THE UNIVERSITY OF CHICAGO

CLASS GROUPS OF KUMMER EXTENSIONS VIA CUP PRODUCTS IN GALOIS COHOMOLOGY

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
KARL SCHAEFER

CHICAGO, ILLINOIS
JUNE 2020

The only thing I am interested in using mathematics for is to have a good time and to help others do the same.

—Paul Lockhart, *A Mathematician's Lament*

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGMENTS

This dissertation is based in part on the previously posted work [12]. I have permission from my coauthor, Eric Stubley, to use this work in my dissertation, and I have tremendous gratitude for his contributions.

It is hard for me to imagine how I would have completed this project without a strong network of support. Great thanks go to my parents Stan and Suzanne Schaefer for their constant love and support from afar. You have seen more than anyone my highs and lows, and you have always been there for me when I needed it. Thanks also to my sister Madeline and to my grandparents Anne and Ed Uher and Janet and Marlin Schaefer for their unconditional love and acceptance.

I want to thank my advisor Matthew Emerton for his unwavering support over the last five years and his patience with me during times of slow progress. He has helped me become a more well-rounded mathematician. I also want to thank Frank Calegari, Romyar Sharifi, and Preston Wake for their mathematical guidance, encouragement, and interest in this project, and John Boller for helping me navigate the world of teaching. Thank you also to my undergraduate professors at Rice University: Anthony Várilly-Alvarado who nurtured my interest in number theory and Tim Cochran who first showed me what it was like to "be a mathematician".

I have many friends who have helped keep me afloat and made Chicago feel like home. I don't know where I would be without you. All of you have made me a better person and I wish I knew how to repay you. Alex Nguyen, we have been out of touch recently, but you were my first true friend. Thomas Silverman and Joel Baranowski, I am so happy that we've stayed connected since college. Dylan Quintana, thank you for your loyalty and patience and all of the support you've given me, and Ronno Das, the way you approach mathematics is inspiring. Thanks to both of you for all of the fun times with puzzles and board games we've had. And to the rest of the "Crossword Crew" – Tim Black, Alan Chang, Nat Mayer, Ben O'Connor, Mariya Sardarli, Isabella Scott, Eric Stubley, and Noah Taylor – thanks for

being a constant source of happiness.

Margaret Nichols and Nick Salter, thanks for always making sure I had plenty of cats-and-beer time. Stephen Cameron, I never thought that grading undergraduate homework assignments could be so fun – thanks for always thinking of me. Raluca Havarneanu, you were my first friend in Chicago and you always made me feel welcome. Drew Moore, you always knew how to make me laugh. MurphyKate Montee, thank you for helping me become a better teacher. Mathilde Gerbelli-Gautier, I felt like we were always on the same page and I admire your thoughtfulness even in times of stress. And to the rest of Firsteous: We finally did it!

I want to thank the rest of my Chicago crew – Andrea DaViera, Dallas Krentzel, Victoria Flores, and Michael LeChevallier – for keeping me grounded and helping me realize that there's more to life than grad school. And with much love, thank you Peter Lido for your love and support over the past two years and especially over the past six months. This has been the most challenging thing I've ever accomplished and your love and support has done more for me than I can express.

ABSTRACT

In this work, we study the class group of the number field $\mathbf{Q}(N^{1/p})$ where p is an odd prime number and $N > 1$ is coprime to p and pth-power-free. We generalize theorems of Calegari–Emerton and Lecouturier and prove a result analogous to the Herbrand–Ribet Theorem for $\mathbf{Q}(\zeta_p)$. Our main tool is Galois cohomology. We relate the p-cotorsion in the class group of $K = \mathbf{Q}(N^{1/p})$ to Selmer subgroups in the cohomology of a $(p-1)$-dimensional Galois representation. The Selmer conditions we used are designed to detect the vanishing of a global cup product using only local information. We then bound the size of the cohomology of that representation through a detailed study of the cohomology of powers of the cyclotomic character, making use of several duality theorems. This allows us to bound the rank r_K of the p-cotorsion of the class group of K above and below in terms of the numbers of prime factors of N satisfying certain congruence conditions modulo p. When $p = 3$ we completely determine the rank r_K in terms of a matrix of cubic residue symbols, and when $p = 5$ and $N \equiv 1 \bmod p$ is prime, we completely determine this rank in terms of whether or not $\prod_{k=1}^{(N-1)/2} k^k$ and $\frac{\sqrt{5}-1}{2}$ are 5th powers modulo N. For $p = 5$ and $p = 7$ we provide some data on the distribution of the rank r_K and use this to formulate a conjecture on this distribution.

CHAPTER 1

INTRODUCTION

The primary object of study in this thesis is the *class group* Cl_K of a number field K; it is a classical result in number theory that it is a finite abelian group that is trivial exactly when the ring of integers of the number field K satisfies a version of the fundamental theorem of arithmetic.

Investigating the failure of unique factorization in number fields dates back to the 19th century. For a fixed prime number p, let $1^{1/p}$ denote a primitive pth root of unity. In the 19th century, Kummer in his pursuit of Fermat's last theorem and higher reciprocity laws investigated the p-torsion in the class group of the cyclotomic field $\mathbf{Q}(1^{1/p})$, and he proved that Fermat's last theorem holds for a prime exponent p whenever the p-torsion in the class group of $\mathbf{Q}(1^{1/p})$ vanishes, that is, primes p for which $\mathrm{Cl}_{\mathbf{Q}(1^{1/p})}[p] = 0$. We call such a prime *regular*. The first irregular prime is 37.

The study of the rank of $\mathrm{Cl}_{\mathbf{Q}(1^{1/p})}$ continued into the 20th century. In the 1970s, a century after Kummer, Ribet [11] completed the proof of the Herbrand–Ribet theorem which demonstrated an equivalence between the non-vanishing of certain Galois eigenspaces in the p-torsion of $\mathrm{Cl}_{\mathbf{Q}(1^{1/p})}$ and divisibility properties of certain classical Bernoulli numbers B_k. This established an important link between the arithmetic of the cyclotomic field $\mathbf{Q}(1^{1/p})$ and special values of L-functions of Dirichlet characters and modular forms. The following decade, Mazur and Wiles [8] proved the Main conjecture of Iwasawa theory, a deep connection between p-adic L-functions and class groups.

This thesis focuses on the fields $K = \mathbf{Q}(N^{1/p})$ for pth-power-free integers $N > 1$ which are coprime to p. Denote by r_K the largest power of p dividing the size of the p-torsion subgroup of Cl_K, that is,

$$\begin{aligned} r_K &= \dim_{\mathbf{F}_p}(\mathrm{Cl}_K \otimes \mathbf{F}_p) \\ &= \dim_{\mathbf{F}_p}(\mathrm{Cl}_K/\mathrm{Cl}_K^p) \end{aligned}$$

This is the analog of the classical quantity studied by Kummer and Herbrand. 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.

Our goal in this thesis is to understand r_K. As a first step, we give coarse bounds on the size of r_K in a very general setting. For example, we prove the following theorem.

Theorem 1.0.1. *Let $p \geq 5$ be prime and let $N > 1$ be pth-power-free and coprime to p. For each prime factor q of N, let f_q be the multiplicative order of q in $\mathbf{F}_p^\times$, and for each divisor f of $p-1$, let*

$$n_f = \#\{q|N \mid q \textit{ is prime}, f_q = f\}.$$

Then,

$$n_1 + n_2 \leq r_K \leq r_{\mathbf{Q}(\zeta_p)} + \left(\sum_{f|p-1} \frac{p-1}{f} n_f \right) - 1.$$

This follows from Theorem 1.2.1 and Propositions 2.4.4 and 2.4.5.

The Herbrand–Ribet theorem gives a way to understand certain Galois eigenspaces in $\mathrm{Cl}_{\mathbf{Q}(1^{1/p})}$ in terms of analytic invariants, and a secondary goal of this thesis is to prove these kinds of statements for $\mathrm{Cl}_{\mathbf{Q}(N^{1/p})}$ for $N > 1$. For the sake of comparison, here is the Herbrand–Ribet theorem phrased using the language of unramified extensions.

Theorem (Herbrand–Ribet theorem)**.** *Fix a prime p and let $i = 2, 4, \ldots, p-3$. The field $\mathbf{Q}(1^{1/p})$ has an unramified $\mathbf{F}_p$-extension E such that $\mathrm{Gal}(E/\mathbf{Q}(1^{1/p}))$ is isomorphic to the $(1-i)$th power of the mod-p cyclotomic character as a $\mathrm{Gal}(\mathbf{Q}(1^{1/p})/\mathbf{Q})$-representation if and only if $B_i \equiv 0 \bmod p$.*

In order to prove similar theorems for the fields $K = \mathbf{Q}(N^{1/p})$ for $N > 1$, we need to find a replacement for $\mathrm{Gal}(\mathbf{Q}(1^{1/p})/\mathbf{Q})$, since $K/\mathbf{Q}$ is not Galois for pth-power-free integers $N > 1$, and for the Bernoulli numbers B_i.

The arithmetic of the field K is very sensitive to the prime factorization of N. The most tractable case is when N is prime and $N \equiv 1 \bmod p$, which is the case $n_1 = 1$ and $n_f = 0$ for

$f \geq 2$ in Theorem 1.0.1. In Chapter 3 we define the *type* of an $\mathbf{F}_p$-extension E/K, and in Section 4.2 we consider integers M_i for odd positive $i \leq p-4$, first defined by Lecouturier in [7], whose logarithms are related to special values of derivatives of L-functions. Using that data, we prove the following theorem.

Theorem 1.0.2. *Let p and $N \equiv 1 \bmod p$ be primes and assume that p is regular. Let $i = 2, 4, \ldots, p-3$. If there is an unramified $\mathbf{F}_p$-extension E/K of type i then M_{i-1} is a pth power modulo N.*

This is a corollary of Proposition 3.4.1, Lemma 4.2.8, and Theorem 4.2.1. By comparing the notion of "type" to the powers of the mod-p cyclotomic character and the numbers M_i to the classical Bernoulli numbers, we can see the similarities with the Herbrand–Ribet theorem. In this case, however, the converse does not hold in general, but it always holds for $i = 2$.

The project discussed in this thesis begins with the following theorem of Calegari and Emerton [2].

Theorem (Calegari–Emerton, 2005)**.** *Suppose that $p \geq 5$, let $N \equiv 1 \bmod p$ be prime, and let $C = \prod_{k=1}^{(N-1)/2} k^k$. If C is a pth power in $\mathbf{F}_N^\times$, then $r_K \geq 2$.*

Previous work of Merel [9] showed that the number C being 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.

In 2018, Lecouturier [7] reproved this direction without using modular forms and he proves that C is a pth power modulo N exactly when M_1 is. Independently, Wake and Wang-Erickson [17] reprove the backward direction using a new perspective on deformation rings and reformulate the condition of C being a pth power modulo N in terms of the vanishing of a particular cup product in Galois cohomology.

Calegari and Emerton also raise the question of whether or not the converse to their theorem holds. Numerical evidence suggested that the converse is true for $p = 5$, but Lecouturier found counterexamples for $p \geq 7$, for example, $p = 7, N = 337$. In this thesis, we prove that the converse is true for $p = 5$; see Theorem 1.1.5 below, which fully determines r_K in this case. Also note that Theorem 1.0.2 above explains why the converse to the theorem of Calegari–Emerton is false in general: One needs to take into account all of the M_i, not just M_1. See Section 1.1 for a summary of additional results in this thesis.

The approach we take in this thesis is similar to the framework previously used by Iimura [4] and Jaulent [5], however, we gain additional leverage by introducing cohomology to this situation, inspired by the methods of Wake–Wang-Erickson. This allows us to bypass Merel's work and connect r_K to Lecouturier's invariants more directly. The crux of the main proof involves exploiting dualities encoded in Galois cohomology, most notably, the Greenberg–Wiles Selmer group formula, a consequence of the Poitou–Tate exact sequence. This tool is traditionally used in modularity theorems, which makes its application to problems like the above unexpected. More details about this strategy are given in Section 1.2.

1.1 Summary of Results

For the remainder of this thesis, let p be an odd prime and $N > 1$ a pth-power-free integer not divisible by p. Fix algebraic closures $\overline{\mathbf{Q}}$ and $\overline{\mathbf{Q}_\ell}$ for $\mathbf{Q}$ and $\mathbf{Q}_\ell$ for all primes ℓ, respectively, and embeddings $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}_\ell}$. This in turn determines embeddings of the absolute Galois groups $G_{\mathbf{Q}_\ell} \hookrightarrow G_{\mathbf{Q}}$ for each prime ℓ. Fix a choice of $N^{1/p} \in \overline{\mathbf{Q}}$ and as before let K denote the field $\mathbf{Q}(N^{1/p})$. Fix a primitive pth root of unity which we will denote ζ_p.

As suggested above, the main results in this thesis come in two flavors: Bounds on r_K valid for any odd prime p as in Theorem 1.0.1 and Herbrand–Ribet-type theorems which hold when $N \equiv 1 \bmod p$ is also prime, like Theorem 1.0.2. It is also a theme in this thesis that for small primes N, more precise statements can be made. For general N, this can be done for $p = 3$, and if we restrict N to be a prime congruent to 1 modulo p, this can be done for $p = 3, 5, 7$, as described below.

For general N and p, Theorem 1.0.1 is the best bound we prove in this thesis using simple arithmetic properties of N and p, though it follows from a more precise and technical bound in terms of dimensions of cohomology groups; see Theorem 3.0.1. While it is stated for $p \geq 5$, the upper bound is still valid for $p = 3$, and with slight modification the lower bound holds as well:

Theorem 1.1.1. *Let $p = 3$ and $N > 1$ be cubefree and prime to 3. Let n_1 be the number of prime factors q of N congruent to 1 modulo 3 and let n_2 be the number of prime factors congruent to -1 modulo 3, not counted with multiplicity. Put $\delta = 1$ if $N \equiv \pm 1 \bmod 9$ and $\delta = 0$ otherwise. Then,*

$$\begin{aligned} n_1 + n_2 - 1 - \delta \leq r_K &\leq \left(\sum_{f \mid p-1} \frac{p-1}{f} n_f \right) - 1 \\ &= 2n_1 + n_2 - 1. \end{aligned}$$

As a basic corollary, note that this implies that if $N \not\equiv \pm 1 \bmod 9$ and if N has no prime factors that are congruent to 1 modulo 3, then r_K is precisely equal to $n_2 - 1$. Even in the general case, we can determine r_K completely in terms of the arithmetic of the prime factors of N.

Theorem 1.1.2. *Let $p = 3$ and let n_1 be the number of prime factors of N congruent to 1 modulo 3. Then we have*

$$r_K = n_1 - 1 + \dim_{\mathbf{F}_3}(\ker T)$$

where T is an explicit matrix whose coefficients are given by cubic residue symbols.

These two theorems are proven in Section 5.1 and are related to results of Gerth [3].

Now, let us restrict to the case that $N \equiv 1 \bmod p$, where we can say more. 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 [7], 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, under no regularity assumptions on p, 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, also without regularity assumptions:

Theorem 1.1.3. *Let $N \equiv 1 \bmod p$ be prime. Then,*

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

This follows from the stronger inequality of Theorem 1.2.2 combined with Theorems 1.2.3 and 1.2.4. For the sake of comparison, we also note here that Theorem 1.0.1 implies that $r_K \leq r_{\mathbf{Q}(\zeta_p)} + p - 2$.

An immediate corollary of Theorem 1.1.3 in the case of regular p is the following partial converse to the theorem of Calegari–Emerton:

Theorem 1.1.4. *Suppose that p is regular, $N \equiv 1 \bmod p$ is prime, 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 1.1.3 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 4.2.2 for this comparison.

When $p = 5$, Theorem 1.1.4 is the full converse to the theorem of Calegari–Emerton, as the only M_i is M_1. Furthermore, we give in Section 5.2 an effective method for completely determining r_K in this case:

Theorem 1.1.5. *Let $p = 5$ and $N \equiv 1 \bmod 5$ be prime. 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 1.1.4 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 1.1.4 is true in the case $p = 7$, which we prove in Section 5.3:

Theorem 1.1.6. *Let $p = 7$ and $N = 1 \bmod 7$ be prime. 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

Keeping the notation of the previous section, let S be the set of places of $\mathbf{Q}$ dividing Np along with the infinite place 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. When $N \equiv 1 \bmod p$ is prime, 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. For a general N, while we don't have an analog of M_1, we can still use cup products in Galois cohomology to control the size of Cl_K.

Let χ be the mod-p cylotomic character and 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 the group

$$\mathrm{Gal}(K(\zeta_p)/\mathbf{Q}) \cong \mathbf{Z}/p\mathbf{Z} \rtimes (\mathbf{Z}/p\mathbf{Z})^\times$$

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 the matrix representing this symmetric power is written using a slightly non-standard basis, see Remark 2.2.1 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 2.3 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 $p \geq 5$ and let $h^1_\Sigma(\mathbf{F}_p(-i))$ denote the $\mathbf{F}_p$-dimension of $H^1_\Sigma(\mathbf{F}_p(-i))$. We have*

$$n_1 + h^1_\Sigma(\mathbf{F}_p(-1)) \leq r_K \leq n_1 - 1 + \sum_{i=1}^{p-2} h^1_\Sigma(\mathbf{F}_p(-i)).$$

where n_1 is the number of prime factors of N which are congruent to 1 *modulo p.*

Chapter 3 is dedicated to the proof of this theorem.

As we will see in the course of the proof, the -1 term in the upper bound is connected to the $i = p-2$ term in the sum. In the specific case that $N \equiv 1 \bmod p$ is prime, Remark 3.4.2 tells us that we can ignore the $i = p-2$ term and thus also the -1, and we get the following theorem.

Theorem 1.2.2. *Let $p \geq 5$ and $N \equiv 1 \bmod p$ be prime. We have*

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

Note that this theorem has as a corollary the statement that if $r_K \geq 2$, then at least one of the $H^1_\Sigma(\mathbf{F}_p(-i))$ is non-zero.

Continuing to assume that $N \equiv 1 \bmod p$ is prime, we then relate the numbers $h^1_\Sigma(\mathbf{F}_p(-i))$ to the quantities M_i introduced earlier by a computation using Gauss sums.

Theorem 1.2.3. *Assume that $3 \leq i \leq p-2$ is odd and $(p, -i)$ is a regular pair, and that N is a prime congruent to 1 modulo p. Then $h^1_\Sigma(\mathbf{F}_p(-i)) = 1$ 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 4.2.1 and 4.2.2.

While not needed to establish Theorem 1.1.3, in order to prove Theorem 1.1.5 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 4.2.3.

Finally, to establish Theorem 1.1.3, we need the following theorem, which comes from duality theorems in Galois cohomology.

Theorem 1.2.4. *Let $N \equiv 1 \bmod p$ be prime. For any $1 \leq i \leq p-3$*

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

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 $h^1_\Sigma(\mathbf{F}_p(-i)) = 0$, 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 Proposition 2.4.4 and Corollary 2.4.8.

The outline of this thesis is as follows. In Chapter 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 Chapter 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 Chapter 4, we restrict our attention to the case that $N \equiv 1 \bmod p$ is prime. First, 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 Chapter 3 and then 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 Chapter 5, we analyze the cases $p = 3$, $p = 5$, and $p = 7$ in more detail, and provide the results of 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.

CHAPTER 2

GALOIS COHOMOLOGY

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 away from p, the primes dividing N, and the archimedean place ∞, 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, where S is the set of places described above.

The main point of this section is to establish some properties about a certain Selmer condition Σ in the cohomology of a family of $G_{\mathbf{Q}_S}$-representations. The definition of a Selmer condition, along with other general background on cohomology, is given in Section 2.1. We study this family of representations in Section 2.2 and define Σ in Section 2.3. The following section is where the majority of the computations with Selmer groups occur, and Section 2.5 provides some motivation for the definition of Σ by relating it to the vanishing of certain cup products.

2.1 Background and Notation

We first establish some notation and conventions used throughout the article as well as recall some facts about group and Galois cohomology. There are many primers on Galois cohomology. The author particularly appreciated the perspective in [19] and found [13] to be a useful reference.

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,
$$H^1(G_{\mathbf{Q},S}, \mathbf{F}_p(1)) = \frac{\mathbf{Z}[1/Np]^\times}{\mathbf{Z}[1/Np]^{\times p}}.$$
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 $A^\vee$ (the *linear dual* of A) and A^* (the *Tate dual* of 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 two 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. Suppose we have two classes $a \in H^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi))$ and $a' \in H^1(G_{\mathbf{Q}}, \mathbf{F}_p(\chi'))$ which correspond to 2-dimensional $G_{\mathbf{Q}}$-representations of the form

  $$\begin{pmatrix} \chi & a \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \chi' & a' \\ 0 & 1 \end{pmatrix},$$

  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 $a \cup a'$.

- More generally, if G is a group and if

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

  is a short exact sequence of G-representations defined over a field F, then the boundary map

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

  in the corresponding long exact sequence of cohomology is given by the cup product map $b \cup -$ where

$$b \in H^1(G, A \otimes C^\vee) = \operatorname{Ext}_{F[G]}(F, A \otimes C^\vee) = \operatorname{Ext}_{F[G]}(C, A)$$

is the class of B as an extension of C by 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 $I_v \subseteq G_{\mathbf{Q}_v}$ 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 $H^1_{\mathcal{L}}(G_{\mathbf{Q}}, A)$ simply 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 an integer M, we will use the notation $H^1_M(A)$ to denote the Selmer group with the unramified condition at all places not dividing M, and any behavior allowed at the places dividing M. Similarly, $H^1_\emptyset(A)$ denotes the Selmer group with the unramified condition at all places.

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 module of $G_{\mathbf{Q},S}$ as well.

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 [10]). 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 [19] 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 the places dividing 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 Representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$

Let V be the 2-dimensional $\mathbf{F}_p$-vector space on which $G_{\mathbf{Q},S}$ acts in some basis via the matrix

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

where $b \in H^1_S(\mathbf{F}_p(1))$ defined in the previous section and χ is the mod-p cyclotomic character. Many of the arguments in Chapters 3 and 4 will rely on understanding certain Selmer subgroups of the cohomology of the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ for $0 \leq i \leq p-2$ and $0 \leq j \leq i$. In this section, we collect some facts about the local cohomology $H^1(G_{\mathbf{Q}_\ell}, -)$ of these representations for use later. First, we begin with some remarks about the structure of $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$.

Remark 2.2.1. It will be useful for us in later sections to fix bases for the $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ which are "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 in which the action of $G_{\mathbf{Q},S}$ takes the above form. 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 upper-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 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

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

commutes.

Remark 2.2.2. The largest of the representations we consider is $\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1)$, which in the above basis takes the form

$$\begin{pmatrix} 1 & \chi^{-1}b & \chi^{-2}\frac{b^2}{2} & \cdots & \chi\frac{b^{p-2}}{(p-2)!} \\ & \chi^{-1} & \chi^{-2}b & \cdots & \chi\frac{b^{p-3}}{(p-3)!} \\ & & \chi^{-2} & & \vdots \\ & & & \ddots & \chi b \\ & & & & \chi \end{pmatrix}.$$

All of the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ for $0 \le i \le p-2$ and $0 \le j \le i$ that we will study are subquotients of this one representation. Visually, the subrepresentations are obtained by restricting to the upper-left $k \times k$ blocks, and the quotients by these subspaces are hence given by the lower-right $(p-1-k) \times (p-1-k)$ blocks.

With this visualization in hand, we can identify $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ by the fact that the powers of χ in the lower-right and upper-left corners are $-i$ and $j-i$, respectively. This also says that the unique 1-dimensional quotient of $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ is $\mathbf{F}_p(-i)$ and the unique 1-dimensional subrepresentation is $\mathbf{F}_p(j-i)$.

Remark 2.2.3. Let $i = p-2 \equiv -1 \bmod p-1$. The same thinking used in the previous remark suggests that we can realize $\mathrm{Sym}^{j+1} V$ as an extension of $\mathbf{F}_p$ by $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(1)$ as a $G_{\mathbf{Q},S}$-representation, which corresponds to a class in $H^1(G_{\mathbf{Q},S}, A)$ as described Section 2.1. This class is important and we give it the name $\mathbf{b}$. As a column vector, it takes the form

$$\mathbf{b} = \begin{bmatrix} \frac{b^{j+1}}{(j+1)!} \\ \frac{b^j}{j!} \\ \vdots \\ b \end{bmatrix}.$$

In order to eventually apply Theorem 2.1.2 to the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$, we need to determine $(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))^*$ which is done in the following lemma.

Lemma 2.2.4. *For $0 \leq i \leq p-2$ and $0 \leq j \leq p-2$, we have*

$$\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))^\vee \cong \mathrm{Sym}^j V \otimes \mathbf{F}_p(i-j).$$

Equivalently,

$$\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))^* \cong \mathrm{Sym}^j V \otimes \mathbf{F}_p(i-j+1).$$

Proof. We show the slightly simpler fact that for $0 \leq n \leq p-1$, $(\mathrm{Sym}^n V)^\vee \cong \mathrm{Sym}^n V \otimes \mathbf{F}_p(-n)$. The full statement follows by combining that with the fact that $\mathbf{F}_p(i)^\vee \cong \mathbf{F}_p(-i)$.

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 powers of 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 $m = -n$; indeed, 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 $m = -n$. □

We now turn to the cohomology of the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ as Galois modules for the absolute Galois groups $G_{\mathbf{Q}_\ell}$ for $\ell = p$ and ℓ dividing N. Our main tool for determining the sizes of these cohomology groups is the local Euler characteristic formula (Theorem 2.8 of [10]), which says that if A is a finite $G_{\mathbf{Q}_\ell}$-module and v_ℓ is the ℓ-adic valuation, then

$$\# H^1(G_{\mathbf{Q}_\ell}, A) = \# H^0(G_{\mathbf{Q}_\ell}, A) \cdot \# H^0(G_{\mathbf{Q}_\ell}, A^*) \cdot \ell^{v_\ell(\# A)}.$$

For $\ell = p$, we focus on the characters $\mathbf{F}_p(i)$.

Lemma 2.2.5. *The dimension of $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(i))$ is 2 if $i \equiv 0, 1 \bmod p-1$ and 1 otherwise. Furthermore, $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p}, \mathbf{F}_p(i))$ is 1-dimensional if $i \equiv 0 \bmod p-1$ and trivial otherwise.*

Proof. First notice that $p^{v_p(\#\mathbf{F}_p(i))} = p^1 = p$ for all i. Additionally, $\#H^0(G_{\mathbf{Q}_p}, \mathbf{F}_p(i))$ is p if $i \equiv 0 \bmod p-1$ and 1 otherwise; similarly, $\#H^0(G_{\mathbf{Q}_p}, \mathbf{F}_p(i)^*)$ is p if $i \equiv 1 \bmod p-1$ and 1 otherwise. The first part of the lemma then follows from the local Euler characteristic formula.

For the second part of the Lemma, recall that

$$H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p}, \mathbf{F}_p(i)) = H^1(G_{\mathbf{F}_p}, \mathbf{F}_p(i)^{I_p})$$

where I_p is the inertia group in $G_{\mathbf{Q}_p}$. The group $\mathbf{F}_p(i)^{I_p}$ is trivial when $i \not\equiv 0 \bmod p-1$ and 1-dimensional otherwise, and the result follows. (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 $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(i))$ for $i \not\equiv 0 \bmod p-1$.) □

Now we move to the primes q dividing N. As a preliminary remark, notice that the order of the mod-p cyclotomic character χ modulo q is exactly equal to the multiplicative order of q in $\mathbf{F}_p^\times$. Denote this integer by f_q and note that $m \equiv m' \bmod f_q$ is equivalent to $\mathbf{F}_p(m) \cong \mathbf{F}_p(m')$ as $G_{\mathbf{Q}_q}$-modules.

Proposition 2.2.6. *Let q be a prime factor of N and let f_q be its multiplicative order in $\mathbf{F}_p^\times$. Let $0 \le i \le p-2$ and $0 \le j \le i$. Then the dimension of $H^1(G_{\mathbf{Q}_q}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$ is 0, 1, or 2, according to the following conditions:*

1. *If $i \equiv -1 \bmod f_q$ then the dimension is at least 1 and the restriction of the class $\mathbf{b}$ defined in Remark 2.2.3 is a nonzero class in $H^1(G_{\mathbf{Q}_q}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$.*

2. *If $i \equiv j \bmod f_q$ then the dimension is at least* 1 *and*

$$\mathbf{a} = \begin{bmatrix} a \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

is a nonzero class in $H^1(G_{\mathbf{Q}_q}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$, where $a \in H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p)$ spans the 1*-dimensional unramified subspace $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_q}, \mathbf{F}_p)$.*

3. *If neither Condition 1 nor Condition 2 holds, then the dimension is* 0.

4. *If exactly one of Condition 1 and Condition 2 holds, then the dimension is* 1.

5. *If both Condition 1 and Condition 2 hold, then the dimension is* 2 *and the classes* $\mathbf{a}$ *and* $\mathbf{b}$ *form a basis of $H^1(G_{\mathbf{Q}_q}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$.*

Proof. Let $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$. We begin by appealing to the local Euler characteristic formula. As $\#A$ is prime to q, the final term $q^{v_q(\#A)}$ is always 1. The first term $\#H^0(G_{\mathbf{Q}_q}, A)$ is p exactly when the unique 1-dimensional subrepresentation of A (which is $\mathbf{F}_p(j-i)$) is isomorphic to $\mathbf{F}_p$, that is, when $j - i \equiv 0 \bmod f_q$. Otherwise, the invariants are trivial and the term is 1.

Using the same reasoning, we conclude that $\#H^0(G_{\mathbf{Q}_q}, A^*)$ is p exactly when the unique 1-dimensional subrepresentation of A^* is isomorphic to $\mathbf{F}_p$. This is equivalent to asking that the unique 1-dimensional quotient of A is isomorphic to $\mathbf{F}_p(1)$, i.e., when $-i \equiv 1 \bmod f_q$.

This shows that the dimension of $H^1(G_{\mathbf{Q}_q}, A)$ is as stated in the proposition. What is left is to determine a basis.

First suppose that $i \equiv -1 \bmod f_q$ so that $\mathrm{Sym}^j V \otimes \mathbf{F}_p(i) \cong \mathrm{Sym}^j V \otimes \mathbf{F}_p(1)$. Then the class $\mathbf{b}$ is an element of $H^1(G_{\mathbf{Q}_q}, A)$ by Remark 2.2.3. To see that it is nonzero, consider the map

$$H^1(G_{\mathbf{Q}_q}, A) \to H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p(1))$$

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

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

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

Now suppose that $i \equiv j \bmod f_q$. Then,

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

is a short exact sequence of $G_{\mathbf{Q}_q}$-modules. Consider the following piece from the corresponding long exact sequence in $G_{\mathbf{Q}_q}$-cohomology:

$$H^0(G_{\mathbf{Q}_q}, \mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i)) \to H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p) \to H^1(G_{\mathbf{Q}_q}, A)$$

The unique 1-dimensional subspace of $\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i)$ is isomorphic to $\mathbf{F}_p(-1)$. There are two cases to consider. If $f_q \neq 1$ then this has no $G_{\mathbf{Q}_q}$-fixed points and the local Euler characteristic formula tells us that $H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p)$ is 1-dimensional and hence equal to $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_q}, \mathbf{F}_p)$.

If f_q is equal to 1, then χ is trivial as a character of $G_{\mathbf{Q}_q}$ and $\zeta_p \in \mathbf{Q}_q$. This implies that:

1. The vector space $H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p)$ is two-dimensional spanned by b (corresponding to the ramified $\mathbf{F}_p$-extension $\mathbf{Q}_q(N^{1/p})/\mathbf{Q}_q$) and by an unramified class a.

2. In our chosen basis for the $\mathrm{Sym}^n V$, the representation $A \cong \mathrm{Sym}^j V$ takes the form

$$\left(\begin{array}{c|cccc}
1 & b & \frac{b^2}{2} & \cdots & \frac{b^j}{j!} \\ \hline
 & 1 & b & \cdots & \frac{b^{j-1}}{(j-1)!} \\
 & & 1 & & \vdots \\
 & & & \ddots & b \\
 & & & & 1
\end{array}\right)$$

where the lines have been added to emphasize the structure of $\mathrm{Sym}^j V$ as an extension of $\mathrm{Sym}^{j-1} V$ by $\mathbf{F}_p$.

3. In this same basis for $\mathrm{Sym}^{j-1} V$, the subspace $G_{\mathbf{Q}_q}$-fixed points is spanned by the first coordinate, i.e., is $\{[c, 0, \ldots, 0]^T \mid c \in \mathbf{F}_p\}$.

From the representation of A and its quotient $\mathrm{Sym}^{j-1} V$ in the second observation above we see that we can view A as an extension class of $\mathrm{Sym}^{j-1} V$ by $\mathbf{F}_p$ via the "row vector" cocycle

$$\begin{bmatrix} b & \frac{b^2}{2} & \cdots & \frac{b^j}{j!} \end{bmatrix} \in H^1(G_{\mathbf{Q}_q}, (\mathrm{Sym}^{j-1} V)^\vee).$$

This realizes the boundary map $H^0(G_{\mathbf{Q}_q}, \mathrm{Sym}^{j-1} V) \to H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p)$ as the cup product map

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{j-1} \end{bmatrix} \mapsto \begin{bmatrix} b & \frac{b^2}{2} & \cdots & \frac{b^j}{j!} \end{bmatrix} \cup \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{j-1} \end{bmatrix} = ba_0 + \frac{b^2}{2} a_1 + \cdots + \frac{b^j}{j!} a_{j-1}.$$

Our final observation above tells us that $a_i = 0$ for positive i so that the image of this map is the class $b \in H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p)$. Since a and b form a basis for $H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p)$, and the image of the boundary map is the span of b, we conclude that the image of

$$H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p) \to H^1(G_{\mathbf{Q}_q}, A)$$

is spanned by the image of a which is the class $\mathbf{a}$ defined above.

Finally if both Condition 1 and Condition 2 are satisfied, we see that $\mathbf{a}$ and $\mathbf{b}$ are linearly independent in $H^1(G_{\mathbf{Q}_q}, A)$ (and therefore constitute a basis) because $\mathbf{b}$ is trivial when restricted to $G_{\mathbf{Q}_q(N^{1/p})}$ (even as a cocycle) and $\mathbf{a}$ is not, as it corresponds to the unique unramified $\mathbf{F}_p$-extension of $\mathbf{Q}_q$, which is disjoint from the ramified extension $\mathbf{Q}_q(N^{1/p})$. □

2.3 The Selmer Condition Σ

We define here the Selmer condition Σ and determine its dual Σ^* for the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$. Previously, we considered the range $0 \leq i \leq p-2$, $0 \leq j \leq i$. We will only need to consider the Selmer conditions Σ and Σ^* for the range $0 \leq j \leq i-1$ (which also forces $i \geq 1$). In reference to Remark 2.2.2, these are all of the representations which don't have a 1 in the upper-left corner. For the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-j)$, we instead use the Selmer condition Λ defined in Section 3.2.

Notice using Lemma 2.2.4 that the Tate dual $(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))^*$ of a representation with $i \leq p-3$ and $j \leq i-1$ is again a representation with parameters in this range, whereas the Tate dual of $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-(p-2)) = \mathrm{Sym}^j V \otimes \mathbf{F}_p(1)$ satisfies "$j = i$". Thus in order to define the dual condition Σ^* in the case $i = p-2$, we need to define the condition Σ in the case $j = i$ despite never using it directly.

There are several equivalent characterizations of the local conditions defining Σ and Σ^*, which differ slightly depending on $i \leq p-3$ and $i = p-2$. Again referencing Remark 2.2.2, this distinction comes down to whether or not the 1-dimensional quotient is isomorphic to $\mathbf{F}_p(1)$.

For places $\ell \nmid Np$, we take the unramified condition. We will first consider the prime p, followed by the primes dividing N. For reference, we summarize the characterizations of Σ and Σ^* in Definition 2.3.1 below, leaving the details and proofs of the equivalences to Sections 2.3.1 and 2.3.2.

The conditions for Σ at the primes dividing Np can be summarized as "a multiple of

b, if that class exists, and 0 otherwise" where **b** is the restriction of the class **b** defined in Remark 2.2.3 to the appropriate local absolute Galois group. Notice also that $\Sigma \subseteq \Sigma^*$ in all cases, and the conditions for Σ and Σ^* at the primes dividing N are the same. See Section 2.5 for motivation behind this definition.

Definition 2.3.1. Let $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ for some $0 \leq i \leq p-2$ and $0 \leq j \leq i-1$. Then $\Sigma = \{L_v\}$ and its dual $\Sigma^* = \{L_v'\}$ are defined by the following local conditions:

- If $v \nmid Np$, we have $L_v = L_v' = H^1_{\mathrm{ur}}(G_{\mathbf{Q}_v}, A)$.
- If $v = q$ divides N, let f_q be its multiplicative order in $\mathbf{F}_p^\times$ and let **b** be the restriction of the global class **b** defined in Remark 2.2.3 to $G_{\mathbf{Q}_q}$. We have:

$$\begin{aligned} L_q = L_q' &= \ker\Big(\mathrm{res}\colon H^1(G_{\mathbf{Q}_q}, A) \to H^1(G_{K_q}, A)\Big) \\ &= \{c \in H^1(G_{\mathbf{Q}_q}, A) \mid \mathbf{b} \cup c = 0\} \\ &= \begin{cases} \langle \mathbf{b} \rangle & i \equiv p-2 \bmod f_q \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

- If $v = p$, let **b** be the restriction of the global class **b** defined in Remark 2.2.3 to $G_{\mathbf{Q}_p}$, and let res be the restriction map from $G_{\mathbf{Q}_p}$-cohomology to $G_{K(\zeta_p)_p}$-cohomology. We have:

$$\begin{aligned} L_p &= \mathrm{res}^{-1}(H^1_{\mathrm{ur}}(G_{K(\zeta_p)_p}, A)) \\ &= \begin{cases} \langle \mathbf{b} \rangle & i = p-2 \\ 0 = H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p}, A) & \text{otherwise} \end{cases} \end{aligned}$$

  and $L_p' = H^1(G_{\mathbf{Q}_p}, A)$ in all cases.

Remark 2.3.2. In Chapter 4, we will add the additional assumption that N is prime and congruent to 1 modulo p, and we will only need to consider the representations $\mathrm{Sym}^j V \otimes$

$\mathbf{F}_p(-i)$ for $i \leq p-3$. In that case, this means that we can just use the definition $L_p = 0$ and $L_p' = H^1(G_{\mathbf{Q}_p}, A)$. Similarly, we will have $f_N = 1$ and so we will always be in the $i \equiv p-2 \bmod f_N$ case at the prime N.

2.3.1 Conditions at p

At the prime p, we give several equivalent local conditions for classes in the cohomology of $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$. As suggested above, we will ignore the case $j = i$, except to say that we take the condition Σ to be 0 in this case so that Σ^* is the "anything goes" condition for the representations with parameter $i = p-2$.

As indicated above, the local condition at p for Σ is slightly different depending on $i \leq p-3$ and $i = p-2$, which in the end come down to the cases in Lemma 2.2.5. We define these conditions in Lemmas 2.3.4 and 2.3.5. Before continuing, we record the following general fact.

Lemma 2.3.3. *Suppose that F and F' are extensions of $\mathbf{Q}_p(\zeta_p)$, each of degree dividing p and Galois over $\mathbf{Q}_p$.*

1. *Suppose further 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.*

2. *Instead, suppose that* $\mathrm{Gal}(F/\mathbf{Q}_p(\zeta_p))$ *and* $\mathrm{Gal}(F'/\mathbf{Q}_p(\zeta_p))$ are *isomorphic as representations of* $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$ *(but not isomorphic to the trivial* 1*-dimensional representation), or that both extensions are trivial. If FF'/F is unramified, then $F = F'$.*

Proof. Both parts follow from the fact that the only unramified $\mathbf{F}_p$-extension of $\mathbf{Q}_p(\zeta_p)$ is abelian over $\mathbf{Q}_p$ and so its Galois group carries the trivial action of $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$. Disregarding the cases where F and F' are the trivial, in the first case we have

$$\mathrm{Gal}(FF'/\mathbf{Q}_p(\zeta_p)) = \mathbf{F}_p(i) \oplus \mathbf{F}_p(j)$$

for some $i \neq j \bmod p-1$. This has exactly two $(\mathbf{Z}/p\mathbf{Z})^\times$-fixed lines, so the only possible unramified subextensions of $FF'/\mathbf{Q}_p(\zeta_p)$ are $F/\mathbf{Q}_p(\zeta_p)$ and $F'/\mathbf{Q}_p(\zeta_p)$.

In the second case, if $F \neq F'$, then $\mathrm{Gal}(FF'/\mathbf{Q}_p(\zeta_p)) = \mathbf{F}_p(i)^{\oplus 2}$ for some $i \neq 0 \bmod p-1$ which also does not have a quotient on which $(\mathbf{Z}/p\mathbf{Z})^\times$ acts trivially, implying that $FF'/\mathbf{Q}_p(\zeta_p)$ is totally ramified, contradicting our assumption that FF'/F is unramified. □

We are now ready to define the local condition for Σ at the prime p. Recall that K is the field $\mathbf{Q}(N^{1/p})$. Throughout, $K(\zeta_p)_p$ denotes the completion of $K(\zeta_p)$ at a prime above p.

Lemma 2.3.4. *Let $1 \leq i \leq p-3$ and $0 \leq j \leq i-1$, and let $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$. Then the following are equivalent for a class $a \in H^1(G_{\mathbf{Q}_p}, A)$:*

1. *$a = 0$*

2. *a is unramified*

3. *a is unramified after restriction to $G_{K(\zeta_p)_p}$*

We define the local condition at p of Σ for A to be the subgroup of classes satisfying any one of the above conditions.

Proof. We need to show is that if a is unramified after restriction to the field $K(\zeta_p)_p$, then $a = 0$. As discussed in Section 2.1 for the group $G_{\mathbf{Q}}$, the class a corresponds to a $G_{\mathbf{Q}_p}$-representation which is an extension of $\mathbf{F}_p$ by A of the form

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

We prove that each a_k is trivial by strong induction on k, starting with a_i. Let M be the extension of $\mathbf{Q}_p$ defined by the kernel of the representation associated to a. By assumption, the extension $M/K(\zeta_p)_p$ is unramified.

Looking at the bottom 2×2 quotient, we notice that a_i gives an extension $L_i/\mathbf{Q}_p(\zeta_p)$ contained in M. Notice that if this extension is nontrivial, its Galois group is $\mathbf{F}_p(-i)$ as a $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$-module. Furthermore, $L_iK(\zeta_p)_p/K(\zeta_p)_p$ is unramified as this is a subextension of $M/K(\zeta_p)_p$. As $-i \neq 1 \bmod p-1$, the first part of Lemma 2.3.3 then applies to conclude that $L_i/\mathbf{Q}_p(\zeta_p)$ is unramified. Equivalently, a_i lies in $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p}, \mathbf{F}_p(-i))$ which is trivial as $i \neq 0 \bmod p-1$ by Lemma 2.2.5.

We now have that the bottom 3×3 quotient of the representation given by the matrix above is

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

Thus $a_{i-1} \in H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1-i))$ and so defines an extension $L_{i-1}/\mathbf{Q}_p(\zeta_p)$. If it is non trivial, it has an action of $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$ by χ^{1-i}. As above, the extension $L_{i-1}K(\zeta_p)_p/K(\zeta_p)_p$ is unramified and $1-i$ is still in the range for which Lemmas 2.3.3 and 2.2.5 allow us to conclude that

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

We can continue inductively in the same manner to show that $a_{i-k} = 0$ for $0 \leq k \leq j$. The two facts we need are that $\chi^{k-i} \neq \chi$ so that the first part of Lemma 2.3.3 applies, and that χ^{k-i} is nontrivial so that $H^1_{\mathrm{ur}}(G_{\mathbf{Q}_p}, \mathbf{F}_p(k-i)) = 0$. □

Lemma 2.3.5. *Let $i = p-2$ and $0 \leq j \leq i-1$, and let $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$. Then the following are equivalent for a class $a \in H^1(G_{\mathbf{Q}_p}, A)$:*

1. *a is a multiple of the restriction of the class* $\mathbf{b}$ *defined in Remark 2.2.3 to $G_{\mathbf{Q}_p}$*

2. *a is unramified after restriction to $G_{K(\zeta_p)_p}$*

We define the local condition at p of Σ for A to be the subgroup of classes satisfying either one of the above conditions.

Proof. The class $\mathbf{b}$ becomes trivial globally when restricted to $G_{K,S}$, so it is certainly unramified upon restriction to $G_{K(\zeta_p)_p}$. Conversely, we begin by following the same steps as in the proof of Lemma 2.3.4. We refer to the same field M and matrix used in that proof, and again we proceed inductively.

The class a_{p-2} gives an extension $L_{p-2}/\mathbf{Q}_p(\zeta_p)$ contained in M. Unlike before, however, the action of $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$ on $\mathrm{Gal}(L_{p-2}/\mathbf{Q}_p(\zeta_p))$ is by $\chi^{2-p} = \chi$, so the first part of Lemma 2.3.3 does not apply and so we cannot conclude that $a_{p-2} = 0$ in general. Instead, we claim that a_{p-2} is a multiple of b (which may itself be trivial) in $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1))$.

Indeed, the second part of Lemma 2.3.3 does apply in this case and we conclude that $L_{p-2} = K(\zeta_p)_p$. This implies that $a_{p-2}|_{\mathbf{Q}_p(\zeta_p)} = cb|_{\mathbf{Q}_p(\zeta_p)}$ for some $c \in \mathbf{F}_p$. But the kernel of the restriction map

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

is $H^1(\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p), \mathbf{F}_p(1))$, which is trivial, so we conclude that $a_{p-2} = cb$ in the group $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1))$ as well.

Let a' be the class $a' = a - c\mathbf{b} \in H^1(G_{\mathbf{Q}_p}, A)$ and consider the short exact sequence

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

which gives rise to an exact sequence

$$H^1(G_{\mathbf{Q}_p}, \mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(2) \to H^1(G_{\mathbf{Q}_p}, A) \to H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1)).$$

The image of the class a' under the second map is 0 and therefore a' lifts to a class in $H^1(G_{\mathbf{Q}_p}, \mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(2))$ which is still unramified when restricted to $G_{K(\zeta_p)_p}$. Noting that $2 \equiv -(p-3) \bmod p-1$, we can invoke Lemma 2.3.4 to conclude that $a' = 0$ and thus $a = c\mathbf{b}$, as desired. □

To conclude this section, we remark that Lemma 2.3.4 implies that the dual condition Σ^* to Σ for any representation $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ with $0 \leq i \leq p-3$ and $0 \leq j \leq i-1$ is the "no restrictions" condition, as the Tate duals to these representations also have parameters in the same range.

The Tate duals of the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-(p-2))$ are the representations with $j = i$, so we formally define Σ to be the trivial condition at p for the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-j)$ so that the dual condition is also "no restrictions" for the range we are interested in.

2.3.2 Conditions at the Primes Dividing N

In this section, we define the local condition at the primes dividing N for the Selmer conditions Σ and Σ^* for the representations $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ with parameters in the range $0 \leq i \leq p-2$ and $0 \leq j \leq i$. Let q be a prime which divides N and let f_q be its multiplicative order in $\mathbf{F}_p^\times$. Similarly to the previous section, we will have two equivalent formulations of this conditions, and the statements will depend slightly on i and j. Lemma 2.3.7 shows that the condition Σ^* is in fact the same as the condition Σ at q.

We will make heavy use of local Tate duality (Corollary 2.3 of [10]) which states that for a finite Galois module A, the local Tate pairing

$$H^k(G_{\mathbf{Q}_q}, A) \times H^{2-k}(G_{\mathbf{Q}_q}, A^*) \to H^2(G_{\mathbf{Q}_q}, \mathbf{F}_p(1)) = \mathbf{F}_p$$

given by the cup product is perfect, i.e., it realizes the two groups on the left as duals.

Proposition 2.2.6 gives a basis for the groups $H^1(G_{\mathbf{Q}_q}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$ in terms of congruence properties of i and j modulo f_q. By Lemma 2.2.4, we then observe that the correspondence $A \leftrightarrow A^*$ on representations of the form $\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ induces the involution

$$(j, i) \longleftrightarrow (j, -(i - j + 1)) =: (j^*, i^*)$$

on pairs (j, i) with $0 \le i \le p - 2$ and $0 \le j \le i$. Notice that

$$i \equiv -1 \bmod f_q \iff i^* \equiv j^* \bmod f_q$$

which implies that $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ satisfies "Condition 1" of Proposition 2.2.6 if and only if A^* satisfies "Condition 2" and vice versa. Further, we observe that if A satisfies both of these conditions, then it must be self-dual as a $G_{\mathbf{Q}_q}$-representation: if $i \equiv j \equiv -1 \bmod f_q$ then $i* = -(i - j + 1) \equiv -1 \equiv i \bmod f_q$ as well.

We are now able to define the local condition for Σ at q. Recall that $K = \mathbf{Q}(N^{1/p})$. The prime q totally ramifies in K, so we can unambiguously consider the completion K_q at a prime above q. As in the statement of Proposition 2.2.6, we let $\mathbf{b}$ be the restriction of the class defined in Remark 2.2.3 to $G_{\mathbf{Q}_q}$.

Lemma 2.3.6. *Let $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ for any $0 \le i \le p - 2$ and $0 \le j \le i$. Let $\tilde{\mathbf{b}} \in H^1(G_{\mathbf{Q}_q}, A)$ be $\mathbf{b}$ if that class exists, i.e. if $i \equiv -1 \bmod f_q$, and 0 otherwise. Then the following are equivalent for a class $c \in H^1(G_{\mathbf{Q}_q}, A)$:*

1. *c is in the kernel of the restriction map $H^1(G_{\mathbf{Q}_q}, A) \to H^1(G_{K_q}, A)$*
2. *c is a multiple of $\tilde{\mathbf{b}}$*
3. *$\mathbf{b} \cup c = 0$*

We define the local condition at q of Σ for A to be the subgroup of classes satisfying any one of the above conditions.

Proof. We first remark that the first two statements are equivalent. Indeed, the class $\tilde{\mathbf{b}}$ vanishes when restricted to G_{K_q}, and the class $\mathbf{a}$ does not, as argued at the end of the proof of Proposition 2.2.6. We also note that the second condition clearly implies the third: the cup product of $\mathbf{b}$ with itself vanishes because $\mathbf{b}$ lives in an odd degree of cohomology.

To see that the third condition implies the second, we invoke the local Tate duality and proceed using Proposition 2.2.6 to separate into cases.

If A is such that $H^1(G_{\mathbf{Q}_q}, A) = 0$ or $H^1(G_{\mathbf{Q}_q}, A) = \langle \mathbf{b} \rangle$, then the second condition is trivially satisfied.

If $H^1(G_{\mathbf{Q}_q}, A) = \langle \mathbf{a} \rangle$, then by the observation above the statement of the lemma we have $H^1(G_{\mathbf{Q}_q}, A^*) = \langle \mathbf{b} \rangle$ and so local Tate duality gives that $\mathbf{a} \cup \mathbf{b} \neq 0$, so the third condition above only occurs for $c = 0$.

Finally, suppose that $H^1(G_{\mathbf{Q}_q}, A) = \langle \mathbf{a}, \mathbf{b} \rangle$. Then by the same observation above, we have $A \cong A^*$. Let $\phi : A \to A^*$ be an isomorphism, and also use ϕ to denote the induced isomorphism $H^1(G_{\mathbf{Q}_q}, A) \to H^1(G_{\mathbf{Q}_q}, A^*)$. This isomorphism on cohomology groups necessarily preserves both the unramified subspace and the kernel of the restriction map to G_{K_q}-cohomology, that is, the subspaces $\langle \mathbf{a} \rangle$ and $\langle \mathbf{b} \rangle$.

Now, by local Tate duality, we know that the annihilator of $\mathbf{b}$ under the cup product is a 1-dimensional subspace which includes $\mathbf{b}$, as we are in an odd degree of cohomology. Thus this annihilator is exactly $\langle \mathbf{b} \rangle$, as desired. □

We end the section with the following lemma which demonstrates that the dual condition Σ^* is the same as the condition Σ at the prime q.

Lemma 2.3.7. *Let $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ for any $0 \leq i \leq p-2$ and $0 \leq j \leq i$. Let $L \subseteq H^1(G_{\mathbf{Q}_q}, A^*)$ be the subspace of elements satisfying the conditions in Lemma 2.3.6 and let $L^\perp$ be its annihilator under the local Tate pairing. Then $L^\perp \subseteq H^1(G_{\mathbf{Q}_q}, A)$ is also the subspace of elements satisfying the conditions in Lemma 2.3.6.*

Proof. Again we use Proposition 2.2.6 and the observation above Lemma 2.3.6. If the group $H^1(G_{\mathbf{Q}_q}, A) = 0$ then $H^1(G_{\mathbf{Q}_q}, A^*) = 0$ as well so the statement is trivial. If $H^1(G_{\mathbf{Q}_q}, A) = \langle \mathbf{a} \rangle$ then $H^1(G_{\mathbf{Q}_q}, A^*) = \langle \mathbf{b} \rangle$ and we have $L = 0$ and $L^\perp = \langle \mathbf{b} \rangle$, and vice versa if $H^1(G_{\mathbf{Q}_q}, A) = \langle \mathbf{b} \rangle$.

If $H^1(G_{\mathbf{Q}_q}, A) = \langle \mathbf{a}, \mathbf{b} \rangle$, then $H^1(G_{\mathbf{Q}_q}, A^*) = \langle \mathbf{a}, \mathbf{b} \rangle$ as well and we have $L = \langle \mathbf{b} \rangle$. $L^\perp$ is, by definition, the subspace of classes whose cup products with the classes in L vanish, but this is exactly the third condition in Lemma 2.3.6. □

2.4 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 $\mathbf{F}_p(i)$. First, we prove statements about this cohomology in general. In Chapter 4, we will assume that N is also prime and congruent to 1 modulo p and we will need more refined statements about the cohomology of the characters $\mathbf{F}_p(i)$ which can be found in the second half of this section. We begin with the following useful definition.

Definition 2.4.1. 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 2.4.2. 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 [20] for a more detailed discussion of these facts.

Recall that N is pth power free and prime to the odd prime p. For each prime factor q of N, let f_q be the multiplicative order of q in $\mathbf{F}_p^\times$, and for each divisor f of $p-1$, let

$$n_f = \#\{q | N \mid q \text{ is prime}, f_q = f\}.$$

Theorem 2.4.3. *We have*

1. *The group $H^1_S(\mathbf{F}_p)$ has dimension $1 + n_1$ and is spanned by the classes of the homomorphisms defining the degree p subfields $\mathbf{Q}(\zeta_q^{(p)})$ and $\mathbf{Q}(\zeta_{p^2}^{(p)})$ of $\mathbf{Q}(\zeta_q)$ and $\mathbf{Q}(\zeta_{p^2})$, respectively, where here q runs over the prime factors of N which are congruent to $1 \bmod p$.*

2. *The group $H^1_S(\mathbf{F}_p(1))$ has dimension $1 + \sum_{f \mid p-1} n_f$ and is spanned by the classes of p and of each of the prime factors q of N under the Kummer isomorphism*

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

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 [20].

5. *Let $i \not\equiv 0, 1 \bmod p-1$. If i is odd, put $\varepsilon = 1$; otherwise put $\varepsilon = 0$. Then we have*

$$\epsilon + \sum_{\substack{f \mid p-1 \\ i \equiv 1 \bmod f}} n_f \leq h^1_S(\mathbf{F}_p(i)) \leq r^{\chi^{1-i}}_{\mathbf{Q}(\zeta_p)} + \epsilon + \sum_{\substack{f \mid p-1 \\ i \equiv 1 \bmod f}} n_f$$

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 are a restatement of a classical reflection theorem due to Kummer. 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 $H^1_{\emptyset}(\mathbf{F}_p(1-i))$.

Finally, Part 5 follows from applying Theorem 2.1.2 to the Selmer condition S and its dual condition $S^* \subseteq \emptyset$. In this case, we know the dimensions of the local cohomology groups using Lemma 2.2.5 and Proposition 2.2.6. □

The cohomology groups $H^1_{\Sigma}(\mathbf{F}_p(i))$ play a large role in controlling the size of the class group of the field K, and we record information about the dimensions of these groups in Propositions 2.4.4 and 2.4.5.

Proposition 2.4.4. *For any $i \not\equiv 0, 1 \bmod p-1$, let $\varepsilon = 1$ if i is odd and 0 otherwise. Then we have*

$$\varepsilon - 1 + \sum_{\substack{f \mid p-1 \\ i \equiv 1 \bmod f}} n_f - \sum_{\substack{f \mid p-1 \\ i \equiv 0 \bmod f}} n_f \leq h^1_{\Sigma}(\mathbf{F}_p(i)) \leq r^{\chi^i}_{\mathbf{Q}(\zeta_p)} + \sum_{\substack{f \mid p-1 \\ i \equiv 1 \bmod f}} n_f.$$

In particular, if $p \geq 5$, we have $h^1_{\Sigma}(\mathbf{F}_p(-1)) \geq n_2$.

Proof. For the upper bound, note that $H^1_{\Sigma}(\mathbf{F}_p(i)) \subseteq H^1_N(\mathbf{F}_p(i))$ where the conditions on the latter group are "unramified at p and anything at the primes dividing N". The bound follows by applying Lemma 2.1.3 to the Selmer conditions $\emptyset$ and N and using Part 3 of the previous theorem.

For the lower bound, we use the fact that

$$H^1_\Sigma(\mathbf{F}_p(i)) = \ker\left(H^1_S(\mathbf{F}_p(i)) \to \bigoplus_{v\in S} \frac{H^1(G_{\mathbf{Q}_v}, \mathbf{F}_p(i))}{L_v}\right)$$

where L_v is the local condition defining Σ at the place v as in Definition 2.3.1. By Part 5 of Theorem 2.4.3 we have that the dimension of $H^1_S(\mathbf{F}_p(i))$ is at least ε plus the sum $\sum n_f$ over divisors f of $p-1$ with $i \equiv 1 \bmod f$. Combining the definition of Σ with Proposition 2.2.6 (for the primes dividing N) and Lemma 2.2.5 (for the prime p) we see that the local factors on the right are 1-dimensional if and only if $v = p$ or if $i \equiv 0 \bmod f_v$ and otherwise they are trivial. The kernel of this map must have dimension at least the difference of these dimensions. □

When $i = 1$, we can do better than Proposition 2.4.4 and use the explicit description of $H^1_S(\mathbf{F}_p(1))$ from Part 2 of Theorem 2.4.3 to determine $h^1_\Sigma(\mathbf{F}_p(1))$ exactly. The idea is the same as the proof of the lower bound in the previous proposition, but in this case we can express this restriction map explicitly using pth power residue symbols whose definition we recall below.

Suppose that $q \equiv 1 \bmod p$ is a prime and let ℓ be prime to both q and p. The pth power residue symbol $\left(\frac{\ell}{q}\right)_p$ is defined by

$$\left(\frac{\ell}{q}\right)_p = \ell^{\frac{q-1}{p}} \bmod q$$

and is always a power of our fixed pth root of unity ζ_p, and it is exactly the root of unity corresponding to the image of ℓ under the standard isomorphism

$$\frac{\mathbf{Q}_q^\times}{\mathbf{Q}_q^{\times p}} \cong \frac{\mathbf{Z}}{p\mathbf{Z}} \oplus \mu_p.$$

The pth power residue symbol is multiplicative in ℓ and it equals 1 exactly when ℓ is a pth power modulo q. Let $\log_p \left(\frac{\ell}{q}\right)_p$ denote the element u of $\mathbf{F}_p$ satisfying $\left(\frac{\ell}{q}\right)_p = \zeta_p^u$.

In a slight abuse of notation, we also define the symbol $\log_p \left(\frac{\ell}{p}\right)_p$ for ℓ prime to p. Fix an isomorphism from $(\mathbf{Z}/p^2\mathbf{Z})^\times$ to the additive group $\mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. An integer ℓ prime to p is a pth power modulo p^2 if and only if $\ell^{p-1} \equiv 1 \bmod p^2$. Define

$$\log_p \left(\frac{\ell}{p}\right)_p = u \in \mathbf{F}_p$$

where u satisfies $\ell^{p-1} \equiv (0, u) \bmod p^2$ under the above isomorphism. This satisfies the property that $\log_p \left(\frac{\ell}{p}\right)_p = 0$ if and only if the Kummer class of ℓ in $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1))$ is trivial.

Proposition 2.4.5. *With notation as above, write $N = \prod_{i=1}^{\omega(N)} q_i^{e_i}$ where $q_i \equiv 1 \bmod p$ for $1 \le i \le n_1$, $e_i \in \{1, 2, \ldots, p-1\}$, and $\omega(N)$ is the number of distinct prime factors of N. Let $\delta = 1$ if $\log_p \left(\frac{N}{p}\right)_p = 0$ and $\delta = 0$ otherwise. Let $T = (\varepsilon_{i,j})$ be the $(n_1 + \delta) \times \omega(N)$ matrix defined over $\mathbf{F}_p$ by:*

$$\varepsilon_{i,j} = \begin{cases} \log_p \left(\frac{q_j}{q_i}\right)_p & \text{if } i \le n_1, i \ne j \\ \log_p \left(\frac{N/q_i^{e_i}}{q_i}\right)_p^{-e_i} & \text{if } i \le n_1, i = j \\ \log_p \left(\frac{q_j}{p}\right)_p & \text{if } i = n_1 + 1 \text{ (and } \delta = 1) \end{cases}$$

Then $h^1_\Sigma(\mathbf{F}_p(1)) = \dim_{\mathbf{F}_p}(\ker T)$.

Proof. Equip $H^1_S(\mathbf{F}_p(1))$ with the basis $\langle p, q \mid q|N\rangle$ defined in Part 2 of Theorem 2.4.3. For each prime q dividing N, equip $H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p(1))$ with the basis from Proposition 2.2.6 and equip $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1))$ with the basis $\{p, u\}$ coming from Kummer theory.

As in the previous proposition, we know that

$$H^1_\Sigma(\mathbf{F}_p(1)) = \ker \left(H^1_S(\mathbf{F}_p(1)) \to \bigoplus_{v \in S} \frac{H^1(G_{\mathbf{Q}_v}, \mathbf{F}_p(1))}{L_v} \right).$$

Observe that any class in $H^1_\Sigma(\mathbf{F}_p(1))$ must lie in the span of the Kummer classes of the primes dividing N in $H^1_S(\mathbf{F}_p(i))$ because the Kummer class of p behaves badly locally at p with respect to the Selmer condition Σ. Let $\tilde{H}^1_S(\mathbf{F}_p(1))$ denote the subspace of $H^1_S(\mathbf{F}_p(1))$ spanned by the Kummer classes of the primes dividing N and notice that the image of this subspace in $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1))$ is entirely contained in $\langle u \rangle$ – call this subspace $\tilde{H}^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1))$.

This observation implies that we can realize $H^1_\Sigma(\mathbf{F}_p(1))$ as the kernel of the "restricted restriction map"

$$\tilde{H}^1_S(\mathbf{F}_p(1)) \to \left(\bigoplus_{q|N} \frac{H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p(1))}{L_q} \right) \oplus \frac{\tilde{H}^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1))}{L_p}.$$

We aim to show that T is the matrix corresponding to this linear map with respect to the bases above.

By the same arguments as in the proof of the previous proposition we see that the local factors on the right are trivial unless $v = q$ is a prime factor of N with $q \equiv 1 \bmod p$ and potentially at the prime p. At p, $L_p = \langle b \rangle$ and thus this factor is nontrivial if and only if b is trivial in $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p(1))$, i.e., if $\delta = 1$. In this case, the image of the Kummer class of a prime q_j is simply $\log_p \left(\frac{q_j}{p}\right)_p$.

Now let q and q' be distinct prime factors of N with $q \equiv 1 \bmod p$. The image of the Kummer class of q in

$$\frac{H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p(1))}{L_q} \cong \frac{\mathbf{Q}_q^\times / \mathbf{Q}_q^{\times p}}{\langle N \rangle} \cong \mu_p$$

is exactly the pth power residue symbol $\left(\frac{q_j}{q_i}\right)_p$ as q' is a unit modulo q.

Finally, we consider the image of the Kummer class of q in $H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p(1))$ for a prime $q \equiv 1 \bmod p$. The idea is the same as in the previous step. Writing $N = q^e M$ where M is prime to q, we can rearrange this to $q = N^{-e} M^{-e}$. In the quotient $H^1(G_{\mathbf{Q}_q}, \mathbf{F}_p(1))/L_q \cong \mu_p$, the image of q is $\left(\frac{M}{q_i}\right)_p^{-e}$, as desired. □

For the remainder of this section, we assume that $N \equiv 1 \bmod p$ is prime.

Theorem 2.4.6. *Let p be an odd prime and assume that $N \equiv 1 \bmod p$ is 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.

5. $h^1_{\Sigma}(\mathbf{F}_p(1)) = 1.$

Proof. The first statement follows from Parts 3 and 4 of Theorem 2.4.3 under the assumption that (p, i) is a regular pair. This implies that $(p, 1-i)$ is a regular pair as well.

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.

The final part is a corollary of Proposition 2.4.5. Under the current assumptions, the matrix T is trivial and its domain is 1-dimensional. □

Theorem 2.4.7. *Let p be an odd prime and assume that $N \equiv 1 \bmod p$ is 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 2.4.8. *Let p be an odd prime and assume that $N \equiv 1 \bmod p$ is 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 2.4.7 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 2.4.9. 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.

2.5 Cup Products and Σ

The goal of this section is to motivate the Selmer conditions Σ and Σ^*: The purpose of the Selmer condition Σ^* is to detect those classes whose cup product with the class $\mathbf{b}$ is equal to 0. That is, we can detect the vanishing of a global cup product using the collection of local conditions Σ^*.

Proposition 2.5.1. *Let* p *be an odd prime and* $0 \leq i \leq p-2$ *with* $i \neq 1$*. Assume either that* $i = 0$ *or that* $(p, 1-i)$ *is a regular pair. Let* A *and* A' *be* $G_{\mathbf{Q},S}$*-modules with a pairing* $A \otimes A' \to \mathbf{F}_p(i)$*. 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* $\mathrm{res}_q(a) \cup \mathrm{res}_q(a') \in H^2(G_{\mathbf{Q}_q}, \mathbf{F}_p(i))$ *does for each prime factor* q *of* N*.*

Proof. We first claim that the restriction map

$$H^2_S(\mathbf{F}_p(i)) \to \bigoplus_{q|N} H^2(G_{\mathbf{Q}_q}, \mathbf{F}_p(i))$$

is injective. To do this, we will show that this map is surjective and that the two terms have the same dimension.

To establish surjectivity, consider the end of the Poitou-Tate exact sequence (Theorem 4.10 of [10]) for $\mathbf{F}_p(i)$:

$$H^2_S(\mathbf{F}_p(i)) \to \bigoplus_{v\in S} H^2(G_{\mathbf{Q}_v}, \mathbf{F}_p(i)) \to H^0(G_{\mathbf{Q},S}, \mathbf{F}_p(1-i))^\vee \to 0$$

Because $i \neq 1$, we know that the final term is 0 and (using local Tate duality) that $H^2(G_{\mathbf{Q}_p}, \mathbf{F}_p(i)) = 0$, which gives us the desired surjectivity.

Recall that f_q is defined to be the multiplicative order of q in $\mathbf{F}_p^\times$, which is also equal to the order of the character χ restricted to $G_{\mathbf{Q}_q}$. Using local Tate duality again, we see that $h^2(G_{\mathbf{Q}_q}, \mathbf{F}_p(i)) = 0$ unless $i \equiv 1 \bmod f_q$, in which case it is 1. Therefore, the dimension of the product of the local second cohomology groups is the sum $\sum n_f$ taken over the divisors f of $p-1$ with $i \equiv 1 \bmod f$.

To see that this is also equal to the dimension of $H^2_S(\mathbf{F}_p(i))$, we use the global Euler characteristic formula (Theorem 5.1 of [10]) and the dimension of $H^1_S(\mathbf{F}_p(i))$ computed in Part 1 (for $i = 0$) and Part 5 (for $i \neq 0, 1$) of Theorem 2.4.3.

Therefore, this restriction map is injective. The commutativity of the diagram

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

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

Remark 2.5.2. In the notation of the previous proposition, when $(p, 1-i)$ is not a regular pair it is still (clearly) true that $a \cup a' = 0$ implies that $\mathrm{res}_q(a) \cup \mathrm{res}_q(a') = 0$ for all q dividing N. However, the converse need not hold in this setting as $h^2_S(\mathbf{F}_p(i))$ can be larger than expected and the restriction map need not be injective.

Remark 2.5.3. As was noted in the proof of Proposition 2.5.1, $H^2(G_{\mathbf{Q}_q}, \mathbf{F}_p(i)) = 0$ unless $i \equiv 1 \bmod f_q$. Therefore, to check if a cup product vanishes globally, it suffices to check locally at the primes q with $i \equiv 1 \bmod f_q$.

Even though the proof of the following proposition is short, we label it as such to indicate its importance.

Proposition 2.5.4. *Let* $A = \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ *with* $0 \le i \le p-2$ *and* $0 \le j \le i$ *and let* $a \in H^1_S(A)$. *Let* $\mathbf{b} \in H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(1))$ *as defined in Remark 2.2.3. Then* $a \in H^1_{\Sigma^*}(A)$ *if and only if* $\mathrm{res}_q(\mathbf{b}) \cup \mathrm{res}_q(a) = 0$ *for all* q *dividing* N. *In particular, if* $\mathbf{b} \cup a = 0$ *then* $a \in H^1_{\Sigma^*}(A)$.

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

Proof. The first statement is exactly the definition of the Selmer condition Σ^*; see Definition 2.3.1.

Now, we write

$$A' = \mathrm{Sym}^j V \otimes \mathbf{F}_p(1) = (\mathrm{Sym}^j V \otimes \mathbf{F}_p(i-j)) \otimes \mathbf{F}_p(j-i+1) = A^\vee \otimes \mathbf{F}_p(j-i+1).$$

This makes it evident that the cup product $\mathbf{b} \cup a$ is induced from the pairing

$$A \otimes A' \to \mathbf{F}_p(j-i+1).$$

The final statement then follows from Proposition 2.5.1. □

CHAPTER 3

SELMER GROUPS AND CL_K

The goal of this chapter 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 $\mathrm{Sym}^{p-3}V$, 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*

$$r_K = n_1 - 1 + h^1_\Sigma(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(1)).$$

Additionally, there is a filtration of $\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(1)$ *that induces the following lower and upper bounds on r_K:*

$$n_1 + h^1_\Sigma(\mathbf{F}_p(-1)) - \delta \leq r_K \leq n_1 - 1 + \sum_{i=1}^{p-2} h^1_\Sigma(\mathbf{F}_p(-i))$$

where $\delta = 1$ if $p = 3$ and $\delta = 0$ otherwise.

This is essentially Theorem 1.2.2. In the case $p \geq 5$ and $N \equiv 1 \bmod p$ is prime, the lower bound is first due to Wake–Wang-Erickson [17]. 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 certain Galois cohomology classes corresponding to unramified $\mathbf{F}_p$-extensions of K. We will also define a filtration on $H^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$ related to the filtration defined by Iimura in [4] on $\mathrm{Cl}_{K(\zeta_p)}$; see Remark 3.2.5. This filtration of Iimura is also used by Lecouturier in [7].

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 2.3. 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 $H^1_\Lambda(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$ to a filtration on the Σ-Selmer subgroup $H^1_\Sigma(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(1))$. In Section 3.4, we use this filtration to bound the rank $h^1_\Sigma(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(1))$ 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.

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

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 $K(\zeta_p)$. Therefore, we have that $A := \mathrm{Gal}(M/K(\zeta_p)) \cong (\mathbf{Z}/p\mathbf{Z})^m$ for some $m \geq 1$. This prompts the following definition.

Definition 3.1.1. With 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 section is to prove the following theorem.

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

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 q be any prime dividing N and choose a prime $\mathfrak{q}$ of M lying above q. The total ramification degree of $\mathfrak{q}$ in $M/\mathbf{Q}(\zeta_p)$ is p, since q is totally ramified in $K(\zeta_p)/\mathbf{Q}(\zeta_p)$ and unramified in $M/K(\zeta_p)$, so the inertia group at $\mathfrak{q}$ 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. □

Our next goal is to show that $1 \leq m \leq p-1$ 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 3.1.4. *The extension E/K is of type 1 (i.e. $m = 1$) if and only if E is a subfield of $E' = K(\zeta_{q_1}^{(p)}, \ldots, \zeta_{q_{n_1}}^{(p)})$, where $q_1, \ldots, q_{n_1}$ are the prime factors of N congruent to $1 \bmod p$ and $\zeta_{q_i}^{(p)}$ is any generator of the degree-p subfield of $\mathbf{Q}(\zeta_{q_i})/\mathbf{Q}$. Furthermore, in this case, $E = LK$ is the compositum of K with a $\mathbf{Z}/p\mathbf{Z}$-extension $L/\mathbf{Q}$.*

In particular, this proposition implies that there are n_1 independent unramified extensions of K of type 1 where n_1 is the number of prime factors of N congruent to $1 \bmod p$.

To establish the backward direction of Proposition 3.1.4, we need the following lemma, which is interesting in its own right and will be referenced again later.

Lemma 3.1.5. *Let q be a prime congruent to $1 \bmod p$. The completion of $\mathbf{Q}(\zeta_q^{(p)})$ at the prime above q is $\mathbf{Q}_q(q^{1/p})$.*

Proof. The two extensions of $\mathbf{Q}_q$ in question are $\mathbf{Q}_q(\zeta_q^{(p)})$ and $\mathbf{Q}_q(q^{1/p})$, both of which are totally ramified $\mathbf{F}_p$-extensions of $\mathbf{Q}_q$. Note that our assumption on q implies that $\zeta_p \in \mathbf{Q}_q$.

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

$$\mathrm{Norm}_{\mathbf{Q}_q}^{\mathbf{Q}_q(q^{1/p})}(q^{1/p}) = \prod_{i=0}^{p-1} \zeta_p^i q^{1/p}$$

$$= q$$

but we also have

$$\begin{aligned}\mathrm{Norm}_{\mathbf{Q}_q}^{\mathbf{Q}_q(\zeta_q^{(p)})}(\mathrm{Norm}_{\mathbf{Q}_q(\zeta_q^{(p)})}^{\mathbf{Q}_q(\zeta_q)}(1-\zeta_q)) &= \mathrm{Norm}_{\mathbf{Q}_q}^{\mathbf{Q}_q(\zeta_q)}(1-\zeta_q)\\ &= \prod_{j=1}^{q-1}(1-\zeta_q^j)\\ &= q.\end{aligned}$$

Therefore we conclude that $\mathbf{Q}_q(\zeta_q^{(p)}) = \mathbf{Q}_q(q^{1/p})$. □

Proof of Proposition 3.1.4. We first establish the backward direction. For each i, we have $K_{q_i} = \mathbf{Q}_{q_i}(N^{1/p})$. Writing N as $q_i^a \cdot u$ for some $1 \leq a \leq p-1$ and q_i-adic unit u, we see using Lemma 3.1.5 that

$$K_{q_i}(\zeta_{q_i}^{(p)}) = K_{q_i}(q_i^{1/p}) = K_{q_i}(u^{1/p})$$

which is an unramified extension of K_q. $\mathbf{Q}(\zeta_{q_i}^{(p)})$ is also unramified away from q_i, which lets us conclude that E'/K is unramified at all places. Finally we remark that for any degree-p subextension E of E'/K, the Galois closure of $E/\mathbf{Q}$ is $E(\zeta_p)$, so that E/K is of type 1.

Conversely, if $m = 1$ then $E(\zeta_p) = M$ is Galois over $\mathbf{Q}$ and $A = \mathrm{Gal}(E(\zeta_p)/K(\zeta_p))$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Consider the action of G on A by conjugation and recall that G is isomorphic to the semidirect product $\mathbf{Z}/p\mathbf{Z} \rtimes_\chi (\mathbf{Z}/p\mathbf{Z})^\times$. 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 $\mathrm{Gal}(E(\zeta_p)/\mathbf{Q})$ is isomorphic to $\mathbf{Z}/p\mathbf{Z} \times G$ by Lemma 3.1.3. Consider $L = E(\zeta_p)^G$, which is $\mathbf{Z}/p\mathbf{Z}$ extension of $\mathbf{Q}$. Because $\mathrm{Gal}(E(\zeta_p)/E) = (\mathbf{Z}/p\mathbf{Z})^\times$ is a subset of G we know that $L \subseteq E$. As $L \neq K$ this tells us that $E = LK$.

We claim that $L \subseteq \mathbf{Q}(\zeta_{q_1}^{(p)}, \dots, \zeta_{q_{n_1}}^{(p)})$. 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 $[\mathbf{Q}(\zeta_p) : \mathbf{Q}]$. Consider 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. The groups $\mathrm{Gal}(L(\zeta_p)/\mathbf{Q}(\zeta_p))$ and $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q}(\zeta_p))$ carry different actions of $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$, so Lemma 2.3.3 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*

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

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 admits a surjection from one of the $\mathrm{Sym}^{p-1}V_k \otimes \mathbf{F}_p(i)$; 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 $0 \leq j \leq p-1$. □

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 the group $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^\times$.*

Proof. The first part of the claim follows once we have shown that

$$H = A^{\mathbf{Z}/p\mathbf{Z}} \cap \mathrm{Gal}(M/E(\zeta_p))$$

is trivial, since $\mathrm{Gal}(M/E(\zeta_p))$ 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 action of $(\mathbf{Z}/p\mathbf{Z})^\times$. □

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 $m \leq p-1$. 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 2.2.1), $\mathrm{Gal}(M/\mathbf{Q})$ is isomorphic to the group of matrices

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

where the i, j-th entry in the upper-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.

If E/K type 1, 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 $L/\mathbf{Q}$ where L is as in the statement of Proposition 3.1.4.

Remark 3.1.8. 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 the case that $N \equiv 1 \bmod p$ is prime, we will see in Section 4.2 that the numbers M_i defined in Section 1.1 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 3.2.5.

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

In Chapter 4, we will restrict our attention to N which are prime and congruent to 1 modulo p. In this case, it is also true that there are no extensions of type $p-1$; see Remark 3.4.2.

Lemma 3.1.9. *There are no unramified* $\mathbf{F}_p$*-extensions* E/K *of type* $m = p$*.*

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). The function a_{p-1} is a homomorphism $G_{\mathbf{Q},S} \to \mathbf{F}_p$ which cuts out a $\mathbf{Z}/p\mathbf{Z}$ extension L of $\mathbf{Q}$ contained in M and hence unramified outside of S. If it were trivial, then $\dim_{\mathbf{F}_p}(A) \leq p-1$ so E/K would not have been type p. We will show that this extension L is necessarily unramified at the primes dividing N and at p as well, contradicting its existence. For p, consider the diagram of fields

$$\begin{tikzcd}
 & LK(\zeta_p) \arrow[dl, no head] \arrow[dr, no head] & \\
K(\zeta_p) \arrow[dr, no head] & & L(\zeta_p) \arrow[dl, no head] \arrow[d, no head] \\
 & \mathbf{Q}(\zeta_p) \arrow[d, no head] & L \arrow[dl, no head] \\
 & \mathbf{Q} &
\end{tikzcd}$$

locally at p. As $L \subseteq M$ we know that $LK(\zeta_p)/K(\zeta_p)$ is unramified at p. Applying Lemma 2.3.3, 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 a prime $q|N$. The inertia group(s) above q 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 $\mathbf{Q}_q$ we know by the functoriality of inertia groups that $b(\tau)$ and $a_{p-1}(\tau)$ are both non-zero, as the extensions $K(\zeta_p)$ and L defined by these classes are tamely ramified at q. 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 get

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

which is non-zero, contradicting the fact that the generator of the inertia group at q has order p. □

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 $\ell \nmid Np$

- $L_q = H^1(G_{\mathbf{Q}_q}, A)$ for q dividing N

- $L_p = \mathrm{res}^{-1}(H^1_{\mathrm{ur}}(G_{K(\zeta_p)_p}, A))$ 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 of the Galois module $\mathbf{F}_p$, 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, since such an L would give rise to a type 1 extension LK/K.

In fact, Lemma 3.1.4 implies that $h^1_\Lambda(\mathbf{F}_p) = n_1$, where n_1 is the number of prime factors of N congruent to 1 mod p, and that $H^1_\Lambda(\mathbf{F}_p)$ is spanned by the classes of the homomorphisms defining the degree p subfields $\mathbf{Q}(\zeta_q^{(p)})$ of $\mathbf{Q}(\zeta_q)$, where here q runs over the prime factors of N which are congruent to 1 mod p.

In light of this fact and the following theorem, it is useful to view $H^1_\Lambda(\mathbf{F}_p)$ as classifying extensions E/K of type 1.

In this section we prove

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

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. In the end, the proof of Theorem 3.2.2 comes down to establishing a bijection between the projectivized space $\mathbf{P}(H^1_\Lambda(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))/B)$, where B is a 1-dimensional subspace which will be specified in Lemma 3.2.3, 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 $H^1_\Lambda(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$, consider the natural filtration on the module $\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1) = \mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(2-p)$ given by

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

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 $1 \leq k \leq p-2$, we get a corresponding filtration in cohomology

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

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

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

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

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 ideally $a_0|_{G_{K,S}} \neq 0$ in order that the fixed field of its kernel $\ker(a_0|_{G_{K,S}})$, denoted E_a, is a proper $\mathbf{F}_p$ extension of K. This is true with one exception, namely the class $\mathbf{b}$ defined in Remark 2.2.3, as we show in Lemma 3.2.3.

Before introducing the lemma, we recall the definition of $\mathbf{b}$. The class $b \in H^1_S(\mathbf{F}_p(1))$ lifts to the class $\mathbf{b} \in H^1_S(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$ defined by

$$\mathbf{b} = \begin{bmatrix} \frac{b^{p-1}}{(p-1)!} \\ \frac{b^{p-2}}{(p-2)!} \\ \vdots \\ b \end{bmatrix}$$

which becomes trivial when restricted to G_K as b does.

Lemma 3.2.3. *If $a \in H^1_\Lambda(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$ is not a multiple of* $\mathbf{b}$*, 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. The proof is in two parts. First, we show that the kernel of

$$H^1_S(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1)) \to H^1(G_{K(\zeta_p),S}, \mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$$

is B, where $B = \langle \mathbf{b} \rangle$ is the span of $\mathbf{b}$. Second, we use the fact that the image of the above restriction map lies in the G-fixed points to show that a_0 is nonzero when restricted to $G_{K(\zeta_p),S}$.

Let $A = \mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1)$ 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 $H^1(G, A)$ is 1-dimensional. Since $\mathbf{b}$ is a nonzero element in this kernel, this will complete the first part of the proof. Using inflation-restriction again and recalling that $G = \mathbf{Z}/p\mathbf{Z} \rtimes_\chi (\mathbf{Z}/p\mathbf{Z})^\times$, we get that

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

where $(\mathbf{Z}/p\mathbf{Z})^\times$ acts on $\mathbf{Z}/p\mathbf{Z}$ by conjugation in G, i.e., by χ. Using this, we can explicitly compute that $H^1(\mathbf{Z}/p\mathbf{Z}, A) = \mathbf{F}_p$ carries a trivial action of $(\mathbf{Z}/p\mathbf{Z})^\times$, implying that

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

Therefore, a nonzero $a \in H^1(G_{\mathbf{Q},S}, A)$ restricts to a nonzero homomorphism

$$a|_{G_{K(\zeta_p),S}} : G_{K(\zeta_p),S} \to A = \mathbf{F}_p^{p-1}$$

which 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. □

Therefore, starting with a cohomology class a, we have produced an $\mathbf{F}_p$-extension E_a/K. We claim that the Selmer condition Λ guarantees that this extension is unramified everywhere. This is obvious for all ℓ not dividing N, p.

At the prime 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.

At primes q dividing N, Proposition 2.2.6 shows that $H^1(G_{\mathbf{Q}_q}, \mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$ is 2-dimensional, spanned by an unramified class and the restriction of class $\mathbf{b}$, and the restrictions of those classes to $H^1(G_{K_N}, \mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$ are both unramified.

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 $a - a'$ is a multiple of the class $\mathbf{b}$.

Remark 3.2.4. As mentioned above Lemma 3.1.9, when N is prime and congruent to 1 modulo p, there are no extensions E/K of type $p - 1$. In this case, it suffices to only consider the cohomology of $\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2)$ to determine r_K. Indeed, the same proof above shows that under the assumption that there are no extensions of type $p-1$, we have $r_K = h^1_\Lambda(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2))$.

Remark 3.2.5. We can now think of the filtration on $H^1_\Lambda(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$ 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 for $k < p-2$, 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 $k+1$. For $k = p-2$, due to the presence of $\mathbf{b}$, this quotient has dimension at least 2 exactly when there is an E/K of type $p-1$.

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. For $\sigma \in G$ of 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. Up to the class $\mathbf{b}$, this realizes Iimura's filtration as the "dual" to our filtration on $H^1_\Lambda(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$.

Remark 3.2.6. 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 $\langle c_1, \ldots, c_k \rangle$ 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 $\langle b, \ldots, b, a_{m-1} \rangle$.

In [14], 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 $\langle b, \ldots, b, a \rangle$.

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 section 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 $1 \leq k \leq p-2$. There is an exact sequence*

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

In particular,

$$h^1_\Lambda(\mathrm{Sym}^{p-2} V \otimes \mathbf{F}_p(1)) = n_1 + h^1_\Sigma(\mathrm{Sym}^{p-3} V \otimes \mathbf{F}_p(2)).$$

where n_1 is the number of prime factors of N congruent to $1 \bmod p$.

The last equality follows from the $k = p-2$ case of the first part of the proposition combined with Remark 3.2.1 which gives that $h^1_\Lambda(\mathbf{F}_p) = n_1$.

Let $1 \leq k \leq p-2$ 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.

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

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 $H^1_\Lambda(\mathbf{F}_p) \subseteq H^1_S(\mathbf{F}_p)$.

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

The proof of the remainder of the proposition is broken up into two parts: managing the local conditions at the primes dividing N and at p. Lemma 3.3.2 establishes Parts 1 and 2 above with Λ replaced by S and Σ replaced by Σ^* by considering the local conditions at the primes dividing N. To get the corresponding statements for Λ and Σ, we need to consider the local conditions at p, which is done in Lemma 3.3.4 the discussion immediately preceding it.

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 4.1 when we discuss issues of extending Galois representations of this kind.

Lemma 3.3.2. *For any $1 \leq i \leq p-2$, and $1 \leq j \leq i$, 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 $j+1$, which is associated to an element a in

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

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

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

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

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 $\mathbf{b}'$ 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 $\mathbf{F}_p(j-i)$. Lemma 2.2.4 shows that

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

which induces an isomorphism

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

We claim that under this isomorphism, the class $\mathbf{b}'$ is taken to (a nonzero multiple of) the class $\mathbf{b}$. Indeed, this isomorphism respects the kernel of restriction to $G_{K(\zeta_p),S}$-cohomology, which is 1-dimensional by the same argument as used in Lemma 3.2.3, and thus spanned by $\mathbf{b}'$ on the left and $\mathbf{b}$ on the right. Alternatively, we could argue that the twisted dual of "$\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i)$ as an extension of $\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i)$ by $\mathbf{F}_p(j-i)$" is exactly "$\mathrm{Sym}^j V$ as an extension of $\mathbf{F}_p$ by $\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(1)$" which is given by the class $\mathbf{b}$.

This is all to say that

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

is equal to

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

A careful (due to a difference in indexing) application of Proposition 2.5.4 tells us that this 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 $j-i=0$. □

We now turn our attention to the prime p. The fact that the image of

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

lies in $H^1_\Sigma(\mathrm{Sym}^{k-1} V \otimes \mathbf{F}_p(-k))$ is immediate from the definition of Σ given in Section 2.3.

Lemma 3.3.4. *Let $1 \leq k \leq p-2$. 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 $a = [a_1, \dots, a_k]^T$. Choose any lift $\tilde{a}$ of a to $H^1_S(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-k))$, and write it as $[a_0, a_1, \dots, a_k]^T$. First, suppose that $k \leq p-3$. 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.

If $k = p-2$, then we have that $a = [a_1, \dots, a_k]^T$ is a multiple of $\mathbf{b} = [\frac{b^k}{k!}, \dots, b]^T$, say $a = u\mathbf{b}$, when restricted to $G_{\mathbf{Q}_p}$. Also using $\mathbf{b}$ to denote $[\frac{b^{k+1}}{(k+1)!}, \frac{b^k}{k!}, \dots, b]^T$, we see that after restricting to $G_{\mathbf{Q}_p}$ we have

$$\tilde{a} - u\mathbf{b} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{bmatrix} - u \begin{bmatrix} \frac{b^{k+1}}{(k+1)!} \\ \frac{b^k}{k!} \\ \vdots \\ b \end{bmatrix} = \begin{bmatrix} a_0 - u\frac{b^{k+1}}{(k+1)!} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let a_0' denote this top entry and notice that $a_0|_{G_{K(\zeta_p)_p}} = a_0'|_{G_{K(\zeta_p)_p}}$. As in the $k \leq p-3$ case, we know that $a_0'|_{G_{\mathbf{Q}_p}}$ is a class in $H^1(G_{\mathbf{Q}_p}, \mathbf{F}_p)$ and thus can be modified to become unramified over $\mathbf{Q}_p$ and therefore over $K(\zeta_p)_p$. Modifying a_0 in the same way, we get our desired conclusion. □

3.4 Cl_K and Selmer Groups of Characters

Recall the filtration by type on $H^1_\Lambda(\mathrm{Sym}^{p-2}V \otimes \mathbf{F}_p(1))$ considered in Remark 3.2.5. As a corollary to Proposition 3.3.1, we conclude that this filtration descends to a filtration

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

In the spirit of Remark 3.2.5, and with the same caveat in the case $k = p-2$, 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. $h^1_\Sigma(\mathbf{F}_p(-1)) \leq h^1_\Sigma(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(1))$.

2. *If there is an E/K is of type $m \geq 2$, then $H^1_\Sigma(\mathbf{F}_p(1-m))$ is nontrivial. If $m = p-1$ then we can additionally conclude that $H^1_\Sigma(\mathbf{F}_p(1))/\langle b\rangle$ is nontrivial*

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

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

$$H^1_\Sigma(\mathbf{F}_p(-1)) \subseteq H^1_\Sigma(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(1)).$$

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, the size of this group is related to the number of inequivalent extensions of type m as discussed above. If $m = p-2$ then we know that the class in $H^1_\Sigma(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(1))$ witnessing E is not a multiple of $\mathbf{b}$ by Theorem 3.2.2, and the class $\mathbf{b}$ does not lie in $H^1_\Sigma(\mathrm{Sym}^{p-4}V \otimes \mathbf{F}_p(2))$.

The associated graded space of $H^1_\Sigma(\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(1))$ equipped with this filtration is

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

which proves the final part of the proposition. □

Remark 3.4.2. If we assume that N is prime and $N \equiv 1 \bmod p$, Part 5 of Theorem 2.4.6 along with Part 2 of the previous proposition imply that there are no extensions E/K of type $p-1$.

The following proposition explains the presence of the δ in Theorem 3.0.1.

Proposition 3.4.3. *Let $\delta = 1$ if $p = 3$ and $\delta = 0$ otherwise. We have $h^1_\Sigma(\mathbf{F}_p(-1)) - \delta \leq r_K$.*

Proof. This follows from Part 1 of Proposition 3.4.1 along with the discussion immediatel preceding it combined with the fact that $\mathbf{F}_p(-1) = \mathbf{F}_p(1)$ exactly when $p = 3$. □

CHAPTER 4

PRIMES $N \equiv 1$ MOD P

We now restrict our attention to the special case that N is prime and congruent to 1 modulo p. In this case, the arithmetic of K is simpler, and this allows us to have more precise control over the rank r_K. We begin in Section 4.1 where we discuss two different methods for improving the lower bound on r_K in Theorem 3.0.1. In Section 4.2 we turn to the problem of relating the Selmer groups $H^1_\Sigma(\mathbf{F}_p(i))$ to certain invariants M_i which arise from a local analysis of Gauss sums.

Throughout these sections, we will ignore extensions of type $p-1$ as none exist by Remark 3.2.4. This also allows us to ignore the Selmer group $H^1_\Sigma(\mathbf{F}_p(1))$ and focus our attention on $\mathrm{Sym}^{p-3}V \otimes \mathbf{F}_p(2)$ and the $H^1_\Sigma(\mathbf{F}_p(-i))$ for $1 \leq i \leq p-3$.

4.1 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 5.2, we show that this is true when $p = 5$. However, it is not true in general. In particular, see Section 5.3 for a detailed analysis of the possible cases when $p = 7$.

We saw in Chapter 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 the Selmer group $H^1_\Sigma(\mathrm{Sym}^{m-2}V \otimes \mathbf{F}_p(1-m))$ 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 $H^1_\Sigma(\mathrm{Sym}^{i-1}V \otimes \mathbf{F}_p(-i))$, 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 4.1.1 and 4.1.2.

It is worth remarking that for $p \geq 5$ 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 Proposition 3.4.3.) 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 4.1.1 ([17], Proposition 11.1.1)**.** *Let $p \geq 5$. If $h^1_\Sigma(\mathbf{F}_p(-1)) \neq 0$ then $r_K \geq 2$.*

Remark 4.1.2. The question of lifting representations is related to the vanishing of higher Massey products $\langle b, \dots, b, a_i \rangle$ in $G_{\mathbf{Q},S}$-cohomology. In [14], 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 4.1.2 is in terms of the vanishing of certain triple Massey products in $G_{\mathbf{Q},S}$-cohomology. Theorem 4.1.8 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 $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$.

4.1.1 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 $H^1_\Sigma(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$, for $1 \leq i \leq p-3$ 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 $a \in H^1_{\Sigma^*}(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$ 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 4.1.3. *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 2.2.6 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 the group $H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$. Let c be any class in $H^1_S(\mathbf{F}_p(j-i))$ whose image in the group $H^1(G_{\mathbf{Q}_N}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))/\langle \mathbf{b} \rangle$ 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

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

Lemma 4.1.4. *Let p be regular. Suppose that $a \in H^1_\Sigma(\mathrm{Sym}^{j-1} V \otimes \mathbf{F}_p(-i))$ for some i, j with $j - i \neq 0, 1 \bmod p-1$, 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 the group $H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$ 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 $H^1_N(\mathbf{F}_p(j-i)) = H^1_{\mathrm{spl}\ p}(\mathbf{F}_p(j-i))$. As above, we abbreviate $\mathrm{Sym}^a V \otimes \mathbf{F}_p(b)$ as $V^a(b)$.

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

We first remark that this diagram makes sense: Each of $H^1_{\mathrm{spl}\ p}(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$ and $H^1_S(\mathbf{F}_p(j-i))$ lands in H under its respective map to $H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$. 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 4.1.3, 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 $a \in H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$. Choose any lift $\tilde{a}$ of a to H and let $\overline{a}$ be the image of $\tilde{a}$ in $H^1(G_{\mathbf{Q}_p}, \mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$. 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 $H^1_{\mathrm{spl}\ p}(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$.

Now, because

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

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 $j - i \not\equiv 0, 1 \bmod p-1$, 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 4.1.5. *Let p be regular. Suppose that $a \in H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$ where i, j satisfy $j - i \not\equiv 0, 1 \bmod p-1$, that there is a lift of a to $\in H^1_{\Sigma^*}(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$, 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 $\in H^1_\Sigma(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$.

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 4.1.4 in reference to the diagram

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

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 4.1.3 and 4.1.5. We state it as its own lemma for easier reference later.

Lemma 4.1.6. *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 the previous lemma 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 2.4.6.

Remark 4.1.7. The assumption that p is regular in each of the lemmas in this section could be replaced with the more general assumption that there merely exists some lift of the class $a \in H^1_\Sigma(\mathrm{Sym}^{j-1}V \otimes \mathbf{F}_p(-i))$ to $H^1_S(\mathrm{Sym}^j V \otimes \mathbf{F}_p(-i))$. We will not need that generality.

4.1.2 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 4.1.3 to show that a class lifts into a Σ^*-Selmer group. Along with continuing to assume that $N \equiv 1 \bmod p$ is prime, 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 2.4 and 2.5. Note that the character $\chi^{\frac{p-1}{2}}$ is its own inverse.

Theorem 4.1.8. *Assume that p is regular and that $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2})) \neq 0$. Suppose that a is any nonzero class in $H^1_\Sigma(\mathbf{F}_p(\frac{p-1}{2}))$ and let $\begin{bmatrix} a' \\ a \end{bmatrix}$ be any lift of a to $H^1_S(V(\frac{p-1}{2}))$. Then we have $\begin{bmatrix} a' \\ a \end{bmatrix} \in H^1_{\Sigma^*}(V(\frac{p-1}{2}))$.*

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 2.5.4 we know that the cup product $b \cup a$ vanishes, 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

$$\begin{pmatrix} \chi^{\frac{p+1}{2}} & \chi^{\frac{p-1}{2}}b & a' \\ 0 & \chi^{\frac{p-1}{2}} & a \\ 0 & 0 & 1 \end{pmatrix}. \tag{†}$$

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

$$\begin{pmatrix} \chi^{\frac{p+1}{2}} & \chi a & ab - a' \\ 0 & \chi & -b \\ 0 & 0 & 1 \end{pmatrix}. \tag{‡}$$

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

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 (†) is a realization of $\mathrm{Gal}(K(\zeta_p)/\mathbf{Q})$ acting on $\mathrm{Gal}(L/K(\zeta_p))$, whereas the representation (‡) 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 4.1.9. *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. We can apply the same Selmer conditions Σ and Σ^* defined in Section 2.3 to the representation W. Noting that a is necessarily a nonzero multiple of b locally at N by Remark 2.4.9, we see that $W(1)$ and $V(\frac{p-1}{2})$ are isomorphic representations locally at N. In particular the results of Section 2.3 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 4.1.10. *The classes generating $H^1_S(W(1))$ and $H^1_S(W(\frac{p-1}{2}))$ are as follows.*

1. *We have that $2 + s_p \leq h^1_S(W(1)) \leq 3 + s_p$. 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 pth 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 $3 \leq h^1_S(W(\frac{p-1}{2})) \leq 4$. 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 $\begin{bmatrix} * \\ z \end{bmatrix}$ of z.

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 2.5.4, 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 $G_{\mathbf{Q}_N}$, local Tate duality along with the fact that cup products can be computed locally (Proposition 2.5.1) tell us that $a \cup b' = 0$ if and only if b' is a multiple of b locally at N. 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 2.4.6).

Using similar reasoning as in the previous paragraph, we have by local Tate duality and Proposition 2.5.1 that $a \cup z = 0$ if and only if z is a multiple of b locally at N, that is, $z \in H^1_{\Sigma^*}(\mathbf{F}_p(\frac{p-1}{2}))$. 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 4.1.11. $H^1_{\Sigma^*}(W(1)) = H^1_S(W(1))$.

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. 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 3.1.5, 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 4.1.10 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 4.1.8. By Lemma 4.1.9, 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 4.1.11 shows that $H^1_{\Sigma^*}(W(1)) = H^1_S(W(1))$, so this latter condition is immediate. □

Remark 4.1.12. 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 5.3 for examples where the automatic lifting of classes in $H^1_\Sigma(\mathbf{F}_p(i))$ to $H^1_{\Sigma^*}(V(i))$ fails.

4.2 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. As in the previous section, we continue to assume that N is prime and congruent to 1 modulo p. 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.

4.2.1 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 4.2.1. *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 2.4.6 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 4.2.2. The existence of such an element in a slightly different formulation is shown by Lecouturier in [7]. 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 3.2.5) in order to deduce bounds on the rank of the class group of K.

We include a proof of Theorem 4.2.1 that is better suited to our formulation using Selmer groups. The quantities M_i of Lecouturier play the same role as the S_i in our statement of Theorem 4.2.1; we show in Lemma 4.2.8 that $M_i = S_i^{-1}$ as elements of $\mathbf{F}_N^\times/\mathbf{F}_N^{\times p}$.

Remark 4.2.3. One can compare the role of S_i in Theorem 4.2.1 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 4.2.1 requires a regularity assumption, the setup does not. Until the beginning of the proof of Theorem 4.2.1, 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 $j : \mathbf{Q}(\zeta_p)^\times_{\mathfrak{n}} \to \mathbf{A}^\times_{\mathbf{Q}(\zeta_p)}$ 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., the class c lies in the Selmer subgroup $H^1_\Sigma(\mathbf{F}_p(-i)))$ if and only if N is in the kernel of $\psi_{c,N}$.

Remark 4.2.4. 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 4.2.5. *Let $i \not\equiv -1 \bmod p-1$ be odd. Suppose 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

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

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 4.2.6. *Let $1 \leq r < p$, $M = (N-1)/p$, 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 4.2.7. *The element $\mathcal{G}_{-i}$ is in $\mathbf{Q}(\zeta_p)^\times$, and satisfies properties (a) and (b) of Lemma 4.2.5. 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

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

The last equality follows from the fact that the character η has order p: This lets us work modulo 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 4.2.5.

To show that $\mathcal{G}_{-i}$ satisfies property (a) of Lemma 4.2.5, we recall that τ satisfies the congruence $\tau(c^{-i}) \equiv \chi^{-i}(c) \bmod p$ and verify that for $c \in (\mathbf{Z}/p\mathbf{Z})^\times$,

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

$$
\begin{aligned}
&= \mathcal{G}_{-i}^{\tau(c^{-i})} \\
&= \mathcal{G}_{-i}^{\chi^{-i}(c)}
\end{aligned}
$$

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 4.2.6, we can write

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

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

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

$$\equiv \left(\prod_{i=1}^{N-1} i\right)^{-1} \mod \pi$$
$$\equiv -1 \bmod \pi$$

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 4.2.1. 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 4.2.1. 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 2.4.2. 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 2.4.6. By Remark 4.2.4, 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 4.2.4 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 4.2.1. 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 $\mathbf{F}_N^\times$. □

4.2.2 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 4.2.8. *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 [7], 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 [6] 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. $\square$

Theorem 4.2.1 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 [17].

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 4.1.1 and Theorem 4.2.1 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 [7], 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 [6] for the construction of Γ_N.

Proposition 4.2.9. *Suppose that* $0 < m < p-1$. *Then*

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

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 4.2.9 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.

4.2.3 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 4.2.10. *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 2.4.6 and 2.4.7 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 both $H^1_N(\mathbf{F}_p(1+i)) = H^1_\Sigma(\mathbf{F}_p(1+i))$ and $H^1_p(\mathbf{F}_p(1+i)) \subseteq H^1_{\Sigma^*}(\mathbf{F}_p(1+i))$ hold. □

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 $\sigma(a) = a^{\chi^{-i}(\sigma)}$ modulo pth 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 [16] for $p = 5$ and $p = 7$.

Theorem 4.2.11. *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 4.2.12. The polynomials in the theorem above are not unique. One could use any other polynomial whose roots generate the same 1-dimensional subspace of

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

CHAPTER 5

SMALL PRIMES

We now apply the results of the previous sections to the specific cases $p = 3$, $p = 5$, and $p = 7$. For the prime $p = 3$, we can completely determine r_K in terms of the arithmetic of N. For the primes $p = 5$ and $p = 7$, we can make more precise statements if we assume that $N \equiv 1 \bmod p$ is prime.

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 1.1.4. These proofs are carried out in Sections 5.1, 5.2, and 5.3. In Section 5.4, we provide some numerical data on ranks of class groups in the cases $p = 5$ and $p = 7$.

Throughout this chapter we will often use without reference the results of Section 2.4 on the dimensions of various Selmer subgroups of $H^1_S(\mathbf{F}_p(-i))$.

5.1 $p = 3$

In the case $p = 3$, we can completely determine the rank r_K. Let n_i denote the number of prime factors of N congruent to i modulo p for $i = 1, 2$. This is consistent with our general definition for any p that n_i represents the number of prime factors of N whose multiplicative order in $\mathbf{F}_p^\times$ is i.

Theorem 3.0.1 tells us that $r_K = n_1 - 1 + h^1_\Sigma(\mathbf{F}_p(1))$ and Proposition 2.4.5 computes the final term in this expression. We summarize this in the following Theorem. See the discussion above Proposition 2.4.5 for remarks about the pth power reside symbol and an introduction to the notation $\log_p \left(\frac{\cdot}{\cdot}\right)_p$.

Theorem 5.1.1. *With notation as above, write* $N = \prod_{i=1}^{n_1+n_2} q_i^{e_i}$ *where* $q_i \equiv 1 \bmod 3$ *for* $1 \leq i \leq n_1$ *and* $e_i \in \{1, 2\}$*. Let* $\delta = 1$ *if* $N \equiv \pm 1 \bmod 9$ *and* $\delta = 0$ *otherwise. Let* $T = (\varepsilon_{i,j})$

be the $(n_1+\delta)\times(n_1+n_2)$ *matrix defined over* $\mathbf{F}_3$ *by:*

$$\varepsilon_{i,j} = \begin{cases} \log_3\left(\frac{q_j}{q_i}\right)_3 & \textit{if } i \le n_1, i \neq j \\ \log_3\left(\frac{N/q_i^{e_i}}{q_i}\right)_3^{-e_i} & \textit{if } i \le n_1, i = j \\ \log_3\left(\frac{q_j}{3}\right)_3 & \textit{if } i = n_1+1 \ (\textit{and } \delta = 1) \end{cases}$$

Then $r_K = n_1 - 1 + \dim_{\mathbf{F}_3}(\ker T)$.

5.2 $p = 5$

In the case $p = 5$, we prove the following refined version of Theorem 3.0.1 for primes N congruent to 1 modulo p.

Theorem 5.2.1. *Let* $p = 5$ *and* $N \equiv 1 \bmod 5$ *be prime. Then we have*

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

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 4.1.

Suppose $h^1_\Sigma(\mathbf{F}_p(-2)) \neq 0$, and hence also $h^1_\Sigma(\mathbf{F}_p(-1)) \neq 0$ by Corollary 2.4.8. We satisfy the conditions of Theorem 4.1.8, 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 2.4.7, we may apply Lemma 4.1.5 to choose a lift which in fact is in $H^1_\Sigma(V(-2))$. □

Combining this theorem with the results of Section 4.2 proves Theorem 1.1.5:

Proof of Theorem 1.1.5. Since each $h^1_\Sigma(\mathbf{F}_p(-i))$ is at most 1, we obtain the upper 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 4.2.1 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 4.2.1 and 4.2.11 happens if and only if both S_1 and $\frac{\sqrt{5}-1}{2}$ are 5th powers in $\mathbf{F}_N^\times$. □

See Section 5.4.1 for data on how often each of the three possible cases $r_K = 1$, 2, or 3 occurs.

5.3 $p = 7$

When $p = 7$, even when we restrict to primes $N \equiv 1 \bmod p$, 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 2.4.8, not all binary strings of length 4 may occur 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 5.3.1. *Let $p = 7$ and $N \equiv 1 \bmod 7$ be prime. 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 2.4.8 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 4.1.1 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 2.4.6 and 2.4.7 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 4.1.6 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 4.1.8 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 2.4.7, we may apply Lemma 4.1.5 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 4.1.6 to show that the class in $H^1_\Sigma(V(-3))$ lifts to a class in the group $H^1_\Sigma(\mathrm{Sym}^2 V \otimes \mathbf{F}_p(-3))$. 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

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

Theorem 1.1.6 follows by combining this result and Theorem 4.2.1: 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 5.3.1 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 for the $h^1_\Sigma(\mathbf{F}_p(-i))$ there exist $N \equiv 1 \bmod 7$ for which the corresponding r_K witness all possible values between the upper and lower bounds. See Section 5.4.2 for data on the distribution of possible 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 5.3.2. 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 4.1.6 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 4.1 are not strong enough to show that either class always contributes to r_K.

When a failure to contribute to r_K can be pinned 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 the group $H^1_S(\mathrm{Sym}^k V \otimes \mathbf{F}_p(-i))$ 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 2.4. 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 4.1.8 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 5.3.3. Suppose that the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ are 0110 and $r_K = 2$. The proof of Theorem 5.3.1 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 4.1.6 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 5.3.4. Suppose that the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ are 1011 and $r_K = 2$. As in the proof of Theorem 5.3.1, Theorem 4.1.8 shows that a_3 lifts to $H^1_{\Sigma^*}(V(-3))$, and then Lemma 4.1.5 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 4.1.5 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 5.3.5. 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 4.1.3 and 4.1.4 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.

5.4 Data for $p = 5, 7$

All computations in this section were performed using PARI/GP [15] and SageMath [16]. 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 5.3 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 4.2 is available on the second author's website. The data in Table 5.2 took approximately 10 hours to gather using a low-range commercial processor.

5.4.1 $p = 5$

For primes $N \equiv 1 \bmod 5$, $N \leq$ 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 4.2. 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 5.3 these are notated by a binary string of length 2 (00, 10, and 11). Note that by Theorem 5.2.1 the dimensions $h^1_\Sigma(\mathbf{F}_p(-i))$ 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 5.1.

Dimensions	r_K	Number of N
00	1	$253,234$
10	2	$51,613$
11	3	$12,740$
Total		$317,587$

Table 5.1: Data for $p = 5$.

From this we see that 20.26% of N in this range have $r_K \geq 2$, and of those N, 19.80% of N have $r_K \geq 3$. We expect that the quantities M_1 and $\frac{\sqrt{5}-1}{2}$ 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 $r_K \geq 2$ 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. We record this in the following conjecture.

Conjecture 5.4.1. *Among primes N congruent to* 1 *modulo* 5*,* 80% *satisfy $r_K = 1$,* 16% *satisfy $r_K = 2$, and* 4% *satisfy $r_K = 3$.*

5.4.2 $p = 7$

For primes $N \equiv 1 \bmod 7$, $N \leq$ 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 4.2. There are 960,023 such primes N, and their distribution among the possible cases is given in Table 5.2.

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 5.2: Dimensions of the $H^1_\Sigma(\mathbf{F}_p(-i))$, $p = 7$ and $N \leq 100{,}000{,}000$.

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 5.3. The empty cells in Table 5.3 are cases that are shown to never occur in Section 5.3; in particular every case not ruled out in Section 5.3 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 5.3: 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*, volume 11 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Modular representations as an introduction to the local representation theory of finite groups.

[2] Frank Calegari and Matthew Emerton. On the ramification of Hecke algebras at Eisenstein primes. *Invent. Math.*, 160(1):97–144, 2005.

[3] Frank Gerth, III. On 3-class groups of pure cubic fields. *J. Reine Angew. Math.*, 278/279:52–62, 1975.

[4] Kiyoaki Iimura. On the l-rank of ideal class groups of certain number fields. *Acta Arith.*, 47(2):153–166, 1986.

[5] Jean-François Jaulent. Unités et classes dans les extensions métabéliennes de degré nl^s sur un corps de nombres algébriques. *Ann. Inst. Fourier (Grenoble)*, 31(1):ix–x, 39–62, 1981.

[6] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[7] Emmanuel Lecouturier. On the Galois structure of the class group of certain Kummer extensions. *J. Lond. Math. Soc. (2)*, 98(1):35–58, 2018.

[8] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[9] 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.*, 477:71–115, 1996.

[10] J.S. Milne. *Arithmetic Duality Theorems.* BookSurge, LLC, second edition, 2006.

[11] Kenneth A. Ribet. A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$. *Inventiones mathematicae*, 34(3):151–162, Oct 1976.

[12] Karl Schaefer and Eric Stubley. Class groups of Kummer extensions via cup products in Galois cohomology. *Trans. Amer. Math. Soc.*, 372(10):6927–6980, 2019.

[13] Romyar Sharifi. Group and Galois cohomology. `http://math.ucla.edu/~sharifi/groupcoh.pdf`. Accessed: 2020-05-12.

[14] Romyar T. Sharifi. Massey products and ideal class groups. *J. Reine Angew. Math.*, 603:1–33, 2007.

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

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

[17] Preston Wake and Carl Wang-Erickson. The rank of Mazur's Eisenstein ideal, 2017. To appear in Duke Mathematical Journal.

[18] Preston Wake and Carl Wang-Erickson. The Eisenstein ideal with squarefree level, 2018. Preprint, available at `https://arxiv.org/abs/1804.06400`.

[19] Lawrence C. Washington. Galois cohomology. In Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors, *Modular Forms and Fermat's Last Theorem*, chapter IV. Springer-Verlag, 1997.

[20] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.