf{F}_p(i)) = 1 + h^1_{N^*}(\mathbf{F}_p(1-i)).$$

We have that the Selmer condition N^* means classes which are split at N and have any behavior at p, hence $H^1_{N^*}(\mathbf{F}_p(1-i)) \subseteq H^1_p(\mathbf{F}_p(1-i))$. Applying Theorem 2.1.2 to $H^1_p(\mathbf{F}_p(1-i))$ yields

$$h^1_p(\mathbf{F}_p(1-i)) = h^1_{p^*}(\mathbf{F}_p(i)).$$

Since the Selmer condition p^* is "unramified at N and split at p", we have

$$H^1_{p^*}(\mathbf{F}_p(i)) \subseteq H^1_\emptyset(\mathbf{F}_p(i)).$$

The statement $h^1_N(\mathbf{F}_p(i)) = 1$ thus follows from the chain of inequalities

$$\begin{aligned} h^1_N(\mathbf{F}_p(i)) &= 1 + h^1_{N^*}(\mathbf{F}_p(1-i)) \\ &\leq 1 + h^1_p(\mathbf{F}_p(1-i)) \\ &= 1 + h^1_{p^*}(\mathbf{F}_p(i)) \\ &\leq 1 + h^1_\emptyset(\mathbf{F}_p(i)) \\ &= 1 + 0. \end{aligned}$$

Part 4 of the theorem now follows from the inclusions $H^1_\Sigma(\mathbf{F}_p(i)) \subseteq H^1_N(\mathbf{F}_p(i))$ and $H^1_\Sigma(\mathbf{F}_p(1-i)) \subseteq H^1_S(\mathbf{F}_p(1-i))$; in both cases we know that the dimension of the larger group is 1. □

Theorem 2.3.6. *Let p be an odd prime. Then for odd $3 \leq i \leq p-2$ we have*

$$\begin{aligned} h^1_\Sigma(\mathbf{F}_p(i)) &= h^1_{\Sigma^*}(\mathbf{F}_p(1-i)) \\ h^1_{\Sigma^*}(\mathbf{F}_p(i)) &= h^1_\Sigma(\mathbf{F}_p(1-i)) + 1 \\ h^1_{\Sigma^*}(\mathbf{F}_p(i)) &\leq 1 + h^1_\Sigma(\mathbf{F}_p(i)). \end{aligned}$$

Proof. The first two statements are proved by applying Theorem 2.1.2 to $H^1_\Sigma(\mathbf{F}_p(i))$ and $H^1_{\Sigma^*}(\mathbf{F}_p(i))$. The final statement follows from Lemma 2.1.3 applied to Σ and Σ^*. □

Corollary 2.3.7. *Let p be an odd prime. Then for even $i \not\equiv 0 \bmod p-1$,*

$$h^1_\Sigma(\mathbf{F}_p(i)) \neq 0 \implies h^1_\Sigma(\mathbf{F}_p(1-i)) \neq 0.$$

Proof. If $h^1_\Sigma(\mathbf{F}_p(i)) \geq 1$, then by Theorem 2.3.6 we have $h^1_{\Sigma^*}(\mathbf{F}_p(1-i)) \geq 2$. Comparing via

$$h^1_{\Sigma^*}(\mathbf{F}_p(1-i)) \leq 1 + h^1_\Sigma(\mathbf{F}_p(1-i))$$

gives that $h^1_\Sigma(\mathbf{F}_p(1-i)) \geq 1$. □

Remark 2.3.8. Under the assumption that (p, i) is a regular pair, we know that any nonzero class in $H^1_\Sigma(\mathbf{F}_p(i))$ (for $i \neq 0, 1$) will be a nonzero multiple of b when restricted to $G_{\mathbf{Q}_N}$: 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 nonzero locally at N.

2.4. **Cup Products and Σ.** The purpose of the Selmer condition Σ^* is to detect those classes whose cup product with b is equal to 0, according to the following propositions.

Proposition 2.4.1. *Let p be an odd prime and $0 \leq i \leq p-2$. Assume either $i = 0$ or 1, that (p, i) is a regular pair if i is odd, or that $(p, 1-i)$ is a regular pair if i is even. Let A and A' be $G_{\mathbf{Q},S}$-modules with a pairing $A \otimes A' \to \mathbf{F}_p(i)$ for some i. Given classes $a \in H^1_S(A)$ and $a' \in H^1_S(A')$, the global cup product $a \cup a' \in H^2_S(G_{\mathbf{Q}}, \mathbf{F}_p(i))$ induced by this pairing vanishes if and only if the local cup product $\mathrm{res}_N(a) \cup \mathrm{res}_N(a') \in H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p(i))$ does.*

Proof. We first claim that the restriction map $H^2_S(\mathbf{F}_p(i)) \to H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p(i))$ is injective. Under the regularity assumption on (p, i), the Global Euler Characteristic Formula (Theorem 5.1 of [8]) combined with Theorems 2.3.3 and 2.3.5 gives us that $H^2_S(\mathbf{F}_p(i))$ is 1-dimensional. Similarly, $H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p(i))$ is 1-dimensional by Local Tate Duality (Corollary 2.3 of [8]). Thus, to prove injectivity it suffices to prove surjectivity.

The end of the Poitou-Tate exact sequence (Theorem 4.10 of [8]) for $\mathbf{F}_p(i)$ is

$$H^2_S(\mathbf{F}_p(i)) \to H^2(G_{\mathbf{Q}_p}, \mathbf{F}_p(i)) \oplus H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p(i)) \to H^0(G_{\mathbf{Q},S}, \mathbf{F}_p(1-i))^\vee \to 0.$$

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

Thus, the commutativity of the diagram

$$\begin{tikzcd}
H^1_S(A) \otimes H^1_S(A') \arrow[r, "\cup"] \arrow[d] & H^2_S(G_{\mathbf{Q}}, \mathbf{F}_p(i)) \arrow[d, hook] \\
H^1(G_{\mathbf{Q}_N}, A) \otimes H^1(G_{\mathbf{Q}_N}, A') \arrow[r, "\cup"] & H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p(i))
\end{tikzcd}$$

shows that the non-vanishing of $a \cup a'$ can be detected locally, as desired. □

Remark 2.4.2. In the notation of the previous proposition, when (p, i) is not a regular pair it is still (clearly) true that $a \cup a' = 0$ implies that $\mathrm{res}_N(a) \cup \mathrm{res}_N(a') = 0$. However, the converse need not hold in this setting as $h^2_S(\mathbf{F}_p(i))$ need not be equal to 1, and thus the map $H^2_S(\mathbf{F}_p(i)) \to H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p(i))$ need not be injective.

Proposition 2.4.3. *Let p be any odd prime and $0 \leq i \leq p-2$. Let A, A' be as in the previous proposition, but assume now that $A, A' \cong \mathrm{Sym}^n V$ as $G_{\mathbf{Q}_N}$-representations. If $a \in H^1_{\Sigma^*}(A)$ and $\mathrm{res}_N(a) \neq 0$, and if $a' \in H^1_S(A')$, then $\mathrm{res}_N(a) \cup \mathrm{res}_N(a') = 0$ if and only if $a' \in H^1_{\Sigma^*}(A')$. In particular, if $a \cup a' = 0$ then $a' \in H^1_{\Sigma^*}(A')$.*

Furthermore, if either $i = 0$ or 1, or if (p, i) is a regular pair and i is odd, or if $(p, 1-i)$ is a regular pair and i is even, then $a \cup a' = 0$ if and only if $a' \in H^1_{\Sigma^*}(A')$.

Proof. Since $\mathrm{res}_N(a)$ is nonzero, Proposition 2.2.2 gives that $\mathrm{res}_N(a) = u\mathbf{b}$ for some nonzero $u \in \mathbf{F}_p$. Furthermore, Proposition 2.2.3 shows that the statement $u\mathbf{b} \cup \mathrm{res}_N(a') = 0$ implies that $\mathrm{res}_N(a')$ is also multiple of $\mathbf{b}$ (possibly 0), which is the condition for a' to be an element of the Selmer group $H^1_{\Sigma^*}(A')$. The final statement of the proposition then follows from Proposition 2.4.1. □

3. Selmer groups and 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 $\mathrm{Sym}^{p-4}V$, which in turn is bounded by dimensions of Selmer subgroups in the Galois cohomology of characters.

The main theorem of this section is:

Theorem 3.0.1. *Let p be odd. Then*

$$r_K = 1 + h^1_\Sigma(\mathrm{Sym}^{p-4}V \otimes \mathbf{F}_p(2)).$$

Additionally, there is a filtration of $\mathrm{Sym}^{p-4}V \otimes \mathbf{F}_p(2)$ *that induces the following lower and upper bounds on r_K:*

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

This is essentially Theorem 1.2.1. The lower bound in this theorem was first established by Wake–Wang-Erickson; we recover this as Proposition 4.0.1. Throughout this section, E will be an unramified $\mathbf{F}_p$-extension of K and M will be its Galois closure over $\mathbf{Q}$. The proof begins in Section 3.1 with some preliminary lemmas on the structure of $\mathrm{Gal}(M/K(\zeta_p))$ as a $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q})$-representation.

In Section 3.2, we introduce an auxiliary Selmer condition Λ, which will encode the local conditions that cut out those Galois cohomology classes corresponding to unramified $\mathbf{F}_p$-extensions of K. We will also define a filtration on the $\mathbf{F}_p$-vector space $H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$ related to the filtration defined by Iimura in [4] on $\mathrm{Cl}_{K(\zeta_p)}$; see Remark 3.2.4. This filtration of Iimura is also used by Lecouturier in [6].

The next step in the proof of Theorem 3.0.1 is to relate the Selmer condition Λ to the Selmer condition Σ defined in Section 2.2. This is done in Section 3.3, which also contains some general lemmas that realize Σ^* as the "correct" Selmer condition for discussing the lifting of representations to higher dimensions.

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

3.1. Indecomposability of some $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q})$-modules arising from Cl_K.

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

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

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

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

Theorem 3.1.2. $A = \mathrm{Gal}(M/K(\zeta_p))$ *is an $\mathbf{F}_p$-vector space, and is isomorphic to* $\mathrm{Sym}^{m-1}V \otimes \mathbf{F}_p(1-m)$ *as a* $G = \mathrm{Gal}(K(\zeta_p)/\mathbf{Q})$*-representation where m is the type*

$$(*)\qquad \begin{tikzcd}
 & M \arrow[d, dash] \arrow[dd, dash, bend left, "A"] \\
 & E(\zeta_p) \arrow[d, dash] \\
E \arrow[ur, dash] \arrow[d, dash] & K(\zeta_p) \arrow[d, dash] \arrow[dd, dash, bend left, "G"] \\
K \arrow[ur, dash] \arrow[dr, dash] & \mathbf{Q}(\zeta_p) \arrow[d, dash] \\
 & \mathbf{Q}
\end{tikzcd}$$

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 pth root of unity ζ_p gives us a canonical generator of $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q}(\zeta_p))$, namely the particular σ with $\sigma(N^{1/p}) = \zeta_p N^{1/p}$. We use this to fix an isomorphism $G \cong \mathbf{Z}/p\mathbf{Z} \rtimes (\mathbf{Z}/p\mathbf{Z})^\times$.

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

$$1 \to A \to \mathrm{Gal}(M/\mathbf{Q}) \to G \to 1$$

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

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

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

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

is an isomorphism.

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

$$1 \to A \to \mathrm{Gal}(M/\mathbf{Q}(\zeta_p)) \to \mathrm{Gal}(K(\zeta_p)/\mathbf{Q}(\zeta_p)) \to 1.$$

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 $M/\mathbf{Q}(\zeta_p)$ is p, since N is totally ramified in $K(\zeta_p)/\mathbf{Q}(\zeta_p)$ and unramified in $M/K(\zeta_p)$, so the inertia group at $\mathfrak{N}$ is a copy of $\mathbf{Z}/p\mathbf{Z}$ in $\mathrm{Gal}(M/\mathbf{Q}(\zeta_p))$ that maps isomorphically onto $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q}(\zeta_p))$. This inertia group is the image our desired splitting. □

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 $\mathbf{Q}_p(\zeta_p)$, each of degree dividing p and Galois over $\mathbf{Q}_p$, and that $\mathrm{Gal}(F/\mathbf{Q}_p(\zeta_p))$ and $\mathrm{Gal}(F'/\mathbf{Q}_p(\zeta_p))$ are not isomorphic as representations of $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p) = (\mathbf{Z}/p\mathbf{Z})^\times$, or that both extensions are trivial. If FF'/F is unramified, then $F'/\mathbf{Q}_p(\zeta_p)$ is also unramified.*

This follows from the fact that any unramified extension of $\mathbf{Q}_p(\zeta_p)$ must be cyclic and Galois over $\mathbf{Q}_p$, and that $\mathbf{F}_p(i) \oplus \mathbf{F}_p(j)$ has exactly two $(\mathbf{Z}/p\mathbf{Z})^\times$-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 $\mathbf{Q}(\zeta_N)/\mathbf{Q}$.*

Proof. The backward direction is trivial: It is clearly unramified away from N, Lemma 2.2.4 shows that $K(\zeta_N^{(p)})/K$ is unramified at N as well, and the Galois closure of $K(\zeta_N^{(p)})/\mathbf{Q}$ is $K(\zeta_p, \zeta_N^{(p)})$.

If $m = 1$ then $E(\zeta_p) = M$ is Galois over $\mathbf{Q}$ and $A = \mathbf{Z}/p\mathbf{Z}$. Consider the action of G on A by conjugation and recall that $G = \mathbf{Z}/p\mathbf{Z} \rtimes_\chi (\mathbf{Z}/p\mathbf{Z})^\times$. The order-$p$ subgroup of G acts trivially on A as there are no non-trivial 1-dimensional $\mathbf{F}_p$-representations of $\mathbf{Z}/p\mathbf{Z}$. Referencing $(*)$, we see that $(\mathbf{Z}/p\mathbf{Z})^\times \subseteq G$ is the image of $\mathrm{Gal}(E(\zeta_p)/E) \subseteq \mathrm{Gal}(E(\zeta_p)/\mathbf{Q})$ which acts trivially on $A = \mathrm{Gal}(E(\zeta_p)/K(\zeta_p))$, 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

$$\mathrm{Gal}(E(\zeta_p)/\mathbf{Q}) = \mathbf{Z}/p\mathbf{Z} \times G$$

by Lemma 3.1.3. Consider $L = E(\zeta_p)^G$, which is $\mathbf{Z}/p\mathbf{Z}$ extension of $\mathbf{Q}$. As $\mathrm{Gal}(E(\zeta_p)/E) = (\mathbf{Z}/p\mathbf{Z})^\times \subseteq G$ we know that $L \subseteq E$. As $L \neq K$ this tells us that $E = LK$.

We claim that $L = \mathbf{Q}(\zeta_N^{(p)})$. 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 $L(\zeta_p)/\mathbf{Q}(\zeta_p)$ is unramified, as $[L : \mathbf{Q}]$ is coprime to $[\mathbf{Q}(\zeta_p) : \mathbf{Q}]$. We have the following diagram of fields:

$$\begin{tikzcd}
 & E(\zeta_p) \arrow[dl, dash] \arrow[dr, dash] & \\
L(\zeta_p) \arrow[d, dash] \arrow[dr, dash] & & K(\zeta_p) \arrow[dl, dash] \\
L \arrow[dr, dash] & \mathbf{Q}(\zeta_p) \arrow[d, dash] & \\
 & \mathbf{Q} &
\end{tikzcd}$$

Consider the corresponding extensions of fields locally at p. Because the groups $\mathrm{Gal}(L(\zeta_p)/\mathbf{Q}(\zeta_p))$ and $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q}(\zeta_p))$ are not isomorphic as modules over the group $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$, 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 $k \in \mathbf{Z}/(p-1)\mathbf{Z}$ and let Γ_k be the group $\mathbf{Z}/p\mathbf{Z} \rtimes (\mathbf{Z}/p\mathbf{Z})^\times$, where $u \in (\mathbf{Z}/p\mathbf{Z})^\times$ acts on $\mathbf{Z}/p\mathbf{Z}$ by multiplication by u^k.*

The indecomposable $\mathbf{F}_p$-representations of Γ_k are exactly

$$\mathrm{Sym}^j V_k \otimes \mathbf{F}_p(i)$$

for $0 \le i \le p-2$ and $0 \le j \le p-1$, where $\mathbf{F}_p(i)$ is the 1-dimensional representation where $u \in (\mathbf{Z}/p\mathbf{Z})^\times$ acts by u^i and V_k is the 2-dimensional representation of Γ_k over $\mathbf{F}_p$ given by the map

$$\Gamma_k \to \mathrm{GL}_2(\mathbf{F}_p)$$
$$(b,u) \mapsto \begin{pmatrix} u^k & b \\ 0 & 1 \end{pmatrix}.$$

Proof. See [1] for a proof. The cyclic case Γ_0 is treated in a discussion following Corollary 7 of Chapter 5, and the general case is treated in discussions following Lemma 8 of Chapter 5 and Corollary 5 of Chapter 6. The structure of the proof is as follows:

- The irreducible $\mathbf{F}_p$-representations of Γ_k are all 1-dimensional, namely they are the 1-dimensional representations $\mathbf{F}_p(i)$ of the quotient $(\mathbf{Z}/p\mathbf{Z})^\times$ of Γ_k.
- There is a bijection between irreducible $\mathbf{F}_p$-representations of Γ_k and indecomposable projective $\mathbf{F}_p[\Gamma_k]$-modules, given by associating $P/\mathrm{rad}(P)$ to each indecomposable projective module P. This is Theorem 3 of Chapter 5 of [1].
- Every $\mathbf{F}_p[\Gamma_k]$-module X with $X/\mathrm{rad}(X) \cong \mathbf{F}_p(i)$ is a homomorphic image of the indecomposable projective module associated to $\mathbf{F}_p(i)$. This is Lemma 5 of Chapter 5 of [1].
- Each indecomposable projective module has radical length exactly p. In particular it is p-dimensional as an $\mathbf{F}_p$-vector space, as all quotients in its radical series are irreducible. This is the discussion after Lemma 8 of Chapter 5 of [1].

  This is enough to show that the unique indecomposable projective module associated to $\mathbf{F}_p(i)$ is $\mathrm{Sym}^{p-1} V_k \otimes \mathbf{F}_p(i)$, as it is p-dimensional, indecomposable, and has $\mathbf{F}_p(i)$ as a quotient.
- Any indecomposable $\mathbf{F}_p$-representation of Γ_k has a unique radical series. In particular if X is an indecomposable $\mathbf{F}_p$-representation of Γ_k, $X/\mathrm{rad}(X)$ is irreducible. This is the discussion after Corollary 5 of Chapter 6 of [1].

  This allows us to conclude that every such X is surjected to by some $\mathrm{Sym}^{p-1} V_k \otimes \mathbf{F}_p(i)$; the quotient modules of $\mathrm{Sym}^{p-1} V_k \otimes \mathbf{F}_p(i)$ are just $\mathrm{Sym}^j V_k \otimes \mathbf{F}_p(i)$ for $0 \le j \le p-1$. □

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 $A^{\mathbf{Z}/p\mathbf{Z}}$. Indeed, each indecomposable factor when considered as a representation of $\mathbf{Z}/p\mathbf{Z}$ corresponds to a Jordan block with eigenvalue 1. Thus we've reduced the indecomposability of A to showing that $A^{\mathbf{Z}/p\mathbf{Z}}$ is 1-dimensional.

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

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

is the Galois closure of $E(\zeta_p)/\mathbf{Q}$, any normal subgroup of $\mathrm{Gal}(M/\mathbf{Q})$ contained in $\mathrm{Gal}(M/E(\zeta_p))$ is necessarily trivial.

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

Referencing $(*)$, notice now that the action of $(\mathbf{Z}/p\mathbf{Z})^\times = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ on A is the same as the action of $\mathrm{Gal}(E(\zeta_p)/E)$ on A. But the action of $\mathrm{Gal}(E(\zeta_p)/E)$ on A clearly stabilizes $\mathrm{Gal}(M/E(\zeta_p)) \subseteq A$.

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

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

The short exact sequence

$$1 \to \mathrm{Gal}(M/E(\zeta_p)) \to A \to \mathrm{Gal}(E(\zeta_p)/K(\zeta_p)) \to 1$$

is $\mathrm{Gal}(K(\zeta_p)/K)$-equivariant. As $A^{\mathbf{Z}/p\mathbf{Z}}$ has trivial intersection with the above kernel, it maps isomorphically onto $\mathrm{Gal}(E(\zeta_p)/K(\zeta_p))$, which we just established carries the trivial $(\mathbf{Z}/p\mathbf{Z})^\times$ action. □

The first part of Lemma 3.1.7 gives $A \cong \mathrm{Sym}^j V \otimes \mathbf{F}_p(i)$ 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 $A \cong \mathrm{Sym}^{m-1} V \otimes \mathbf{F}_p(1-m)$ 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 $\mathrm{Gal}(M/\mathbf{Q})$ as an explicit matrix group that we can view as the image of a representation of $G_{\mathbf{Q},S}$.

Suppose that A is an $\mathbf{F}_p$-vector space and that $G \to \mathrm{Aut}(A) = \mathrm{GL}_m(\mathbf{F}_p)$ is an injective homomorphism. Then $A \rtimes G$ 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 $\mathrm{GL}_m(\mathbf{F}_p)$ 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 paragraph establishes that in a suitable basis of $\mathrm{Sym}^{m-1} V \otimes \mathbf{F}_p(1-m)$ (see Remark 3.1.8), $\mathrm{Gal}(M/\mathbf{Q})$ is isomorphic to the group of matrices

$$(**) \qquad \left(\begin{array}{ccccc|c} 1 & \chi^{-1} b & \chi^{-2} \frac{b^2}{2} & \cdots & \chi^{-(m-1)} \frac{b^{m-1}}{(m-1)!} & a_0 \\ & \chi^{-1} & \chi^{-2} b & \cdots & \chi^{-(m-1)} \frac{b^{m-2}}{(m-2)!} & a_1 \\ & & \chi^{-2} & & \vdots & \vdots \\ & & & \ddots & \chi^{-(m-1)} b & a_{m-2} \\ & & & & \chi^{-(m-1)} & a_{m-1} \\ \hline & & & & & 1 \end{array}\right)$$

where the i,j-th entry in the top left block is $\chi^{-(j-1)}\frac{b^{j-i}}{(j-i)!}$. This also defines a representation

$$G_{\mathbf{Q},S} \to \mathrm{Gal}(M/\mathbf{Q}) \to \mathrm{GL}_{m+1}(\mathbf{F}_p)$$

of dimension $m+1$ that we will consider more carefully in Section 3.2.

Remark 3.1.8. In light of the discussion after Lemma 3.1.7, it will be useful for us to fix bases of the $\mathrm{Sym}^j V \otimes \mathbf{F}_p(i)$ for i,j in the range of Theorem 3.1.6 so that we can view $\mathrm{Gal}(M/\mathbf{Q}) = A \rtimes G$ as an explicit matrix group. Furthermore, we would like these bases to be compatible with the quotient maps $\mathrm{Sym}^k V \to \mathrm{Sym}^{k-1} V$.

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 $\mathrm{Sym}^k V$ 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, $\binom{j-1}{i-1} b^{j-i}$.

We can rescale this basis so that the image of the representation $\mathrm{Sym}^k V$ is the matrix group

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

This map $G \to \mathrm{GL}_{k+1}(\mathbf{F}_p)$ factors through the group U_{k+1} of upper-triangular matrices. Similarly, $\mathrm{Sym}^{k-1} V$ gives a map $G \to U_k$. There is also a projection $U_{k+1} \to U_k$ given by "forget the first row and column", and the bases above are chosen so that the triangle

$$\begin{tikzcd} & U_{k+1} \arrow[dd] \\ G \arrow[ur] \arrow[dr] & \\ & U_k \end{tikzcd}$$

commutes.

If $E = \mathbf{Q}(N^{1/p}, \zeta_N^{(p)})$ is the genus field, we instead consider the representation $G_{\mathbf{Q},S} \to \mathrm{GL}_2(\mathbf{F}_p)$ of the form

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

where $c \in \mathrm{Hom}(G_{\mathbf{Q},S}, \mathbf{F}_p) = H^1_S(\mathbf{F}_p)$ is the class defining the extension $\mathbf{Q}(\zeta_N^{(p)})/\mathbf{Q}$.

Remark 3.1.9. 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 $\mathrm{Cl}_{K(\zeta_p)}$. The results above can then be viewed through the lens of decomposing this class group into a sum of indecomposable $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q})$-representations, similar to classical results on decomposing the p part of $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}$ into a sum of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$-representations. In Section 5 we will see that the numbers M_i defined in Section 1 play a similar role to that of the Bernoulli numbers in the structure of $\mathrm{Cl}_{\mathbf{Q}(\zeta_p)}$.

The structure of $\mathrm{Cl}_{K(\zeta_p)}$ as a Galois module was also studied by Iimura in [4]. The connection between Iimura's work and our current approach is discussed in slightly more detail in Remark 3.2.4.

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 no larger than p. We will show directly that $m \neq p, p-1$.

Lemma 3.1.10. *$m \neq p$.*

Proof. Suppose that $m = p$. The lower 2×2 corner of the matrix $(**)$ will thus be

$$\begin{pmatrix} 1 & a_{p-1} \\ 0 & 1 \end{pmatrix}$$

which we think of as a quotient of $\mathrm{Gal}(M/\mathbf{Q})$ (alternatively, as a new $G_{\mathbf{Q},S}$-representation with $G_{M,S}$ in the kernel). This gives us a class $a_{p-1} \in H^1_S(\mathbf{F}_p)$, and it cuts out a $\mathbf{Z}/p\mathbf{Z}$ extension L of $\mathbf{Q}$ 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. We begin by considering the behavior at p. Consider the diagram of fields

$$\begin{tikzcd}
 & LK(\zeta_p) \arrow[dl, dash] \arrow[dr, dash] & \\
K(\zeta_p) \arrow[dr, dash] & & L(\zeta_p) \arrow[dl, dash] \arrow[d, dash] \\
 & \mathbf{Q}(\zeta_p) \arrow[d, dash] & L \arrow[dl, dash] \\
 & \mathbf{Q} &
\end{tikzcd}$$

locally at p. As $L \subseteq M$ we know that $LK(\zeta_p)/K(\zeta_p)$ is unramified at p. Applying Lemma 3.1.4, we conclude that $L(\zeta_p)/\mathbf{Q}(\zeta_p)$, and hence $L/\mathbf{Q}$, is also unramified at p.

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

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

Raising this to the pth power, we see that the top-right entry of the image of τ^p is $b(\tau)^{p-1}a_{p-1}(\tau)$. But this is nonzero, contradicting the fact that the generator of the inertia group at N has order p. □

Lemma 3.1.11. *$m \neq p-1$.*

Proof. The lower 2×2 corner of the matrix $(**)$ will thus be

$$\begin{pmatrix} \chi & a_{p-2} \\ 0 & 1 \end{pmatrix}$$

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

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

of the matrix $(**)$, so a_{p-2} must be a multiple of b by Proposition 2.4.3. This gives that $a_{p-2} = 0$, but then $\dim_{\mathbf{F}_p}(A) \le p-2$ 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 $\mathbf{F}_p$-extension E/K of type m a representation $G_{\mathbf{Q},S} \to \mathrm{GL}_{m+1}(\mathbf{F}_p)$ of the form $(**)$. As a representation, it is an extension of the trivial representation by $\mathrm{Sym}^{m-1}V \otimes \mathbf{F}_p(1-m)$ considered as a $G_{\mathbf{Q},S}$-representation via the quotient $G_{\mathbf{Q},S} \to G$, so it gives a class

$$a_E = \begin{bmatrix} a_0 \\ \vdots \\ a_{m-1} \end{bmatrix} \in H^1_S(\mathrm{Sym}^{m-1}V \otimes \mathbf{F}_p(1-m))$$

as discussed in Section 2.1.

Let Λ be the Selmer condition defined by

- $L_\ell = H^1_{\mathrm{ur}}(G_{\mathbf{Q}_\ell}, A)$ for $\ell \neq N, p$
- $L_N = H^1(G_{\mathbf{Q}_N}, A)$
- $L_p = \mathrm{res}^{-1}(H^1_{\mathrm{ur}}(G_{K(\zeta_p)_p}, A))$ where res is the restriction map

$$H^1(G_{\mathbf{Q}_p}, A) \to H^1(G_{K(\zeta_p)_p}, A).$$

Remark 3.2.1. In the case $A = \mathbf{F}_p$, the containment $H^1_N(\mathbf{F}_p) \subseteq H^1_\Lambda(\mathbf{F}_p)$ is an equality. This is to say that any $\mathbf{F}_p$-extension $L/\mathbf{Q}$ unramified away from S and unramified at p after base change to $K(\zeta_p)$ was necessarily unramified at p over $\mathbf{Q}$. This follows from Lemma 3.1.4 as in the end of the proof of Proposition 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 $\mathrm{Gal}(M/K(\zeta_p))$, one has $H^1_N(A) = H^1_\Lambda(A)$; this follows from Lemma 3.3.5. However, if one wants to use the methods of this section to study $\mathrm{Cl}_{K(\zeta_p)}$ or the case of composite N, it is necessary to use modules A for which $H^1_N(A) \neq H^1_\Lambda(A)$.

In this subsection we prove

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

The main step in the proof of this theorem is to show that the class a_E lies in the Λ-Selmer subgroup $H^1_\Lambda(\mathrm{Sym}^{m-1}V \otimes \mathbf{F}_p(1-m))$ and conversely that any such Selmer class arises from an unramified $\mathbf{F}_p$-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. The proof of Theorem 3.2.2 comes down to establishing a bijection between the projectivized space $\mathbf{P}H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$ and the set of unramified $\mathbf{F}_p$-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 $H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$, consider the natural filtration on the module $\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2) = \mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(3-p)$ given by

$$\begin{aligned} 0 \subseteq \mathbf{F}_p &= \mathrm{Sym}^0 V \otimes \mathbf{F}_p(0) \\ &\subseteq \mathrm{Sym}^1 V \otimes \mathbf{F}_p(-1) \\ &\subseteq \mathrm{Sym}^2 V \otimes \mathbf{F}_p(-2) \\ &\subseteq \cdots \\ &\subseteq \mathrm{Sym}^{p-3} V \otimes \mathbf{F}_p(3-p). \end{aligned}$$

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

$$\frac{\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k)}{\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(1-k)} \cong \mathbf{F}_p(-k).$$

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

$$\begin{aligned} 0 \subseteq H^1_S(\mathbf{F}_p) &\subseteq H^1_S(\mathrm{Sym}^1 V \otimes \mathbf{F}_p(-1)) \\ &\subseteq H^1_S(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-2)) \\ &\subseteq \cdots \\ &\subseteq H^1_S(\mathrm{Sym}^{p-3} V \otimes \mathbf{F}_p(3-p)) \end{aligned}$$

where each inclusion can be realized concretely via

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

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 in $H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$, defined up to a scalar, as desired.

Conversely, given a nonzero class $a \in H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$, we can restrict it to a class in $G_{K,S}$-cohomology to get a representation of $G_{K,S}$ of the form

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

From this we see that $a_0|_{G_{K,S}}$ is a homomorphism $G_{K,S} \to \mathbf{F}_p$. 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, the fixed field of $\ker(a_0|_{G_{K,S}})$, denoted E_a, is an $\mathbf{F}_p$-extension of K.

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

Proof. We will show the equivalent statement that $a_0|_{G_{K(\zeta_p),S}}$ is nonzero. Let A be $\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2)$ and consider the inflation-restriction sequence

$$0 \to H^1(G, A) \to H^1(G_{\mathbf{Q},S}, A) \to H^1(G_{K(\zeta_p),S}, A)^G.$$

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

$$H^1(G, A) \cong H^1(\mathbf{Z}/p\mathbf{Z}, A)^{(\mathbf{Z}/p\mathbf{Z})^\times}.$$

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

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

Therefore, a nonzero $a \in H^1(G_{\mathbf{Q},S}, A)$ restricts to a nonzero homomorphism $G_{K(\zeta_p),S} \to A = \mathbf{F}_p^{p-2}$ 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 Λ guarantees that this extension E_a/K is unramified everywhere. This is obvious for all $\ell \neq N, p$.

At N, Proposition 2.2.2 shows that $H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))$ is 2-dimensional, spanned by an unramified class and the class corresponding to K_N, so the image of any class here in $H^1(G_{K_N}, \mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))$ 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 $E_a(\zeta_p)/K(\zeta_p)$ 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 E_{a_E} is the unique $\mathbf{F}_p$-subextension of M/K such that $\mathrm{Gal}(K(\zeta_p)/K) = (\mathbf{Z}/p\mathbf{Z})^\times$ acts trivially on $\mathrm{Gal}(E_{a_E}(\zeta_p)/K(\zeta_p))$. But E satisfies this last property as well, and thus $E = E_{a_E}$.

Conversely, take any two cohomology classes $a, a' \in H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$ 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 $H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$ from the perspective of the types m of the extensions E/K. Under the correspondence used to prove Theorem 3.2.2, the subspace $H^1_\Lambda(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))$ contains the E of type $m \leq k+1$, and the quotient

$$\frac{H^1_\Lambda(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))}{H^1_\Lambda(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(1-k))}$$

is nonzero exactly when there is an E/K of type $k+1$.

In [4], Iimura defines a descending filtration on the p-part of $A = \mathrm{Cl}_{K(\zeta_p)}$ by considering it as a $\mathbf{F}_p[G]$-module. Let $\sigma \in G$ be order p. The ith 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 $(\mathbf{Z}/p\mathbf{Z})^\times$-coinvariants of J_0/J_k give extensions E/K of type $m \leq k$, and that quotients of the $(\mathbf{Z}/p\mathbf{Z})^\times$-coinvariants of J_{m-1}/J_m give extensions E/K of type exactly m. This realizes Iimura's filtration as the "dual" to our filtration on $H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$.

Remark 3.2.5. Recall that if $c_j \in H^1(G, \mathbf{F}_p(i_j))$ for $1 \leq j \leq k$, then the k-fold Massey product $\langle c_1, \dots, c_k\rangle$ is a subset of $H^2(G, \mathbf{F}_p(\sum_{j=1}^k i_j))$ that contains 0 if and only if there is an upper-triangular $\mathbf{F}_p$-representation of G whose image has powers of χ on the diagonal and the cocycles c_i on the upper-diagonal. For example, the matrix $(**)$ witnesses the vanishing of the Massey product $\langle b, \dots, b, a_{m-1}\rangle$.

In [9], Sharifi works in an Iwasawa-theoretic situation and relates the inverse limit of class groups to the inverse limits of Massey products. In broad terms, his Theorem A estabishes an isomorphism between the kth graded piece of an Iimura-like filtration and the quotient of another group by inverse limits of $(k+1)$-fold Massey products of the form $\langle b, \dots, b, a\rangle$. That is, "if more Massey products vanish, then the kth piece of Iimura's filtration is larger", which is consistent with the themes of this section.

3.3. **An Exact Sequence of Selmer Groups.**

The goal of this subsection is to provide some motivation for the definitions of the Selmer conditions Σ and Σ^* and to prove the following proposition:

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

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

In particular,

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

The last equality follows from the $k = p-3$ case of the first part of the proposition combined with part 1 of Theorem 2.3.3, which gives that $h^1_N(\mathbf{F}_p) = 1$.

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

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

$\mathrm{Sym}^{k-1}V \otimes \mathbf{F}_p(-k)$ has no $G_{\mathbf{Q},S}$-fixed points, so taking $G_{\mathbf{Q},S}$-cohomology gives that the top row of the following commutative diagram is exact.

$$\begin{tikzcd}
0 \arrow[r] & H^1_S(\mathbf{F}_p) \arrow[r] & H^1_S(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k)) \arrow[r] & H^1_S(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(-k)) & \\
0 \arrow[r] & H^1_N(\mathbf{F}_p) \arrow[r] \arrow[u, hook] & H^1_\Lambda(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k)) \arrow[r, dashed] \arrow[u, hook] & H^1_\Sigma(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(-k)) \arrow[r] \arrow[u, hook] & 0
\end{tikzcd}$$

To prove Proposition 3.3.1, we need to show:

(1) The image of $H^1_\Lambda(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))$ in $H^1_S(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(-k))$ is contained in the Selmer subgroup $H^1_\Sigma(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(-k))$.
(2) The induced map $H^1_\Lambda(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k)) \to H^1_\Sigma(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(-k))$ is surjective.
(3) The kernel of this induced map is precisely $H^1_N(\mathbf{F}_p) \subseteq H^1_S(\mathbf{F}_p)$.

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

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 Λ replaced by S and Σ replaced by Σ^* by considering the local condition at N. To get the corresponding statements for Λ and Σ, we need to consider the local conditions at p, which is done in Lemmas 3.3.4 and 3.3.5.

Lemma 3.3.2 is stated in slightly more generality than we presently need. To establish Proposition 3.3.1, we only need the case $i = j$. The full strength of this lemma is used in Section 4 when we discuss issues of extending Galois representations of this kind.

Lemma 3.3.2. *For any $1 \leq i \leq p-3$, and $0 \leq j \leq i$, the image of*

$$H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)) \to H^1_S(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$$

is contained in $H^1_{\Sigma^*}(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$. If in addition we assume that p is regular or that $i = j$, then the image is precisely $H^1_{\Sigma^*}(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$.

Remark 3.3.3. The second statement in the proposition is equivalent to the following statement: A $G_{\mathbf{Q},S}$-representation of dimension $j+1$, coming from an element $a \in H^1_S(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$, of the form

$$\begin{pmatrix} \chi^{j-1-i} & \chi^{j-2-i} b & \cdots & \chi^{-i} \frac{b^{j-1}}{(j-1)!} & a_{i-(j-1)} \\ & \chi^{j-2-i} & \cdots & \chi^{-i} \frac{b^{j-2}}{(j-2)!} & a_{i-(j-2)} \\ & & \ddots & \vdots & \vdots \\ & & & \ddots \quad \chi^{-i} b & a_{i-1} \\ & & & \chi^{-i} & a_i \\ & & & & 1 \end{pmatrix}$$

extends to a $G_{\mathbf{Q},S}$-representation of dimension $j+2$ of the form

$$\begin{pmatrix} \chi^{j-i} & \chi^{j-1-i} b & \cdots & \chi^{-i} \frac{b^{j}}{j!} & * \\ & \chi^{j-1-i} & \cdots & \chi^{-i} \frac{b^{j-1}}{(j-1)!} & a_{i-(j-1)} \\ & & \ddots & \vdots & \vdots \\ & & & \ddots \quad \chi^{-i} b & a_{i-1} \\ & & & \chi^{-i} & a_i \\ & & & & 1 \end{pmatrix}$$

if and only if $a \in H^1_{\Sigma^*}(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$.

Proof of Lemma 3.3.2. The exact sequence

$$0 \to \mathbf{F}_p(j-i) \to \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i) \to \mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i) \to 0$$

induces the commutative diagram

$$\begin{tikzcd} H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)) \arrow[r] \arrow[d] & H^1_S(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i)) \arrow[r] \arrow[d] & H^2_S(\mathbf{F}_p(j-i)) \arrow[d] \\ H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^j V) \arrow[r] & H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^{j-1} V) \arrow[r] & H^2(G_{\mathbf{Q}_N}, \mathbf{F}_p). \end{tikzcd}$$

We are concerned with the image of the first map in the top row, which is the kernel of the second map in that row. This boundary map is given by taking the cup product with the class $\tilde{\mathbf{b}}$ in

$$H^1_S(\mathbf{F}_p(j-i) \otimes (\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))^\vee)$$

that realizes $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ as an extension of $\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i)$ by $\mathbf{F}_p(j-i)$. Locally at N, all of the present modules are self-dual by Lemma 2.2.1 and thus we might as well think of $\mathrm{Sym}^j V$ as an extension of $\mathbf{F}_p$ by $\mathrm{Sym}^{j-1} V$. The corresponding class in $H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^{j-1} V)$ giving this extension is the column vector $\mathrm{res}_N(\tilde{\mathbf{b}}) = \mathbf{b} = [\frac{b^j}{j!}, \cdots, \frac{b^2}{2}, b]^T$ in the notation of Proposition 2.2.2.

That is,

$$\mathrm{im}(H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)) \to H^1_S(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i)))$$

is equal to

$$\{a \in H^1_S(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i)) \mid a \cup \tilde{\mathbf{b}} = 0\}.$$

Noting that $\tilde{\mathbf{b}}$ satisfies the Σ^*-Selmer condition and that $\mathrm{res}_N(\tilde{\mathbf{b}}) \neq 0$, Proposition 2.4.3 then gives that the latter set is contained in $H^1_{\Sigma^*}(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$, and that this containment is an equality if p is regular or if $j - i = 0$. □

Lemma 3.3.4. *Let $1 \leq k \leq p-3$. Let $a \in H^1_\Sigma(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(-k))$ and assume that a has a lift to $H^1_S(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))$. Then a has a lift to $H^1_\Lambda(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))$.*

Proof. Write $a = [a_1, \ldots, a_k]^T$. Choose any lift of a to $H^1_S(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))$, and write it as $[a_0, a_1, \ldots, a_k]^T$. By assumption, $a_i|_{G_{\mathbf{Q}_p}} = 0$ 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 $K(\zeta_p)_p$.

It can in fact be chosen to be unramified over $\mathbf{Q}_p$. The fact that the a_i for $i \geq 1$ vanish when restricted to $G_{\mathbf{Q}_p}$ gives that $a_0|_{G_{\mathbf{Q}_p}}$ is a class in $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p)$. This is a 2-dimensional $\mathbf{F}_p$-vector space, spanned by an unramified class and the class corresponding to $\mathbf{Q}_p(\zeta_{p^2}^{(p)})$. 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 3.3.5. *Let $1 \leq k \leq p-3$. Let a be any class*

$$a = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{bmatrix} \in H^1_\Lambda(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k)).$$

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

Proof. The proof is by strong induction on i, starting with a_k. Let M be the Galois extension of $\mathbf{Q}$ defined by the kernel of the representation associated to a. We begin by examining the $G_{\mathbf{Q},S}$-representation associated to the image of a in

$H^1_S(\mathrm{Sym}^{k-1}V\otimes\mathbf{F}_p(-k))$:

$$\begin{pmatrix}\chi^{-1} & \chi^{-2}b & \chi^{-3}\frac{b^2}{2} & \cdots & \chi^{-k}\frac{b^{k-1}}{(k-1)!} & a_1\\ & \chi^{-2} & \chi^{-3}b & \cdots & \chi^{-k}\frac{b^{k-2}}{(k-2)!} & a_2\\ & & \ddots & & \vdots & \vdots\\ & & & \chi^{1-k} & \chi^{-k}b & a_{k-1}\\ & & & & \chi^{-k} & a_k\\ & & & & & 1\end{pmatrix}$$

Restrict this representation to $G_{\mathbf{Q}_p}$. Looking at the bottom 2×2 quotient, we notice that $a_k|_{G_{\mathbf{Q}_p}}$ gives an extension $L_k/\mathbf{Q}_p(\zeta_p)$ contained in M_p. If it is nontrivial, its Galois group is $\mathbf{F}_p(-k)$ as a $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$-module. Since a satisfies the Selmer condition Λ, $L_kK(\zeta_p)_p/K(\zeta_p)_p$ is unramified. As $-k\neq 1 \bmod p-1$, Lemma 3.1.4 then applies to conclude that $L_k/\mathbf{Q}_p(\zeta_p)$ is unramified. Equivalently, $a_k|_{G_{\mathbf{Q}_p}}$ lies in $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p},\mathbf{F}_p(-k))$ which is trivial as $k\neq 0 \bmod p-1$. (Indeed, the unique unramified $\mathbf{F}_p$-extension of $\mathbf{Q}_p(\zeta_p)$ is abelian over $\mathbf{Q}_p$, and thus does not correspond to a class in $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p},\mathbf{F}_p(-k))$.)

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

$$\begin{pmatrix}\chi^{1-k} & \chi^{-k}b & a_{k-1}\\ & \chi^{-k} & 0\\ & & 1\end{pmatrix}.$$

Thus $a_{k-1}\in H^1(G_{\mathbf{Q}_p},\mathbf{F}_p(1-k))$ and so defines an extension $L_{k-1}/\mathbf{Q}_p(\zeta_p)$. If it is non trivial, it has an action of $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$ by χ^{1-k}. As above, the extension $L_{k-1}K(\zeta_p)_p/K(\zeta_p)_p$ is unramified, so we conclude that

$$a_{k-1}\in H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p},\mathbf{F}_p(1-k))=0.$$

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 $\chi^{i-k}\neq\chi$ so that Lemma 3.1.4 applies, and that χ^{i-k} is nontrivial so that $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p},\mathbf{F}_p(i))=0$.

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. **$\mathbf{Cl}_K$ and Selmer Groups of Characters.** Recall the filtration by type on $H^1_\Lambda(\mathrm{Sym}^{p-3}V\otimes\mathbf{F}_p(2))$ considered in Remark 3.2.4. As a corollary to Proposition 3.3.1, we conclude that this filtration descends to a filtration

$$\begin{aligned}0 &\subseteq H^1_\Sigma(\mathbf{F}_p(-1))\\ &\subseteq H^1_\Sigma(\mathrm{Sym}^1V\otimes\mathbf{F}_p(-2))\\ &\subseteq H^1_\Sigma(\mathrm{Sym}^2V\otimes\mathbf{F}_p(-3))\\ &\subseteq\cdots\\ &\subseteq H^1_\Sigma(\mathrm{Sym}^{p-4}V\otimes\mathbf{F}_p(2)).\end{aligned}$$

In the spirit of Remark 3.2.4, we think of the kth piece $H^1_\Sigma(\mathrm{Sym}^{k-1}V\otimes\mathbf{F}_p(-k))$ in the above filtration as corresponding to those E/K of type $2\leq m\leq k+1$, and the quotient

$$\frac{H^1_\Sigma(\mathrm{Sym}^{k-1}V\otimes\mathbf{F}_p(-k))}{H^1_\Sigma(\mathrm{Sym}^{k-2}V\otimes\mathbf{F}_p(1-k))}$$

as corresponding to the extensions of type exactly $k+1$, in the sense that its dimension is the number of inequivalent 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. $h^1_\Sigma(\mathbf{F}_p(-1)) \le h^1_\Sigma(\mathrm{Sym}^{p-4}V \otimes \mathbf{F}_p(2))$.
2. *If there is an E/K is of type $m \ge 2$, then $H^1_\Sigma(\mathbf{F}_p(1-m))$ is nontrivial.*
3. $h^1_\Sigma(\mathrm{Sym}^{p-4}V \otimes \mathbf{F}_p(2)) \le \sum_{i=1}^{p-3} h^1_\Sigma(\mathbf{F}_p(-i))$.

Proof. The first part of the proposition follows from the fact that the smallest piece in the above filtration is

$$H^1_\Sigma(\mathbf{F}_p(-1)) \subseteq H^1_\Sigma(\mathrm{Sym}^{p-4}V \otimes \mathbf{F}_p(2)).$$

Now, take the exact sequence

$$0 \to \mathrm{Sym}^{k-2}V \otimes \mathbf{F}_p(1-k) \to \mathrm{Sym}^{k-1}V \otimes \mathbf{F}_p(-k) \to \mathbf{F}_p(-k) \to 0$$

and look at the Σ-Selmer subgroups of the long exact sequence in $G_{\mathbf{Q},S}$-cohomology to get the exact sequence

$$0 \to H^1_\Sigma(\mathrm{Sym}^{k-2}V \otimes \mathbf{F}_p(1-k)) \to H^1_\Sigma(\mathrm{Sym}^{k-1}V \otimes \mathbf{F}_p(-k)) \to H^1_\Sigma(\mathbf{F}_p(-k)).$$

Thus

$$\frac{H^1_\Sigma(\mathrm{Sym}^{k-1}V \otimes \mathbf{F}_p(-k))}{H^1_\Sigma(\mathrm{Sym}^{k-2}V \otimes \mathbf{F}_p(1-k))} \subseteq H^1_\Sigma(\mathbf{F}_p(-k))$$

which establishes the second part of the proposition: if there is an E/K is of type m then $H^1_\Sigma(\mathbf{F}_p(1-m))$ is nonzero, 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 $H^1_\Sigma(\mathrm{Sym}^{p-4}V \otimes \mathbf{F}_p(2))$ equipped with this filtration is

$$\begin{aligned}\mathrm{gr}(H^1_\Sigma(\mathrm{Sym}^{p-4}V \otimes \mathbf{F}_p(2))) &= \bigoplus_{k-1}^{p-3} \frac{H^1_\Sigma(\mathrm{Sym}^{k-1}V \otimes \mathbf{F}_p(-k))}{H^1_\Sigma(\mathrm{Sym}^{k-2}V \otimes \mathbf{F}_p(1-k))} \\ &\subseteq \bigoplus_{k=1}^{p-3} H^1_\Sigma(\mathbf{F}_p(-k))\end{aligned}$$

which proves the final part of the proposition. □

4. Lifting Selmer Classes

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

$$r_K \overset{?}{=} 1 + \sum_{i=1}^{p-3} h^1_\Sigma(\mathbf{F}_p(-i)).$$

In Section 6.2, we show that this is true when $p=5$. However, it is not true in general. In particular, see Section 6.3 for a detailed analysis of the possible cases when $p=7$.

We have seen in Section 3 that given an unramified $\mathbf{F}_p$-extension E/K of type $m>1$, we get a $G_{\mathbf{Q},S}$-representation of dimension $m+1$ whose image is isomorphic to the Galois group $\mathrm{Gal}(M/\mathbf{Q})$ where M is the Galois closure of $E/\mathbf{Q}$. This gives a class in $H^1_\Sigma(\mathrm{Sym}^{m-2}V \otimes \mathbf{F}_p(1-m))$ whose image in the quotient $H^1_\Sigma(\mathbf{F}_p(1-m))$ is nonzero.

This section will tackle the converse to this construction, namely by providing criteria for when a nonzero class a_i in $H^1_\Sigma(\mathbf{F}_p(-i))$ may be lifted to an element in $H^1_\Sigma(\mathrm{Sym}^{i-1}V \otimes \mathbf{F}_p(-i))$, as such a lift gives a representation of the form $(**)$ by Proposition 3.3.1, which corresponds to an extension E/K of type $i+1$. We consider two separate methods, one in each of Sections 4.1 and 4.2.

It is worth remarking that in the case $i = 1$, there are no obstructions to worry about: The class $a_1 \in H^1_\Sigma(\mathbf{F}_p(-1))$ lifts directly to a class in $H^1_\Lambda(\mathrm{Sym}^1 V \otimes \mathbf{F}_p(-1))$ which gives an extension E/K of type 2. (This is the $k = 1$ case of Proposition 3.3.1, or equivalently the first part of Proposition 3.4.1.) This is the method that Wake–Wang-Erickson use to prove the lower bound in Theorem 3.0.1, which they state as the following proposition.

Proposition 4.0.1 ([12], Proposition 11.1.1)**.** *If $h^1_\Sigma(\mathbf{F}_p(-1)) \neq 0$ then $r_K \geq 2$.*

Remark 4.0.2. The question of lifting representations is related to the vanishing of higher Massey products $\langle b, \ldots, b, a_i \rangle$ in $G_{\mathbf{Q},S}$-cohomology. In [9], Sharifi has shown that certain higher Massey products of this type vanish in $G_{\mathbf{Q}}$-cohomology.

For example, one way of interpreting the results of Section 4.2 is in terms of the vanishing of certain triple Massey products in $G_{\mathbf{Q},S}$-cohomology. Theorem 4.2.1 could be restated as saying that the triple $G_{\mathbf{Q},S}$-Massey product $\langle b, b, a \rangle$ vanishes, where a is a class that spans $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$.

4.1. **Climbing the Ladder.** We approach the problem of lifting the classes in $H^1_\Sigma(\mathbf{F}_p(-i))$ one dimension at a time. Namely, we will give a sequence of lemmas which provide criteria for when a class in $H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$ may be lifted "one rung up the ladder" to a class in $H^1_\Sigma(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$, for $1 \leq 1 \leq p-2$ and $1 \leq j \leq i-1$. Lemma 3.3.2 shows that one obstruction to this lifting is the irregularity of p. Therefore we assume for simplicity for the remainder of this section that p is regular. Given this assumption, Lemma 3.3.2 tells us that every class in $H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(i))$ in the range of j and i we consider has a lift to $H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$, so we are tasked with showing that there are lifts which satisfy the local conditions of the Selmer condition Σ.

Our strategy is as follows. Recall the short exact sequence of $G_{\mathbf{Q},S}$-modules

$$0 \to \mathbf{F}_p(j-i) \to \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i) \to \mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i) \to 0$$

which induces the following piece of the long exact sequence in $G_{\mathbf{Q},S}$-cohomology

$$0 \to H^1_S(\mathbf{F}_p(j-i)) \to H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)) \to H^1_S(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$$

as $H^0(G_{\mathbf{Q},S}, \mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i)) = 0$ for the i and j considered.

Thus, if a is a fixed class in $H^1_{\Sigma^*}(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$ which has a lift $\tilde{a}$ to $H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$, we may modify $\tilde{a}$ by adding classes in $H^1_S(\mathbf{F}_p(j-i))$ in an attempt to produce others lifts of a which satisfy the local conditions of Σ. The following lemmas give conditions for when such modification is possible.

Lemma 4.1.1. *Let p be regular. Suppose that $a \in H^1_{\Sigma^*}(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$, and that*

$$h^1_{\Sigma^*}(\mathbf{F}_p(j-i)) < h^1_S(\mathbf{F}_p(j-i))$$

Then there is a lift of a to $H^1_{\Sigma^*}(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$.

Proof. The proof is essentially a diagram chase. Consider the following commutative diagram. For space considerations, we abbreviate $\mathrm{Sym}^a V \otimes \mathbf{F}_p(b)$ as $V^a(b)$.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & H^1_{\Sigma*}(\mathbf{F}_p(j-i)) \arrow[d] & H^1_{\Sigma^*}(V^j(-i)) \arrow[d] \arrow[dr, dashed] & & \\
0 \arrow[r] & H^1_S(\mathbf{F}_p(j-i)) \arrow[r] \arrow[d] \arrow[dr, dashed] & H^1_S(V^j(-i)) \arrow[r] \arrow[d] & H^1_{\Sigma^*}(V^{j-1}(-i)) \arrow[r] & 0 \\
 & H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p(j-i))/\langle b \rangle \arrow[r, "\sim"] & H^1(G_{\mathbf{Q}_N}, V^j(-i))/\langle \mathbf{b} \rangle & &
\end{tikzcd}$$

The middle row is exact by Lemma 3.3.2, and Proposition 2.2.2 gives that the bottom arrow is an isomorphism and that the two groups are both 1-dimensional, as well as the fact that the two columns are exact.

The lemma is equivalent to the statement that the top-right diagonal arrow

$$H^1_{\Sigma^*}(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)) \to H^1_{\Sigma^*}(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$$

is surjective. We first claim that this is implied by the surjectivity of the bottom-left diagonal arrow

$$H^1_S(\mathbf{F}_p(j-i)) \to H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))/\langle \mathbf{b} \rangle.$$

Indeed, suppose that diagonal map is surjective and let $\tilde{a}$ be any lift of a to $H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$. Let c be any class in $H^1_S(\mathbf{F}_p(j-i))$ whose image in $H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))/\langle \mathbf{b} \rangle$ is equal to the image of $\tilde{a}$. Then $\tilde{a} - c$ is a lift of a that lies in $H^1_{\Sigma^*}(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$.

We are reduced to showing that the bottom-left diagonal arrow is surjective. Because the bottom horizontal arrow is an isomorphism, it suffices to show that the vertical map

$$H^1_S(\mathbf{F}_p(j-i)) \to H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p)/\langle b \rangle$$

is surjective. As the latter group is 1-dimensional, we just need to show that this map is nonzero, which follows from the assumption

$$h^1_{\Sigma^*}(\mathbf{F}_p(j-i)) < h^1_S(\mathbf{F}_p(j-i)).$$ □

Lemma 4.1.2. *Let p be regular. Suppose that $a \in H^1_\Sigma(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$ where $j - i \neq 0, 1 \bmod p-1$, and that*

$$h^1_N(\mathbf{F}_p(j-i)) < h^1_S(\mathbf{F}_p(j-i)).$$

Then there is a lift of a to $H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$ which is trivial when restricted to $G_{\mathbf{Q}_p}$.

Proof. The argument is similar to the previous one. Let H be the preimage of $H^1_\Sigma(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$ under the map

$$H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)) \to H^1_{\Sigma^*}(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i)).$$

We will reference the following diagram, where the local condition "split at p" is abbreviated "spl p". Because $j - i \neq 0 \bmod p-1$, we have $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p}, \mathbf{F}_p(j-i)) = 0$, and thus $H^1_N(\mathbf{F}_p(j-i)) = H^1_{\text{spl } p}(\mathbf{F}_p(j-i))$. As above, we abbreviate $\text{Sym}^a V \otimes \mathbf{F}_p(b)$ as $V^a(b)$.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & H^1_N(\mathbf{F}_p(j-i)) \arrow[d] & H^1_{\text{spl } p}(V^j(-i)) \arrow[d] \arrow[dr, dashed] & & \\
0 \arrow[r] & H^1_S(\mathbf{F}_p(j-i)) \arrow[r] \arrow[d] \arrow[dr, dashed] & H \arrow[r] \arrow[d] & H^1_\Sigma(V^{j-1}(-i)) \arrow[r] \arrow[d, "0"] & 0 \\
 & H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(j-i)) \arrow[r] & H^1(G_{\mathbf{Q}_p}, V^j(-i)) \arrow[r, "\phi"] & H^1(G_{\mathbf{Q}_p}, V^{j-1}(-i)) &
\end{tikzcd}$$

We first remark that this diagram makes sense: Each of $H^1_{\text{spl } p}(\text{Sym}^j V \otimes \mathbf{F}_p(-i))$ and $H^1_S(\mathbf{F}_p(j-i))$ lands in H under its respective map to $H^1_S(\text{Sym}^j V \otimes \mathbf{F}_p(-i))$. Note that the middle row is exact by Lemma 3.3.2 and the two columns are exact by definition. Similarly, the vertical map in the final column is 0.

As in the proof of Lemma 4.1.1, we want to show that the top-right diagonal map is surjective. Note that the image of the bottom-left diagonal arrow is contained in the kernel of ϕ. We first argue that if this map surjects onto $\ker \phi$, then the top-right diagonal map is surjective as well.

Indeed, suppose that the diagonal map

$$H^1_S(\mathbf{F}_p(j-i)) \to \ker \phi$$

is surjective and let $a \in H^1_\Sigma(\text{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$. Choose any lift $\tilde{a}$ of a to H and let $\overline{a}$ be the image of $\tilde{a}$ in $H^1(G_{\mathbf{Q}_p}, \text{Sym}^j V \otimes \mathbf{F}_p(-i))$. Since the right-hand vertical map is 0, we know that $\overline{a} \in \ker \phi$. If $c \in H^1_S(\mathbf{F}_p(j-i))$ is a class whose image in $\ker \phi$ under the diagonal map is $\overline{a}$, then $\tilde{a} - c$ is a lift of a that lies in $H^1_{\text{spl } p}(\text{Sym}^j V \otimes \mathbf{F}_p(-i))$.

Now, because

$$\ker \phi = \text{im}(H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(j-i)) \to H^1(G_{\mathbf{Q}_p}, \text{Sym}^j V \otimes \mathbf{F}_p(-i))),$$

we are reduced to showing that the vertical map

$$H^1_S(\mathbf{F}_p(j-i)) \to H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(j-i))$$

is surjective.

Since $j - i \neq 0, 1 \bmod p-1$, we have that the latter group is 1-dimensional by the Local Euler Characteristic Formula, so the surjectivity of this map is equivalent to the map being nonzero. As the kernel of this map is $H^1_N(\mathbf{F}_p(j-i))$, this final statement follows from the assumption

$$h^1_N(\mathbf{F}_p(j-i)) < h^1_S(\mathbf{F}_p(j-i)). \qquad \square$$

Lemma 4.1.3. *Let p be regular. Suppose that $a \in H^1_\Sigma(\text{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$ where $j - i \neq 0, 1 \bmod p-1$, that there is a lift of a to $\in H^1_{\Sigma^*}(\text{Sym}^j V \otimes \mathbf{F}_p(-i))$, and that*

$$h^1_\Sigma(\mathbf{F}_p(j-i)) < h^1_{\Sigma^*}(\mathbf{F}_p(j-i)).$$

Then there is a lift of a to $\in H^1_\Sigma(\text{Sym}^j V \otimes \mathbf{F}_p(-i))$.

Proof. The argument is nearly identical to the one above. Let H' be the preimage of $H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$ under the map

$$H^1_{\Sigma^*}(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)) \to H^1_{\Sigma^*}(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i)).$$

Now, repeat the argument given in Lemma 4.1.2 in reference to the diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & H^1_\Sigma(\mathbf{F}_p(j-i)) \arrow[d] & H^1_\Sigma(V^j(-i)) \arrow[d] \arrow[rd, dashed] & & \\
0 \arrow[r] & H^1_{\Sigma^*}(\mathbf{F}_p(j-i)) \arrow[r] \arrow[d] \arrow[rd, dashed] & H' \arrow[r] \arrow[d] & H^1_\Sigma(V^{j-1}(-i)) \arrow[r] \arrow[d, "0"] & 0 \\
 & H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(j-i)) \arrow[r] & H^1(G_{\mathbf{Q}_p}, V^j(-i)) \arrow[r] & H^1(G_{\mathbf{Q}_p}, V^{j-1}(-i)) &
\end{tikzcd}$$

where, as before, $\mathrm{Sym}^a V \otimes \mathbf{F}_p(b)$ is abbreviated to $V^a(b)$. □

The final lemma of this section is just a concatenation of Lemmas 4.1.1 and 4.1.3. We state it as its own lemma for easier reference later.

Lemma 4.1.4. *Let p be regular. Suppose that $a \in H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$, and that*

$$h^1_\Sigma(\mathbf{F}_p(j-i)) < h^1_{\Sigma^*}(\mathbf{F}_p(j-i)) < h^1_S(\mathbf{F}_p(j-i)).$$

Then there is a lift of a to $H^1_\Sigma(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$.

As p is regular, the condition in Lemma 4.1.4 can only occur when $j-i$ is odd, $h^1_\Sigma(\mathbf{F}_p(j-i)) = 0$, and $h^1_{\Sigma^*}(\mathbf{F}_p(j-i)) = 1$; see Theorem 2.3.5.

Remark 4.1.5. The assumption that p is regular in each of the lemmas in this section could be replaced with the more general assumption that there exists a lift of $a \in H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$ to $H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$. We will not need that generality.

4.2. **Lifting Classes in $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$.** In this section we will prove that in a special case, some classes in a Σ-Selmer group of a character always lift to the Σ^*-Selmer group of a 2-dimensional representation. In particular we will be able to apply this result in situations where it is not possible to use Lemma 4.1.1 to show that a class lifts into a Σ^*-Selmer group. Our standing assumptions for this section will be that p is regular and $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2})) \neq 0$. In addition to ensuring that classes in $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$ always lift to $H^1_S(V(\frac{p-1}{2}))$ by Lemma 3.3.2, the regularity assumption provides access to the full strength of the results of Sections 2.3 and 2.4. Note that the character $\chi^{\frac{p-1}{2}}$ is its own inverse.

Theorem 4.2.1. *Assume that p is regular, and that $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2})) \neq 0$. If a class $a \in H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$ is nonzero, and if $\begin{bmatrix} a' \\ a \end{bmatrix}$ is any lift of a to $H^1_S(V(\frac{p-1}{2}))$, then $\begin{bmatrix} a' \\ a \end{bmatrix} \in H^1_{\Sigma^*}(V(\frac{p-1}{2}))$.*

The idea behind the proof of this theorem is to work with a related representation W which allows us to exploit the self-inverse property of $\chi^{\frac{p-1}{2}}$ to determine the Σ-Selmer group of a twist of W explicitly. Taken together with Theorem 2.1.2, we will be able to use this explicit determination of a Selmer group to get positive information about the local properties of the class $\begin{bmatrix} a' \\ a \end{bmatrix}$ (namely, that it is always in the Σ^*-Selmer group). We define the representation W that will be used, and then prove the theorem over the course of several lemmas.

We let W be the 2-dimensional $\mathbf{F}_p$-vector space on which $G_{\mathbf{Q},S}$ acts by

$$\begin{pmatrix} \chi^{\frac{p-1}{2}} & a \\ 0 & 1 \end{pmatrix}$$

where a is a nonzero class in $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$. By Proposition 2.4.3 we know that $b \cup a = 0$, hence a lifts to a class $\begin{bmatrix} a' \\ a \end{bmatrix} \in H^1_S(V(\frac{p-1}{2}))$. In other words there is a 3-dimensional representation of $G_{\mathbf{Q},S}$ (which is an extension of $\mathbf{F}_p$ by $V(\frac{p-1}{2})$) defined by

$$(\dagger) \qquad \begin{pmatrix} \chi^{\frac{p+1}{2}} & \chi^{\frac{p-1}{2}} b & a' \\ 0 & \chi^{\frac{p-1}{2}} & a \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that the representation $(\dagger)$ is also an extension of W by $\chi^{\frac{p+1}{2}}$. Taking the contragredient of the representation $(\dagger)$ and twisting by $\chi^{-\frac{p+1}{2}}$ yields another 3-dimensional representation of $G_{\mathbf{Q},S}$ defined by

$$(\ddagger) \qquad \begin{pmatrix} \chi^{\frac{p+1}{2}} & \chi a & ab - a' \\ 0 & \chi & -b \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that this representation is an extension of $\mathbf{F}_p$ by $W(1)$, which is to say that $\begin{bmatrix} ab - a' \\ -b \end{bmatrix} \in H^1_S(W(1))$.

Both 3-dimensional representations share the same kernel; the operation of taking contragredient and twisting by $\chi^{-\frac{p+1}{2}}$ doesn't change the kernel. Let $L/\mathbf{Q}$ be the fixed field of this kernel. We have a diagram of fields

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
K(\zeta_p) \arrow[dr, dash] & & L_a \arrow[dl, dash] \\
 & \mathbf{Q}(\zeta_p) \arrow[d, dash] & \\
 & \mathbf{Q} &
\end{tikzcd}$$

where L_a is the fixed field of the kernel of the representation W, which is Galois over $\mathbf{Q}$ with Galois group isomorphic to the semi-direct product $\mathbf{Z}/p\mathbf{Z} \rtimes (\mathbf{Z}/p\mathbf{Z})^\times$ where $(\mathbf{Z}/p\mathbf{Z})^\times$ acts by $\chi^{\frac{p-1}{2}}$. (This is the group $\Gamma_{\frac{p-1}{2}}$ in the notation of Theorem 3.1.6.) The representation $(\dagger)$ is a realization of $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q})$ acting on $\mathrm{Gal}(L/K(\zeta_p))$, whereas the representation $(\ddagger)$ is a realization of $\mathrm{Gal}(L_a/\mathbf{Q})$ acting on $\mathrm{Gal}(L/L_a)$.

This commonality between the representations (†) and (‡) and their associated cohomology classes $\begin{bmatrix} a' \\ a \end{bmatrix}$ and $\begin{bmatrix} ab-a' \\ -b \end{bmatrix}$ allows us to relate the local behavior of these classes.

Lemma 4.2.2. *The class* $\begin{bmatrix} a' \\ a \end{bmatrix}$ *is in* $H^1_{\Sigma^*}(V(\frac{p-1}{2}))$ *if and only if the class* $\begin{bmatrix} ab-a' \\ -b \end{bmatrix}$ *is in* $H^1_{\Sigma^*}(W(1))$.

Proof. Noting that a is necessarily a nonzero multiple of b locally at N by Remark 2.3.8, we see that $W(1)$ and $V(\frac{p-1}{2})$ 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 $V(\frac{p-1}{2})$ and $W(1)$, the Σ^* condition is just that classes vanish when restricted to K_N. Interpreting this in terms of the Galois extension $L/\mathbf{Q}$ cut out by both classes, we see that either class satisfies the Σ^* condition if and only if N is split in $L/L_aK(\zeta_p)$, as we know that locally at N the extension $L_aK(\zeta_p)$ is K_N. □

We will use the fact that $\chi^{\frac{p-1}{2}}$ is self-inverse to show that we have an equality $H^1_{\Sigma^*}(W(1)) = H^1_S(W(1))$, hence the equivalent statements of the previous lemma will always hold. Since we will be applying Theorem 2.1.2 to compute $h^1_{\Sigma^*}(W(1))$, we will need the fact that

$$W(1)^* \cong W(\tfrac{p-1}{2}).$$

We start by determining the dimensions of $H^1_S(W(1))$ and $H^1_S(W(\frac{p-1}{2}))$. As this result will depend on whether $p \equiv 1$ or $3 \bmod 4$ we will use the notation

$$s_p = \begin{cases} 1 & p \equiv 1 \bmod 4 \\ 0 & p \equiv 3 \bmod 4. \end{cases}$$

Lemma 4.2.3. *The classes generating* $H^1_S(W(1))$ *and* $H^1_S(W(\frac{p-1}{2}))$ *are as follows.*

(1) *We have that* $2 + s_p \le h^1_S(W(1)) \le 3 + s_p$. *The classes*

$$\begin{bmatrix} x \\ 0 \end{bmatrix}, \begin{bmatrix} * \\ b \end{bmatrix}$$

for $x \in H^1_S(\mathbf{F}_p(\frac{p+1}{2}))$ *always span a* $(2+s_p)$*-dimensional subspace. Let* b' *be the class of* p *in* $H^1_S(\mathbf{F}_p(1))$. *The dimension* $h^1_S(W(1))$ *is equal to* $3+s_p$ *if and only if* p *is a* p*th power modulo* N, *in which case the final dimension is spanned by some lift of* b',

$$\begin{bmatrix} * \\ b' \end{bmatrix}.$$

(2) *We have that* $3 \le h^1_S(W(\frac{p-1}{2})) \le 4$. *The classes*

$$\begin{bmatrix} y \\ 0 \end{bmatrix}, \begin{bmatrix} a^2/2 \\ a \end{bmatrix}$$

for $y \in H^1_S(\mathbf{F}_p)$ *span a* 3*-dimensional subspace, and* $h^1_S(W(\frac{p-1}{2})) = 4$ *if and only if* $p \equiv 3 \bmod 4$ *and* $H^1_{\Sigma^*}(\mathbf{F}_p(\frac{p-1}{2})) = H^1_S(\mathbf{F}_p(\frac{p-1}{2}))$. *In this case, if* z *is a class spanning* $H^1_p(\mathbf{F}_p(\frac{p-1}{2}))$ *then the final dimension is spanned by some lift of* z,

$$\begin{bmatrix} * \\ z \end{bmatrix}.$$

Proof. For the first part of this lemma, consider the following piece of the long exact sequence in $G_{\mathbf{Q},S}$-cohomology:

$$0 = H^0_S(\mathbf{F}_p(1)) \to H^1_S(\mathbf{F}_p(\tfrac{p+1}{2})) \to H^1_S(W(1)) \to H^1_S(\mathbf{F}_p(1)) \xrightarrow{a\cup -} H^2_S(\mathbf{F}_p(\tfrac{p+1}{2})).$$

The $1 + s_p$ dimensions of $H^1_S(\mathbf{F}_p(\frac{p+1}{2}))$ give classes in $H^1_S(W(1))$ immediately. The classes b, b', which span $H^1_S(\mathbf{F}_p(1))$ lift to $H^1_S(W(1))$ if and only if their cup product with a vanishes.

For the class b, we know that $a \cup b = 0$ by Proposition 2.4.3, as $a \in H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$. Since a is a nonzero multiple of b when viewed as a class for $G_{\mathbf{Q}_N}$, we have that $a \cup b' = 0$ if and only if b' is a multiple of b locally at N, again by Proposition 2.4.3. As b' is unramified at N, the only way for it to be a multiple of b locally at N is if N is split in the extension defined by b', which is $\mathbf{Q}(\zeta_p, p^{1/p})$. N splits in this extension if and only if p is a pth power in $\mathbf{Q}_N^\times$, which happens if and only if p is a pth power in $\mathbf{F}_N^\times$. Thus the class b' lifts to $H^1_S(W(1))$ if and only if p is a pth power modulo N.

The proof for the second part of the lemma is similar, using the long exact sequence for $W(\frac{p-1}{2})$:

$$0 = H^0_S(\mathbf{F}_p(\tfrac{p-1}{2})) \to H^1_S(\mathbf{F}_p) \to H^1_S(W(\tfrac{p-1}{2})) \to H^1_S(\mathbf{F}_p(\tfrac{p-1}{2})) \xrightarrow{a\cup -} H^2_S(\mathbf{F}_p).$$

The 2 dimensions of $H^1_S(\mathbf{F}_p)$ give classes in $H^1_S(W(\frac{p-1}{2}))$ immediately. The class a always lifts to $H^1_S(W(\frac{p-1}{2}))$, as we certainly have $a \cup a = 0$ as $a \in H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$. If $p \equiv 1 \bmod 4$, a spans $H^1_S(\mathbf{F}_p(\frac{p-1}{2}))$ and we conclude that $h^1_S(W(\frac{p-1}{2})) = 3$. If $p \equiv 3 \bmod 4$, let z be a class spanning $H^1_p(\mathbf{F}_p(\frac{p-1}{2}))$ (so a, z together necessarily span $H^1_S(\mathbf{F}_p(\frac{p-1}{2}))$ which is 2-dimensional, see part 2 of Theorem 2.3.5). We have by Proposition 2.4.3 that $a \cup z = 0$ if and only if $z \in H^1_{\Sigma^*}(\mathbf{F}_p(\frac{p-1}{2}))$, hence we conclude that z lifts to $H^1_S(W(\frac{p-1}{2}))$ if and only if $H^1_{\Sigma^*}(\mathbf{F}_p(\frac{p-1}{2})) = H^1_S(\mathbf{F}_p(\frac{p-1}{2}))$. □

Lemma 4.2.4. $H^1_{\Sigma^*}(W(1)) = H^1_S(W(1))$.

Proof. Applying Theorem 2.1.2 to $H^1_{\Sigma^*}(W(1))$ produces the relation:

$$h^1_{\Sigma^*}(W(1)) = 1 + s_p + h^1_\Sigma(W(\tfrac{p-1}{2})),$$

where we have used that $W \cong V$ as $G_{\mathbf{Q}_N}$-representations so Proposition 2.2.3 applies to the twists of W. We determine $h^1_\Sigma(W(\frac{p-1}{2}))$ explicitly based on our knowledge of the classes spanning it. Let c, c' be the classes spanning $H^1_S(\mathbf{F}_p)$, which correspond respectively to $\mathbf{Q}(\zeta_N^{(p)})$ and $\mathbf{Q}(\zeta_{p^2}^{(p)})$.

- the class $\begin{bmatrix} a^2/2 \\ a \end{bmatrix}$ is always in $H^1_\Sigma(W(\frac{p-1}{2}))$, since a itself is in $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$.
- the class $\begin{bmatrix} c' \\ 0 \end{bmatrix}$ is never in $H^1_\Sigma(W(\frac{p-1}{2}))$ as it is ramified at p.
- the class $\begin{bmatrix} c \\ 0 \end{bmatrix}$ is in $H^1_{\Sigma^*}(W(\frac{p-1}{2}))$ by Lemma 2.2.4, and is in $H^1_\Sigma(W(\frac{p-1}{2}))$ if and only if p is split in $\mathbf{Q}(\zeta_N^{(p)})$, which happens if and only if p is a pth power mod N, since $\mathrm{Gal}(\mathbf{Q}(\zeta_N^{(p)})/\mathbf{Q})$ is canonically $(\mathbf{Z}/N\mathbf{Z})^\times/(\mathbf{Z}/N\mathbf{Z})^{\times p}$.
- if $p \equiv 3 \bmod 4$, there is a class $z \in H^1_p(\mathbf{F}_p(\frac{p-1}{2}))$ which may or may not lift to $H^1_S(W(\frac{p-1}{2}))$; this class will never lift to $H^1_\Sigma(W(\frac{p-1}{2}))$ as it is ramified at p.

Putting this description together with the Lemma 4.2.3 we have that:

$$\begin{aligned} p \text{ is a } p\text{th power mod } N &\implies h^1_\Sigma(W(\tfrac{p-1}{2})) = 2 \text{ and } h^1_S(W(1)) = 3 + s_p \\ &\implies h^1_{\Sigma^*}(W(1)) = 1 + s_p + 2 = 3 + s_p = h^1_S(W(1)) \\ p \text{ is not a } p\text{th power mod } N &\implies h^1_\Sigma(W(\tfrac{p-1}{2})) = 1 \text{ and } h^1_S(W(1)) = 2 + s_p \\ &\implies h^1_{\Sigma^*}(W(1)) = 1 + s_p + 1 = 2 + s_p = h^1_S(W(1)) \end{aligned}$$

Thus in all cases we have $h^1_{\Sigma^*}(W(1)) = h^1_S(W(1))$; since $H^1_{\Sigma^*}(W(1)) \subseteq H^1_S(W(1))$ we conclude that these groups are equal. □

Proof of Theorem 4.2.1. By Lemma 4.2.2, to show that $\begin{bmatrix} a' \\ a \end{bmatrix} \in H^1_{\Sigma^*}(V(\frac{p-1}{2}))$ it suffices to show that $\begin{bmatrix} ab - a' \\ -b \end{bmatrix}$ (which a priori is just an element of $H^1_S(W(1))$) is an element of $H^1_{\Sigma^*}(W(1))$. Lemma 4.2.4 shows that $H^1_{\Sigma^*}(W(1)) = H^1_S(W(1))$, so this latter condition is immediate. □

Remark 4.2.5. The property that $\chi^{\frac{p-1}{2}}$ is self-inverse is crucial to this argument, and similar results are not true for other powers of χ. See Section 6.3 for examples where the automatic lifting of classes in $H^1_\Sigma(\mathbf{F}_p(i))$ to $H^1_{\Sigma^*}(V(i))$ fails.

5. Effective Criteria for $H^1_\Sigma(\mathbf{F}_p(-i)) \neq 0$

Our goal in this section is to find an effective method for determining whether the various $H^1_\Sigma(\mathbf{F}_p(-i))$, $1 \leq i \leq p-3$ are zero or not. The cases i even and i odd are treated separately. For each i, under a regularity assumption, we relate the question of whether or not $H^1_\Sigma(\mathbf{F}_p(-i)) = 1$ to whether or not a certain quantity in $\mathbf{F}_N^\times$ is a pth power.

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

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

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

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

Theorem 5.1.1. *Let p be an odd prime, $1 \leq i \leq p-4$ be odd, and assume that $(p,-i)$ is a regular pair. Then S_i is a pth power in $\mathbf{F}_N^\times$ if and only if $H^1_\Sigma(\mathbf{F}_p(-i)) \neq 0$*

The general strategy is as follows: Recall from part 2 of Theorem 2.3.5 that

$$h^1_\Sigma(\mathbf{F}_p(-i)) \leq h^1_N(\mathbf{F}_p(-i)) = 1.$$

We will show that the vanishing of S_i in $\mathbf{F}_N^\times/\mathbf{F}_N^{\times p}$ is equivalent to the statement that the nontrivial class in $H^1_N(\mathbf{F}_p(-i))$ satisfies the Selmer condition Σ. To do this, we will produce an element $\mathcal{G}_{-i} \in \mathbf{Q}(\zeta_p)^\times$ whose local properties will control the local properties of the nontrivial class in $H^1_N(\mathbf{F}_p(-i))$.

Remark 5.1.2. The existence of such an element in a slightly different formulation is shown by Lecouturier in [6]. Lecouturier computes the image of this element in $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$ using the Gross-Koblitz formula and N-adic Gamma function, and the quantity $M_i = \prod_{k=1}^{N-1}\prod_{a=1}^{k-1} k^{a^i}$ arises as the image of this element in the factor $\mathbf{Z}_N^\times/\mathbf{Z}_N^{\times p}$ of $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$. His results are not stated in terms of the Selmer groups

$H^1_\Sigma(\mathbf{F}_p(-i))$; instead he relates the vanishing of M_i directly to Iimura's filtration on the class group of $K(\zeta_p)$ (see Remark 3.2.4) in order to deduce bounds on the rank of the class group of K.

We include a proof of Theorem 5.1.1 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 5.1.1; we show in Lemma 5.2.1 that $M_i = S_i^{-1}$ as elements of $\mathbf{F}_N^\times/\mathbf{F}_N^{\times p}$.

Remark 5.1.3. One can compare the role of S_i in Theorem 5.1.1 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 pth powers. Recall that when i is odd, $B_i = 0$. Similarly, the invariant S_i for even i is always a pth power, as the following computation in $\mathbf{F}_N^\times/\mathbf{F}_N^{\times p}$ shows. If $i = 2j$ is even, then

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

where the last step follows from the fact that $a!(N-1-a)! \equiv \pm 1 \in \mathbf{F}_N^\times$ for any $a \not\equiv 0$. Since p is odd, the fact that S_i^2 is a pth power means that S_i itself must be a pth power.

While Theorem 5.1.1 requires a regularity assumption, the setup does not. Until the beginning of the proof of Theorem 5.1.1, we make no regularity assumptions.

For any prime $\mathfrak{n}|N$ of $\mathbf{Q}(\zeta_p)$, define

$$\iota_\mathfrak{n} : \mathbf{Q}(\zeta_p) \to \mathbf{Q}(\zeta_p)_\mathfrak{n} = \mathbf{Q}_N.$$

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

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

Now, fix a prime $\mathfrak{n}|N$, and set $\iota = \iota_\mathfrak{n}$, and $\iota_a = \iota_{[a]\mathfrak{n}}$ for $a \in (\mathbf{Z}/p\mathbf{Z})^\times$.

Let $c \neq 0$ be a class in $H^1_N(\mathbf{F}_p(-i))$. This class c defines an extension $L/\mathbf{Q}(\zeta_p)$ which is Galois over $\mathbf{Q}$ with Galois group $\Gamma_{-i} = \mathbf{Z}/p\mathbf{Z} \rtimes_{\chi^{-i}} (\mathbf{Z}/p\mathbf{Z})^\times$, and c lies in $H^1_\Sigma(\mathbf{F}_p(-i))$ if and only if L localized at a prime above $\mathfrak{n}$ is either trivial or isomorphic to K_N.

The extension $L/\mathbf{Q}(\zeta_p)$ corresponds, by global class field theory, to a homomorphism

$$\psi_c : \mathbf{A}^\times_{\mathbf{Q}(\zeta_p)} \to \mathbf{F}_p$$

which factors through the χ^{-i}-eigenspace of the p-coinvariants of the double quotient

$$\mathbf{Q}(\zeta_p)^\times \backslash \mathbf{A}^\times_{\mathbf{Q}(\zeta_p)}/U$$

where U is the subgroup

$$U = \prod_{\mathfrak{n}'|N} (1 + \mathfrak{n}'\mathcal{O}_{\mathbf{Q}(\zeta_p)_{\mathfrak{n}'}}) \times \prod_{\mathfrak{q}\nmid N} \mathcal{O}^\times_{\mathbf{Q}(\zeta_p)_\mathfrak{q}} \times (\mathbf{Q}(\zeta_p) \otimes \mathbf{R})^\times.$$

We call this eigenspace C_{-i}.

Identifying $\mathbf{Q}(\zeta_p)_{\mathfrak{n}}$ with $\mathbf{Q}_N$, the extension of $\mathbf{Q}_N$ given by localizing L at a prime above $\mathfrak{n}$ is, by local class field theory, determined by a map $\psi_{c,N} : \mathbf{Q}_N^\times \to \mathbf{F}_p$. This map is the composition of the inclusion $j : \mathbf{Q}(\zeta_p)_{\mathfrak{n}}^\times \to \mathbf{A}^\times_{\mathbf{Q}(\zeta_p)}$ and the map ψ_c. This is summarized in the following commutative diagram:

$$\begin{tikzcd}
\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p} \arrow[d, "j"] \arrow[dr, "\psi_{c,N}"] & \\
C_{-i} = (\mathbf{Q}(\zeta_p)^\times\backslash\mathbf{A}^\times_{\mathbf{Q}(\zeta_p)}/U)_p^{\chi^{-i}} \arrow[r, "\psi_c"] & \mathbf{F}_p
\end{tikzcd}$$

The kernel of $\psi_{c,N}$ is the norm subgroup of the extension of $\mathbf{Q}_N$ coming from L. As $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$ is 2-dimensional, this extension is either trivial or isomorphic to K_N (i.e., $c \in H^1_\Sigma(\mathbf{F}_p(-i))$) if and only if N is in the kernel of $\psi_{c,N}$.

Remark 5.1.4. The above construction realizes the idele group C_{-i} as the dual of the cohomology group $H^1_N(\mathbf{F}_p(-i))$. Indeed, by class field theory as above, every element of the cohomology group corresponds to a map $\psi_c : C_{-i} \to \mathbf{F}_p$, and conversely every such homomorphism gives an $\mathbf{F}_p$-extension of $\mathbf{Q}(\zeta_p)$ that is Galois over $\mathbf{Q}$ with Galois group Γ_{-i} and that satisfies the local conditions to lie in $H^1_N(\mathbf{F}_p(-i))$.

Similarly, one identifies $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$ with the dual of $H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p)$. Then the map j defined above is nothing more than the dual to the restriction map

$$\mathrm{res}_N : H^1_N(\mathbf{F}_p(-i)) \to H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p).$$

We turn now to the map j. Under certain conditions, we will prove that the kernel of j is 1-dimensional, spanned by an element $\mathcal{G}_{-i}$ that will be related to S_i.

Lemma 5.1.5. *Let $i \not\equiv -1 \bmod p-1$ be odd. Suppose that there exists an element $\mathcal{G}_{-i} \in \mathbf{Z}[\zeta_p]$ which satisfies the following properties:*

(a) *$\mathcal{G}_{-i}$ lies in the χ^{-i}-eigenspace of $\mathbf{Q}(\zeta_p)^\times/\mathbf{Q}(\zeta_p)^{\times p}$.*

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

Then $\iota(\mathcal{G}_{-i})$ is in the kernel of j.

Proof. We will show that $j(\iota(\mathcal{G}_{-i})) = 0$ in the idelic quotient C_{-i} by showing that $j(\iota(\mathcal{G}_{-i}))$ is equal to the diagonal embedding of the global element $\mathcal{G}_{-i}$ in the χ^{-i}-eigenspace of the p-coinvariants of $\mathbf{A}^\times_{\mathbf{Q}(\zeta_p)}/U$, which we denote by C'_{-i}.

Note that since $\mathcal{G}_{-i}$ is a unit at all primes not dividing N by property (b), it will suffice to work only in the coordinates of the ideles above N, as the quotient by U kills all units at primes not dividing N and all information at the infinite places. We index the primes above N relative to our fixed choice $\mathfrak{n}|N$ and the Galois action on primes; namely the set of primes above N is

$$\{[a]\mathfrak{n} \mid a \in (\mathbf{Z}/p\mathbf{Z})^\times\}.$$

Note that an element $a' \in (\mathbf{Z}/p\mathbf{Z})^\times$ permutes the coordinates above N, sending the $[a]\mathfrak{n}$-coordinate to the $[a'a]\mathfrak{n}$-coordinate. The projection operator

$$P_{\chi^{-i}} : \left(\mathbf{A}^\times_{\mathbf{Q}(\zeta_p)}/U\right)_p \to C'_{-i}$$

is given by the formula

$$P_{\chi^{-i}} = \sum_{a\in(\mathbf{Z}/p\mathbf{Z})^\times} \chi^{-i}(a^{-1})[a]$$

where we have used additive notation for the group ring $\mathbf{F}_p[(\mathbf{Z}/p\mathbf{Z})^\times]$, despite it acting on the multiplicative groups of ideles. With this notation set up, we are trying to show that

$$P_{\chi^{-i}}(j(\iota(\mathcal{G}_{-i}))) = P_{\chi^{-i}}((\iota(\mathcal{G}_{-i}), 1, \dots, 1))$$

is equal the diagonal embedding of $\mathcal{G}_{-i}$:

$$(\iota_a(\mathcal{G}_{-i}))_{a\in(\mathbf{Z}/p\mathbf{Z})^\times}.$$

We compute directly with the formula for $P_{\chi^{-i}}$ that in C'_{-i} we have

$$\begin{aligned} P_{\chi^{-i}}(j(\iota(\mathcal{G}_{-i}))) &= (\chi^{-i}(a^{-1})\iota(\mathcal{G}_{-i}))_{a\in(\mathbf{Z}/p\mathbf{Z})^\times} \\ &= (\iota(\mathcal{G}_{-i}^{\chi^{-i}(a^{-1})}))_{a\in(\mathbf{Z}/p\mathbf{Z})^\times}. \end{aligned}$$

Now, by property (a), we know that $\mathcal{G}_{-i}^{\chi^{-i}(a^{-1})} = [a^{-1}]\mathcal{G}_{-i}$, hence

$$\begin{aligned} P_{\chi^{-i}}(j(\iota(\mathcal{G}_{-i}))) &= (\iota([a^{-1}]\mathcal{G}_{-i}))_{a\in(\mathbf{Z}/p\mathbf{Z})^\times} \\ &= (\iota_a(\mathcal{G}_{-i}))_{a\in(\mathbf{Z}/p\mathbf{Z})^\times} \end{aligned}$$

where we have used that $\iota_a = \iota \circ [a^{-1}]$. □

Now we turn our attention to constructing such a $\mathcal{G}_{-i}$ and relating it to the invariant S_i.

Let $A = \mathbf{Q}(\zeta_p, \zeta_N^{(p)})$ and let $B = \mathbf{Q}(\zeta_p, \zeta_N)$. For any character η

$$\eta : \mathrm{Gal}(B/\mathbf{Q}(\zeta_p)) \cong (\mathbf{Z}/N\mathbf{Z})^\times \to \mu_p$$

of order p, define the Gauss sum

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

Let $\mathfrak{N}$ be the prime above $\mathfrak{n}$ in B (so we have $\mathfrak{N}^{N-1} = \mathfrak{n}$). The Gauss sums g_η satisfy the following properties

- g_η is an element of the ring of integers of A, and is divisible only by primes above N.
- Since $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^\times$ acts on $\mathcal{O}_A$, we have that for $a \in (\mathbf{Z}/p\mathbf{Z})^\times$
$$[a]g_\eta = g_{\eta^a}.$$
- If $[b] \in \mathrm{Gal}(B/\mathbf{Q}(\zeta_p)) = (\mathbf{Z}/N\mathbf{Z})^\times$, then
$$[b]g_\eta = \eta(b^{-1})g_\eta.$$
- $g_\eta^p \in \mathbf{Q}(\zeta_p)$.

Fix the choice of η so that the composite map

$$(\mathbf{Z}/N\mathbf{Z})^\times \xrightarrow{\eta} \mu_p \hookrightarrow (\mathbf{Z}[\mu_p]/\mathfrak{n})^\times = (\mathbf{Z}/N\mathbf{Z})^\times$$

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

$$(\mathbf{Z}/p\mathbf{Z})^\times \xrightarrow{\tau} \mathbf{Z} \setminus \{0\} \to (\mathbf{Z}/p^2\mathbf{Z})^\times$$

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

$$\mathcal{G}_{-i} = \prod_{a\in(\mathbf{Z}/p\mathbf{Z})^\times} ([a]g_\eta)^{\tau(a^i)} = \prod_{a\in(\mathbf{Z}/p\mathbf{Z})^\times} (g_{\eta^a})^{\tau(a^i)}.$$

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

Lemma 5.1.6. *Let $1 \le r < p$, $M = (N-1)/p$, and $m = rM$. Let*

$$I : B \to B_{\mathfrak{N}} = \mathbf{Q}_N(\zeta_N)$$

be an embedding extending ι. Note that $\pi = 1 - \zeta_N$ is a uniformizer in $\mathbf{Q}_N(\zeta_N)$. Then we have that

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

Proof. By definition, we have

$$\begin{aligned} I(g_{\eta^r}) &= \sum_{k=1}^{N-1} \eta(k)^r (1-\pi)^k \\ &= \sum_{k=1}^{N-1} \eta(k)^r - \pi \sum_{k=1}^{N-1} \binom{k}{1} \eta(k)^r + \pi^2 \sum_{k=2}^{N-1} \binom{k}{2} \eta(k)^r - \ldots + \pi^{N-1} \\ &= \sum_{j=0}^{N-1} (-1)^j \pi^j \sum_{k=1}^{N-1} \binom{k}{j} \eta(k)^r \end{aligned}$$

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

$$(-1)^j \pi^j \frac{a}{j!} \sum_{k=1}^{N-1} k^l \eta(k)^r$$

for some $l < j$ and integer a. Note that

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

since $\mathfrak{n} = \mathfrak{N}^{N-1}$ and we have that

$$\sum_{k=1}^{N-1} k^l \eta(k)^r \equiv \sum_{k=1}^{N-1} k^{l-m} \bmod \mathfrak{n}$$

using that η^r is the map $k \mapsto k^{-m}$ modulo $\mathfrak{n}$.

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

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

Lemma 5.1.7. *The element $\mathcal{G}_{-i}$ is in $\mathbf{Q}(\zeta_p)^\times$, and satisfies properties (a) and (b) of Lemma 5.1.5. Furthermore, as elements of $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$, we have*

$$\iota(\mathcal{G}_{-i}) = N^{B_{1,\chi^i}} S_i^{-1}$$

where B_{1,χ^i} is the generalized Bernoulli number.

Proof. For $b \in \mathrm{Gal}(B/\mathbf{Q}(\zeta_p)) = (\mathbf{Z}/N\mathbf{Z})^\times$, we have that

$$\begin{aligned}[b]\mathcal{G}_{-i} &= \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} [b](g_{\eta^a})^{\tau(a^i)} \\ &= \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} (\eta^a(b^{-1}) g_{\eta^a})^{\tau(a^i)} \\ &= \mathcal{G}_{-i} \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \eta^{a\tau(a^i)}(b^{-1}) \\ &= \mathcal{G}_{-i} \cdot \eta^{(\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} a\tau(a^i))}(b^{-1}) \\ &= \mathcal{G}_{-i}.\end{aligned}$$

The last equality follows from the fact that the character η has order p: This lets us work mod p in the exponent, so we can use that $\tau(a^i) \equiv a^i \bmod p$ and that $\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} a^{i+1} \equiv 0 \bmod p$ when $i \not\equiv -1 \bmod p-1$. This establishes that $\mathcal{G}_{-i} \in \mathbf{Z}[\zeta_p]$. Along with the properties of the Gauss sums g_η, we conclude that $\mathcal{G}_{-i}$ is only divisible by the primes above N, which is to say it satisfies property (b) of Lemma 5.1.5.

To show that $\mathcal{G}_{-i}$ satisfies property (a) of Lemma 5.1.5, we recall that τ satisfies $\tau(c^{-i}) \equiv \chi^{-i}(c) \bmod p$ and verify that for $c \in (\mathbf{Z}/p\mathbf{Z})^\times$,

$$\begin{aligned}[c]\mathcal{G}_{-i} &= \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} [c]([a]g_\eta)^{\tau(a^i)} \\ &= \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} ([ac]g_\eta)^{\tau(a^i)} \\ &= \prod_{a' \in (\mathbf{Z}/p\mathbf{Z})^\times} ([a']g_\eta)^{\tau(a'^i)\tau(c^{-i})} \\ &= \mathcal{G}_{-i}^{\tau(c^{-i})} \\ &= \mathcal{G}_{-i}^{\chi^{-i}(c)}\end{aligned}$$

where all equalities are taken to be in $\mathbf{Q}(\zeta_p)^\times/\mathbf{Q}(\zeta_p)^{\times p}$. In the third equality, we have used that $g_\eta^p \in \mathbf{Q}(\zeta_p)^\times$, so $g_\eta^{p^2} \in \mathbf{Q}(\zeta_p)^{\times p}$ which means we can work mod p^2 in the exponent. For the final equality, we recall from above that $\mathcal{G}_{-i} \in \mathbf{Q}(\zeta_p^\times)$ and thus we can take the exponent mod p.

What remains is to show that $\iota(\mathcal{G}_{-i}) = N^{B_{1,\chi^i}} S_i^{-1}$ in $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$.

Using Lemma 5.1.6, we can write

$$\begin{aligned}\iota(\mathcal{G}_{-i}) &= \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} I(g_{\eta^a})^{\tau(a^i)} \\ &= \prod_{r=1}^{p-1} \left((-1)^{rM+1} \frac{\pi^{rM}}{(rM)!} + O(\pi^{rM+1}) \right)^{\tau(r^i)}\end{aligned}$$

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

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

To understand the final term, we first write

$$\begin{aligned}
\frac{\pi^{N-1}}{N} &= \frac{1}{N}(1-\zeta_N)^{N-1}\\
&= \frac{1}{N}\mathrm{Norm}^{\mathbf{Q}_N(\zeta_N)}_{\mathbf{Q}_N}(1-\zeta_N)\prod_{i=1}^{N-1}\frac{1-\zeta_N}{1-\zeta_N^i}\\
&= \prod_{i=1}^{N-1}(1+\zeta_N+\cdots+\zeta_N^{i-1})^{-1}\\
&\equiv \left(\prod_{i=1}^{N-1} i\right)^{-1} \mod \pi\\
&\equiv -1 \bmod \pi
\end{aligned}$$

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

$$\begin{aligned}
\pi^{\sum_{r=1}^{p-1} rM\tau(r^i)} &= \pi^{(N-1)\frac{1}{p}\sum_{r=1}^{p-1} r\tau(r^i)}\\
&= \pm N^{\frac{1}{p}\sum_{r=1}^{p-1} r\tau(r^i)}(1+O(\pi)).
\end{aligned}$$

Working modulo p in the exponent, we can substitute $\tau(r^i)$ with $\chi(r^i)$. This new exponent $\frac{1}{p}\sum_{r=1}^{p-1} r\chi(r^i)$ is exactly the generalized Bernoulli number B_{1,χ^i}.

Combining the previous calculations, we have now shown that in $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$,

$$\iota(\mathcal{G}_{-i}) = S_i^{-1} N^{B_{1,\chi^i}} w$$

where w is a unit in $\mathbf{Z}_N$ that, considered as an element of $\mathbf{Z}_N[\zeta_N]$, is congruent to 1 modulo π. The isomorphism $\mathbf{Z}_N[\zeta_N]/(\pi) = \mathbf{Z}_N/(N)$ tells us that $w \equiv 1 \bmod N$ and is thus a pth power in $\mathbf{Q}_N^\times$. Thus

$$\iota(\mathcal{G}_{-i}) = N^{B_{1,\chi^i}} S_i^{-1}$$

in $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$, as desired. □

We are now ready to prove Theorem 5.1.1. Up until this point, we have not made any regularity assumptions. From now on, we assume that $(p,-i)$ is a regular pair.

Proof of Theorem 5.1.1. We first check that $\ker j$ is 1-dimensional and spanned by $\iota(\mathcal{G}_{-i})$. As $(p,-i)$ is a regular pair, we know that the generalized Bernoulli number B_{1,χ^i} is a p-adic unit by Remark 2.3.2. Therefore, in $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$ we have that

$$\iota(\mathcal{G}_{-i}) = N^{B_{1,\chi^i}} S_i^{-1}$$

is a nonzero element of $\ker j$.

(Equivalently, one could instead notice that $h^1_N(\mathbf{F}_p(-i)) = 1$ from part 2 of Theorem 2.3.5. By Remark 5.1.4, this gives us that the codomain of j is 1-dimensional as well. The domain of j is $\mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$ which is 2-dimensional, which shows that j has a nontrivial kernel.)

Now we need to check that j is nonzero, which by Remark 5.1.4 is equivalent to showing that the dual map

$$\mathrm{res}_N : H^1_N(\mathbf{F}_p(-i)) \to H^1(G_{\mathbf{Q}_N}, \mathbf{F}_p)$$

is nonzero.

This must be the case, as the class in $H^1_N(\mathbf{F}_p(-i))$ is unramified away from N, and thus must be ramified at N as $(p, -i)$ is a regular pair. In particular, it is not split at N.

To finish, let c be a generator of $H^1_N(\mathbf{F}_p(-i))$. This gives a $\psi_c : C_{-i} \to \mathbf{F}_p$ as in the discussion after the statement of Theorem 5.1.1. Recall also from that discussion that $c \in H^1_\Sigma(\mathbf{F}_p(-i))$ if and only if the kernel of $\psi_{c,N} = \psi_c \circ j$ contains the element $N \in \mathbf{Q}_N^\times/\mathbf{Q}_N^{\times p}$.

Because ψ_c is an isomorphism, we have $\ker \psi_{c,N} = \ker j$ and thus the local behavior of c is completely determined by $\ker j$. By the above, $\ker j$ is spanned by

$$\iota(\mathcal{G}_{-i}) = N^{B_{1,\chi^i}} S_i^{-1}$$

and thus contains N if and only if S_i is a pth power in $\mathbf{F}_N^\times$. □

5.2. **Relationship between S_i, M_i, and C.** We begin by showing that our S_i is a pth power in $\mathbf{F}_N^\times$ if and only if Lecouturier's M_i is. Recall from Section 1.1 that for odd $1 \leq i \leq p-4$, M_i is defined by

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

Lemma 5.2.1. *As elements of $\mathbf{F}_N^\times/\mathbf{F}_N^{\times p}$, $S_i^{-1} = M_i$.*

Proof. All equalities in this proof take place in $\mathbf{F}_N^\times/\mathbf{F}_N^{\times p}$. In Lemma 4.3 of [6], Lecouturier proves that

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

where Γ_N denotes the N-adic Gamma function (see below for a summary of the properties of this function, and Chapter IV.2 of [5] for the detailed construction). Using that $\frac{k}{p} \equiv M(p-k) + 1 \bmod N$, the Gamma functions can be replaced by factorials

$$\begin{aligned} M_i &= \prod_{k=1}^{p-1} ((M(p-k))!)^{k^i} \\ &= \prod_{k=1}^{p-1} ((Mk)!)^{-k^i} \\ &= S_i^{-1} \end{aligned}$$

where the second step follows by changing variables from k to $p-k$ and discarding p-th powers. □

Theorem 5.1.1 establishes that under a regularity assumption, $H^1_\Sigma(\mathbf{F}_p(-i))$ is nonzero if and only if S_i is a pth power for odd $i \not\equiv -1 \bmod p-1$. A similar relationship was known to Wake–Wang-Erickson in the case $i \equiv 1 \bmod p-1$; see Theorem 12.5.1 of [12].

However, these results are not stated in terms of S_1, but rather in terms of Merel's number

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

Theorem 1.3, (ii) of [2] states that if $r_K = 1$ then C is not a pth power mod N. Similarly, Proposition 4.0.1 and Theorem 5.1.1 together imply that if $r_K = 1$ then S_1 is not a pth power mod N. Thus one might expect that the quantities C and S_1 can be related in $\mathbf{F}_N^\times/\mathbf{F}_N^{\times p}$. 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

$$A_m = \prod_{k=1}^{N-1} k^{k^m}.$$

In Proposition 1.2 of [6], Lecouturier proves that

$$C = A_2^{-3/4} \text{ in } \mathbf{F}_N^\times/\mathbf{F}_N^{\times p}.$$

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

- $\Gamma_N : \mathbf{Z}_N \to \mathbf{Z}_N^\times$ is a continuous function, constructed by extending the function
$$\Gamma_N(x) = (-1)^x \prod_{0<j<x, N\nmid j} j$$
defined for positive integers x by continuity to all of $\mathbf{Z}_N$.
- For an integer $0 < x < N$, we have $\Gamma_N(x) = (-1)^x(x-1)!$.
- If $x \equiv y \bmod N$, then $\Gamma_N(x) \equiv \Gamma_N(y) \bmod N$.
- If $x + r$ is not divisible by N for $0 \le r \le M-1$ where $M = \frac{N-1}{p}$, then
$$\prod_{r=0}^{M-1}(x+r) = (-1)^M \frac{\Gamma_N(M+x)}{\Gamma_N(x)}.$$

See Chapter IV.2 of [5] for the construction of Γ_N.

Proposition 5.2.2. *Suppose that* $0 < m < p-1$. *Then*

$$A_m = \prod_{j=1}^{m-1} S_j^{(-1)^j\binom{m}{j}} \textit{ in } \mathbf{F}_N^\times/\mathbf{F}_N^{\times p}.$$

Proof. All equalities in this proof are in $\mathbf{F}_N^\times/\mathbf{F}_N^{\times p}$. 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 pth powers from the exponent and factoring out a pth power of p we have that

$$\begin{aligned} A_m &= \prod_{k=1}^{p-1} \prod_{r=0}^{M-1} \left(\frac{k}{p} + r\right)^{k^m} \\ &= \prod_{k=1}^{p-1} \left((-1)^M \frac{\Gamma_N(M + k/p)}{\Gamma_N(k/p)}\right)^{k^m} \end{aligned}$$

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

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

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

$$\begin{aligned} A_m &= \prod_{k=1}^{p-1} ((M(p-k))!)^{(k+1)^m - k^m} \\ &= \prod_{k=1}^{p-1} ((Mk)!)^{(p-k+1)^m - (p-k)^m} \end{aligned}$$

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

$$A_m = \prod_{j=0}^{m-1} S_j^{(-1)^j \binom{m}{j}}. \qquad \square$$

Note that this theorem implies that

$$A_2 = S_1^{-2} \text{ in } \mathbf{F}_N^\times / \mathbf{F}_N^{\times p}$$

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 pth power mod N if and only if all of them are.

Proposition 5.2.2 also shows that the S_i can be recovered from the A_m, at least as elements of $\mathbf{F}_N^\times / \mathbf{F}_N^{\times p}$, using inductively that $S_1 = A_2^2$ and that

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

for all i.

5.3. A Criterion for $H^1_\Sigma(\mathbf{F}_p(-i)) \neq 0$, i Even.

So far, the focus of this section has been on odd i. At this point, we turn to finding invariants that will let us compute whether or not $H^1_\Sigma(\mathbf{F}_p(-i))$ is trivial for even $i \neq 0 \bmod p-1$.

Proposition 5.3.1. *Let p be an odd prime, and let $2 \leq i \leq p-3$ be even. Suppose that $(p, 1+i)$ is a regular pair. Then $H^1_\Sigma(\mathbf{F}_p(-i))$ is non-trivial if and only if both of the following are satisfied:*

(1) $H^1_\Sigma(\mathbf{F}_p(1+i)) \neq 0$
(2) $H^1_p(\mathbf{F}_p(1+i)) \subseteq H^1_{\Sigma^*}(\mathbf{F}_p(1+i))$

Proof. We see by Theorems 2.3.5 and 2.3.6 that $H^1_\Sigma(\mathbf{F}_p(-i))$ is non-trivial if and only if $H^1_{\Sigma^*}(\mathbf{F}_p(1+i))$ is 2-dimensional and thus equal to $H^1_S(\mathbf{F}_p(1+i))$. Since $H^1_S(\mathbf{F}_p(1+i))$ is spanned by the subspaces $H^1_N(\mathbf{F}_p(i+1))$ and $H^1_p(\mathbf{F}_p(i+1))$, this second condition happens if and only if we have both $H^1_N(\mathbf{F}_p(1+i)) = H^1_\Sigma(\mathbf{F}_p(1+i))$ and $H^1_p(\mathbf{F}_p(1+i)) \subseteq H^1_{\Sigma^*}(\mathbf{F}_p(1+i))$. □

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 $H^1_p(\mathbf{F}_p(1+i)) \subseteq H^1_{\Sigma^*}(\mathbf{F}_p(1+i))$.

The class in $H^1_p(\mathbf{F}_p(1+i))$ 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. By using the inflation-restriction sequence and Kummer theory, we get that

$$\begin{aligned} H^1_p(\mathbf{F}_p(1+i)) &\cong H^1_p(G_{\mathbf{Q}(\zeta_p)}, \mathbf{F}_p(1+i))^{\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})} \\ &\cong (H^1_p(G_{\mathbf{Q}(\zeta_p)}, \mathbf{F}_p(1))(i))^{\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})} \\ &\cong \left(\left(\frac{\mathbf{Z}[\zeta_p, p^{-1}]^\times}{\mathbf{Z}[\zeta_p, p^{-1}]^{\times p}}\right)(i)\right)^{\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})} \\ &\cong \left(\frac{\mathbf{Z}[\zeta_p, p^{-1}]^\times}{\mathbf{Z}[\zeta_p, p^{-1}]^{\times p}}\right)^{\chi^{-i}} \end{aligned}$$

where we have used that the restriction map is an isomorphism as the order of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ is prime to p. In other words, the extension of $\mathbf{Q}$ defined by a class in $H^1_p(\mathbf{F}_p(1+i))$ is always of the form $\mathbf{Q}(\zeta_p, a^{1/p})$, where $a \in \mathbf{Z}[\zeta_p, p^{-1}]^\times$ and

$$\sigma(a) = a^{\chi^{-i}(\sigma)} \text{ modulo } p\text{th powers}$$

for all $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Note that given such an element, all of its Galois conjugates are also Kummer generators of the same extension. Thus it suffices to find such a Kummer generator a (which is independent of N), and then use that the cohomology class spanning $H^1_p(\mathbf{F}_p(1+i))$ is trivial at N if and only if the Kummer generator is a pth power in $\mathbf{Q}_N^\times$, which happens if and only if the Kummer generator is a pth power mod N.

The minimal polynomials of such elements can be computed using a computer algebra system. This was done using SageMath [11] for $p = 5$ and $p = 7$. The SageMath code is available on the second author's personal website.

Theorem 5.3.2. *We have:*

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

(2) *Suppose $p = 7$. Then*

  (a) *$H^1_\Sigma(\mathbf{F}_p(-2))$ is nonzero if and only both S_3 and the roots of*

$$x^3 + 41x^2 + 54x + 1$$

  are 7th powers in $\mathbf{F}_N^\times$.

  (b) *$H^1_\Sigma(\mathbf{F}_p(-4))$ is nonzero if and only if both S_1 and the roots of*

$$x^3 - 25x^2 + 31x + 1$$

  are 7th powers in $\mathbf{F}_N^\times$.

Remark 5.3.3. The polynomials in the theorem above are not unique. One could use any other polynomial whose roots generate the same 1-dimensional subspace of

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

6. Specific Primes

We now apply the results of the previous sections 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 1.1.2.

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

6.1. $p = 3$.

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

The results of Section 3.1 recover this result in the following way. Lemmas 3.1.10 and 3.1.11 imply that the type m of any unramified extension E/K must satisfy $m \leq p - 2 = 1$. Lemma 3.1.5 shows that the only extension of type 1 is the genus field $K(\zeta_N^{(p)})$. This proves the following theorem.

Theorem 6.1.1. *Let $p = 3$. Then $r_K = 1$.*

6.2. $p = 5$.

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

Theorem 6.2.1. *Let $p = 5$. Then $r_K = 1 + h^1_\Sigma(\mathbf{F}_p(-1)) + h^1_\Sigma(\mathbf{F}_p(-2))$.*

Proof. We know from Theorem 3.0.1 that

$$r_K = 1 + h^1_\Sigma(\mathrm{Sym}^{p-4} V \otimes \mathbf{F}_p(2)) = 1 + h^1_\Sigma(V(-2)).$$

Thus to prove the theorem it suffices to show that

$$h^1_\Sigma(V(-2)) = h^1_\Sigma(\mathbf{F}_p(-1)) + h^1_\Sigma(\mathbf{F}_p(-2)).$$

In light of the short exact sequence of $G_{\mathbf{Q},S}$-modules

$$0 \to \mathbf{F}_p(-1) \to V(-2) \to \mathbf{F}_p(-2) \to 0$$

and the fact that $H^1_\Sigma(\mathbf{F}_p(-1)) \subseteq H^1_\Sigma(V(-2))$ by the associated long exact sequence in $G_{\mathbf{Q},S}$-cohomology, it will suffice to prove that any class in $H^1_\Sigma(\mathbf{F}_p(-2))$ lifts to $H^1_\Sigma(V(-2))$, as in the discussion at the beginning of Section 4.

Suppose $h^1_\Sigma(\mathbf{F}_p(-2)) \neq 0$, and hence also $h^1_\Sigma(\mathbf{F}_p(-1)) \neq 0$ by Corollary 2.3.7. We satisfy the conditions of Theorem 4.2.1, as $\frac{p-1}{2} = 2 \equiv -2 \bmod 4$, so we know that the class spanning $H^1_\Sigma(\mathbf{F}_p(-2))$ lifts to a class in $H^1_{\Sigma^*}(V(-2))$. Since we also have

$$h^1_{\Sigma^*}(\mathbf{F}_p(-1)) = 2 > 1 = h^1_\Sigma(\mathbf{F}_p(-1))$$

in this situation by Theorem 2.3.6, we may apply Lemma 4.1.3 to choose a lift which in fact is in $H^1_\Sigma(V(-2))$. □

Combining this theorem with the results of Section 5 proves Theorem 1.1.3:

Proof of Theorem 1.1.3. Since each $h^1_\Sigma(\mathbf{F}_p(-i))$ is at most 1, we obtain the bound $r_K \leq 3$. We know that $r_K \geq 2$ if and only if $S_1 = \prod_{k=1}^{p-1}((Mk)!)^k$ is a 5th power in $\mathbf{F}_N^\times$, as Theorem 5.1.1 proves that $h^1_\Sigma(\mathbf{F}_p(-1)) = 1$ if and only if S_1 is a 5th power, and further, $r_K = 3$ if and only if $h^1_\Sigma(\mathbf{F}_p(-1)) = h^1_\Sigma(\mathbf{F}_p(-2)) = 1$, which by Theorems 5.1.1 and 5.3.2 happens if and only if both S_1 and $\frac{\sqrt{5}-1}{2}$ are 5th powers in $\mathbf{F}_N^\times$. □

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

6.3. $p = 7$. When $p = 7$ it is not the case that r_K can be determined completely by the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$. Note that when $p = 7$ the possible groups $H^1_\Sigma(\mathbf{F}_p(-i))$ that may arise are those for $i \in \{1, 2, 3, 4\}$. When discussing the possible cases we will indicate the dimensions of these $H^1_\Sigma(\mathbf{F}_p(-i))$ by a binary string of length 4; so for example 1000 is used to indicate $h^1_\Sigma(\mathbf{F}_p(-1)) = 1$ and $h^1_\Sigma(\mathbf{F}_p(-i)) = 0$ for $i \in \{2, 3, 4\}$. By Corollary 2.3.7, not all binary strings of length 4 may occur of as the dimensions of the $h^1_\Sigma(\mathbf{F}_p(-i))$; if $h^1_\Sigma(\mathbf{F}_p(-i)) = 1$ for $i = 2$ or 4, we must have that $h^1_\Sigma(\mathbf{F}_p(-i)) = 1$ for $i = 3$ or 1, respectively.

Theorem 6.3.1. *Let $p = 7$. Then $r_K \geq 2$ if and only if at least one of $H^1_\Sigma(\mathbf{F}_p(-1))$ or $H^1_\Sigma(\mathbf{F}_p(-3))$ is nonzero.*

Proof. By the upper bound given in Proposition 3.4.1, if $r_K \geq 2$ we must have at least one of the $h^1_\Sigma(\mathbf{F}_p(-i)) \neq 0$. Corollary 2.3.7 shows that if any of the $h^1_\Sigma(\mathbf{F}_p(-i))$ is nonzero we must have that $h^1_\Sigma(\mathbf{F}_p(-i)) = 1$ for $i = 1$ or 3. This proves the “only if” direction.

We have established in Proposition 4.0.1 that $h^1_\Sigma(\mathbf{F}_p(-1)) = 1 \implies r_K \geq 2$. Thus it remains to show that when $h^1_\Sigma(\mathbf{F}_p(-1)) = 0$ and $h^1_\Sigma(\mathbf{F}_p(-3)) = 1$ we have $r_K \geq 2$. There are two possible cases, based on whether or not $h^1_\Sigma(\mathbf{F}_p(-2)) = 0$.

Case 1: The dimensions of the $H^1_\Sigma(\mathbf{F}_p(-i))$ are 0110. In this situation, we have by Theorems 2.3.5 and 2.3.6 that

$$2 = h^1_S(\mathbf{F}_p(-1)) > 1 = h^1_{\Sigma^*}(\mathbf{F}_p(-1)) > 0 = h^1_\Sigma(\mathbf{F}_p(-1)),$$

hence we may apply Lemma 4.1.4 to show that the class spanning $H^1_\Sigma(\mathbf{F}_p(-2))$ lifts to $H^1_\Sigma(V(-2))$. Since $V(-2)$ is the 2-dimensional subrepresentation of

$$\mathrm{Sym}^{p-4} V \otimes \mathbf{F}_p(2) = \mathrm{Sym}^3 V \otimes \mathbf{F}_p(-4),$$

we have by Theorem 3.0.1 and the discussion at the start of Section 3.4 that

$$\begin{aligned} r_K &= 1 + h^1_\Sigma(\mathrm{Sym}^3 V \otimes \mathbf{F}_p(-4)) \\ &\geq 1 + h^1_\Sigma(V(-2)) \\ &\geq 1 + 1 = 2. \end{aligned}$$

Case 2: The dimensions of the $H^1_\Sigma(\mathbf{F}_p(-i))$ are 0010. The conditions of Theorem 4.2.1 are satisfied here, so a class spanning $H^1_\Sigma(\mathbf{F}_p(-3))$ lifts to a class in $H^1_{\Sigma^*}(V(-3))$. Using that

$$1 = h^1_{\Sigma^*}(\mathbf{F}_p(-2)) > 0 = h^1_\Sigma(\mathbf{F}_p(-2))$$

by Theorem 2.3.6, we may apply Lemma 4.1.3 to show that there is in fact a lift to $H^1_\Sigma(V(-3))$. Now, using that again that

$$2 = h^1_S(\mathbf{F}_p(-1)) > 1 = h^1_{\Sigma^*}(\mathbf{F}_p(-1)) > 0 = h^1_\Sigma(\mathbf{F}_p(-1)),$$

we apply Lemma 4.1.4 to show that the class in $H^1_\Sigma(V(-3))$ lifts to a class in $H^1_\Sigma(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$. Since $\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3)$ is the 3-dimensional subrepresentation of $\mathrm{Sym}^3 V \otimes \mathbf{F}_p(-4)$, we have again by Theorem 3.0.1 and the discussion in Section 3.4 that

$$\begin{aligned} r_K &= 1 + h^1_\Sigma(\mathrm{Sym}^3 V \otimes \mathbf{F}_p(-4)) \\ &\geq 1 + h^1_\Sigma(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3)) \\ &\geq 1 + 1 = 2. \end{aligned}$$ □

Theorem 1.1.4 follows by combining this result and Theorem 5.1.1: the dimensions $h^1_\Sigma(\mathbf{F}_p(-1))$ and $h^1_\Sigma(\mathbf{F}_p(-3))$ are nonzero if and only if, respectively, S_1 and S_3 are 7th powers in $\mathbf{F}_N^\times$.

We have upper and lower bounds on r_K by Theorem 3.0.1, and we may interpret Theorem 6.3.1 as improving the lower bound to

$$1 + \max\{h^1_\Sigma(\mathbf{F}_p(-1)), h^1_\Sigma(\mathbf{F}_p(-3))\} \leq r_K \leq 1 + \sum_{i=1}^{4} h^1_\Sigma(\mathbf{F}_p(-i)).$$

These bounds are optimal, in the sense that for a given binary string of dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ there exist $N \equiv 1 \bmod 7$ for which the corresponding r_K witness all possible values between the upper and lower bounds. See Appendix A.2 for data on the distribution of N among values for the $h^1_\Sigma(\mathbf{F}_p(-i))$ and r_K.

We turn now to a study of the possibilities that may occur when r_K does not achieve the upper bound of Theorem 3.0.1. We say that a class $a_i \in H^1_\Sigma(\mathbf{F}_p(-i))$ "contributes to r_K" if a_i lifts all the way to $H^1_\Sigma(\mathrm{Sym}^{i-1} V \otimes \mathbf{F}_p(-i))$, which is a subset of $H^1_\Sigma(\mathrm{Sym}^3 V \otimes \mathbf{F}_p(-4))$.

Remark 6.3.2. If $r_K < 1 + \sum_{i=1}^4 h^1_\Sigma(\mathbf{F}_p(-i))$, it is not always possible to determine using the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ which class $a_i \in H^1_\Sigma(\mathbf{F}_p(-i))$ is failing to contribute to r_K.

For example, suppose that $r_K = 3$ and the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ are 1011. It must be the case that one of $a_3 \in H^1_\Sigma(\mathbf{F}_p(-3))$ and $a_4 \in H^1_\Sigma(\mathbf{F}_p(-4))$ is contributing to r_K and the other is failing to. However, the conditions of Lemma 4.1.4 are not satisfied in this situation as $H^1_S(\mathbf{F}_p(-1)) = H^1_{\Sigma^*}(\mathbf{F}_p(-1))$, so the results of Section 4 are not strong enough to show that either class always contributes to r_K.

When a failure to contribute to r_K can be tracked down to a specific class $a_i \in H^1_\Sigma(\mathbf{F}_p(-i))$ there are two aspects of its failure to contribute which may be considered. First, there is the stage of lifting at which the failure occurs: there is a $k \geq 1$ such that a_i lifts to $H^1_\Sigma(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(-i))$ but not one step further to $H^1_\Sigma(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-i))$. Second, there is the type of failure which occurs at this kth stage. The class a_i always lifts to $H^1_S(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-i))$ but it could be the case that:

(1) No lift to $H^1_S(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-i))$ is split at p;
(2) No lift to $H^1_S(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-i))$ 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 some cases it is possible to determine at which stage and which type of failure to lift is occurring, by an analysis of the dimensions of the subgroups of the $H^1_S(\mathbf{F}_p(-i))$ using the results of Section 2.3. Examples of situations witnessing each of the above types of local failure are collected below. In each example, the class $a_3 \in H^1_\Sigma(\mathbf{F}_p(-3))$ fails to contribute to r_K. Note that by Theorem 4.2.1 there is a lift of a_3 to $H^1_{\Sigma^*}(V(-3))$, and since the set of all lifts is a coset of $H^1_S(\mathbf{F}_p(-2)) = H^1_{\Sigma^*}(\mathbf{F}_p(-2))$, we in fact have that every lift of a_3 is in $H^1_{\Sigma^*}(V(-3))$.

Example 6.3.3. Suppose that the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ are 0110 and $r_K = 2$. The proof of Theorem 6.3.1 showed that the class in $H^1_\Sigma(\mathbf{F}_p(-2))$ contributes to r_K, so it must be the case that $a_3 \in H^1_\Sigma(\mathbf{F}_p(-3))$ does not lift to $H^1_\Sigma(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$.

Suppose that a_3 lifts to $H^1_\Sigma(V(-3))$. Then Lemma 4.1.4 would apply as

$$\begin{aligned} h^1_S(\mathbf{F}_p(-1)) &= 2 \\ h^1_{\Sigma^*}(\mathbf{F}_p(-1)) &= 1 + h^1_\Sigma(\mathbf{F}_p(-4)) = 1 \\ h^1_\Sigma(\mathbf{F}_p(-1)) &= 0, \end{aligned}$$

so there would exist a lift of a_3 to $H^1_\Sigma(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$. Since our assumption that $r_K = 2$ implies that a_3 does not lift to $H^1_\Sigma(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$, it must be the case that a_3 does not lift to $H^1_\Sigma(V(-3))$.

We know that every lift of a_3 to $H^1_S(V(-3))$ is in $H^1_{\Sigma^*}(V(-3))$, thus it must be the case that no lift is split at p.

Example 6.3.4. Suppose that the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ are 1011 and $r_K = 2$. As in the proof of Theorem 6.3.1, Theorem 4.2.1 shows that a_3 lifts to $H^1_{\Sigma^*}(V(-3))$, and then Lemma 4.1.3 shows that there is a modification of this lift which is in $H^1_\Sigma(V(-3))$.

Suppose that there is a lift of this class to $H^1_{\Sigma^*}(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$. Then Lemma 4.1.3 would apply to show that there is a lift to $H^1_\Sigma(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$, as

$$\begin{aligned} h^1_{\Sigma^*}(\mathbf{F}_p(-1)) &= 1 + h^1_\Sigma(\mathbf{F}_p(-4)) = 2 \\ h^1_\Sigma(\mathbf{F}_p(-1)) &= 1. \end{aligned}$$

Our assumption that $r_K = 2$ means that a_3 does not contribute to r_K, hence there cannot be a lift of a_3 to $H^1_{\Sigma^*}(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$.

Example 6.3.5. Suppose that the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ are 1010 and $r_K = 2$. As in the previous example, a_3 lifts to $H^1_\Sigma(V(-3))$.

We have that

$$2 = h^1_S(\mathbf{F}_p(-1)) > 1 = h^1_{\Sigma^*}(\mathbf{F}_p(-1)) = h^1_N(\mathbf{F}_p(-1)) = h^1_\Sigma(\mathbf{F}_p(-1)),$$

hence we may apply Lemmas 4.1.1 and 4.1.2 to show that there are lifts of a_3 to both $H^1_{\Sigma^*}(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$ and $H^1_N(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$, respectively.

However, we know that a_3 fails to contribute to r_K, so it must be the case that no lift of a_3 is in

$$H^1_\Sigma(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3)) = H^1_{\Sigma^*}(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3)) \cap H^1_N(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3)).$$

In other words there is no lift of a_3 which satisfies the conditions at p and N simultaneously, despite there being lifts which satisfy each condition individually.

Appendix A. Data for $p = 5, 7$

All computations in this section were performed using PARI/GP [10] and SageMath [11]. The computation of ranks of class groups when $p = 7$ used PARI/GP's built-in algorithms for computing class groups of number fields, which assume GRH to optimize computation. Thus the ranks computed when $p = 7$ in all cases other than those where the rank is determined by the numbers $h^1_\Sigma(\mathbf{F}_p(-i))$ as in Section 6.3 are conditional on GRH.

The SageMath code for computing the numbers $h^1_\Sigma(\mathbf{F}_p(-i))$ for $p = 7$ via the methods in Section 5 is available on the second author's website. The data in Table 2 took approximately 10 hours to gather using a low-range commercial processor.

A.1. $p = 5$**.** For primes $N \equiv 1 \bmod 5$, $N \le 20{,}000{,}000$ we computed the dimensions $h^1_\Sigma(\mathbf{F}_p(-1))$ and $h^1_\Sigma(\mathbf{F}_p(-2))$ using the results of Section 5. For each N there are three possible sets of dimensions: both are 0, $h^1_\Sigma(\mathbf{F}_p(-1)) = 1$ and $h^1_\Sigma(\mathbf{F}_p(-2)) = 0$, and both are 1; as in Section 6.3 these are notated by a binary string of length 2 (00, 10, and 11). Note that by Theorem 6.2.1 the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ 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.

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 $r_K \ge 2$, and of those N, 19.80% of N have $r_K \ge 3$. We expect that the quantities M_1 and $\frac{\sqrt{5}-1}{2}$ should be "uniformly distributed" in $\mathbf{Z}/5\mathbf{Z} \cong \mathbf{F}_N^\times/\mathbf{F}_N^{\times 5}$, meaning that they are 5th powers for a set of primes of density $\frac{1}{5}$ in the primes $N \equiv 1 \bmod 5$. This would imply that $r_K \ge 2$ for $\frac{1}{5}$ of those primes and that $r_K = 3$ for $\frac{1}{25}$ of primes $N \equiv 1 \bmod 5$, which is suggested by the data.

A.2. $p = 7$**.** For primes $N \equiv 1 \bmod 7$, $N \le 100{,}000{,}000$, we computed the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ for $i = 1, 2, 3, 4$ using the results of Section 5. There are 960,023 such primes N, and their distribution among the possible cases is given in Table 2.

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 $H^1_\Sigma(\mathbf{F}_p(-i))$, $p = 7$ and $N \le 100{,}000{,}000$.

For primes $N \equiv 1 \bmod 7$ and $N \leq 20{,}000{,}000$, we computed the rank r_K (which is not determined completely by the $h^1_\Sigma(\mathbf{F}_p(-i))$ in this case). There are 211,766 such primes N, and their distribution between possible ranks $1 \leq r_K \leq 5$ and dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ are given in Table 3. The empty cells in Table 3 are cases that are shown to never occur in Section 6.3; in particular every case not ruled out in Section 6.3 does occur.

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	2	$211,766$

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

As in the case $p = 5$, one might expect that $H^1_\Sigma(\mathbf{F}_p(-1))$ and $H^1_\Sigma(\mathbf{F}_p(-3))$ are each nonzero for $\frac{1}{7}$ of primes $N \equiv 1 \bmod 7$. Indeed, the data supports this guess, with 14.24% of the N tested having $H^1_\Sigma(\mathbf{F}_p(-1))$ nonzero, and 14.39% of the N tested having $H^1_\Sigma(\mathbf{F}_p(-3))$ nonzero.

One might also expect that $\frac{1}{7}$ of primes with $H^1_\Sigma(\mathbf{F}_p(-1))$ nonzero also have $H^1_\Sigma(\mathbf{F}_p(-4))$ nonzero, 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, $H^1_\Sigma(\mathbf{F}_p(-2))$ is nonzero for 14.30% of the primes tested for which $H^1_\Sigma(\mathbf{F}_p(-3))$ is nonzero.

References

1. J. L. Alperin, *Local representation theory*, Cambridge Studies in Advanced Mathematics, vol. 11, Cambridge University Press, Cambridge, 1986, Modular representations as an introduction to the local representation theory of finite groups. MR 860771
2. Frank Calegari and Matthew Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160** (2005), no. 1, 97–144. MR 2129709
3. Frank Gerth, III, *On 3-class groups of pure cubic fields*, J. Reine Angew. Math. **278/279** (1975), 52–62. MR 0387234
4. Kiyoaki Iimura, *On the l-rank of ideal class groups of certain number fields*, Acta Arith. **47** (1986), no. 2, 153–166. MR 867494
5. Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR 754003
6. Emmanuel Lecouturier, *On the galois structure of the class group of certain kummer extensions*, Journal of the London Mathematical Society **0**, no. 0.
7. Loïc Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$*, J. Reine Angew. Math. **477** (1996), 71–115. MR 1405312
8. J.S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, 2006.
9. Romyar T. Sharifi, *Massey products and ideal class groups*, J. Reine Angew. Math. **603** (2007), 1–33. MR 2312552

10. The PARI Group, Univ. Bordeaux, *PARI/GP version* `2.7.5`, 2015, available from `http://pari.math.u-bordeaux.fr/`.
11. The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 7.5.1)*, 2017, `http://www.sagemath.org`.
12. Preston Wake and Carl Wang-Erickson, *The rank of mazur's eisenstein ideal*, Preprint available at `http://arxiv.org/abs/1707.01894`.
13. Lawrence C. Washington, *Galois cohomology*, Modular Forms and Fermat's Last Theorem (Gary Cornell, Joseph H. Silverman, and Glenn Stevens, eds.), Springer-Verlag, 1997.
14. ———, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575

University of Chicago Department of Mathematics, Chicago, IL
Email address: `karl@math.uchicago.edu`

University of Chicago Department of Mathematics, Chicago, IL
Email address: `stubley@uchicago.edu`