ℓ^{∞}-Selmer Groups in Degree ℓ Twist Families

ℓ^∞-Selmer groups in degree ℓ twist families

A dissertation presented

by

Alexander Smith

to

The Department of Mathematics

in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
in the subject of
Mathematics

Harvard University
Cambridge, Massachusetts

April 2020

Dissertation Advisor: Professor Elkies and Professor Kisin Alexander Smith

ℓ^∞-Selmer groups in degree ℓ twist families

Abstract

Suppose E is an elliptic curve over $\mathbb{Q}$ with no nontrivial rational 2-torsion point. Given a nonzero integer d, take E^d to be the quadratic twist of E coming from the field $\mathbb{Q}(\sqrt{d})$. For every nonnegative integer r, we will determine the natural density of d such that E^d has 2-Selmer rank r. We will also give a generalization of this result to abelian varieties defined over number fields.

These results fit into the following general framework: take ℓ to be a rational prime, take F to be number field, take ζ to be a primitive ℓ^{th} root of unity, and take N to be an ℓ-divisible $\mathbb{Z}_\ell[\zeta]$-module with an action of the absolute Galois group G_F of F. Given a homomorphism χ from G_F to $\langle\zeta\rangle$, we can define a twist N^χ, and we can define a $(1-\zeta)$-Selmer group for each of these twists. Under some hypotheses, we determine the distribution of $(1-\zeta)$-Selmer ranks in this family of degree ℓ twists. To give a non-geometric example, this framework allows us to determine some aspects of the distribution of ℓ-primary part of the class groups in families of degree ℓ extensions.

One of the main goals of this dissertation is to prove these results in a way that streamlines the approach to finding the distribution of higher Selmer groups given by the author in [48]. Along the way, we generalize the Cassels-Tate pairing to a certain pairing between Selmer groups defined from finite Galois modules. On the analytic side, we give a general bilinear character sum estimate that is suitable both for the base-case work of this dissertation and as a replacement for the Chebotarev density theorem in a future generalization of [48].

CONTENTS

Acknowledgements vi

1. Introduction 1

1.1. Outline of this work and its connection to ongoing work 11

Part 1. The Cassels-Tate pairing, Theta Groups, and 1-Cocycle Parameterization 19

2. Legendre symbols and spin 19

3. Theta groups 33

3.1. Theta groups of abelian varieties 37

3.2. Involution spin 40

4. The Cassels-Tate pairing 44

4.1. Antisymmetry 55

5. Appendix: Review of Galois cohomology 59

5.1. Review of group cohomology 59

5.2. Local bookkeeping 64

5.3. Poitou-Tate duality 71

Part 2. Bilinear character sums 72

6. Main results for bilinear character sums 72

7. Proof of Theorem 6.3 79

Part 3. The Base Case I: Linear Algebra 82

8. Twistable modules and Selmer groups 82

8.1. Tamagawa ratios 89

8.2. Dual modules and base-case Selmer groups 91

8.3. Tuple sets of twists and moment estimates 95

9. Favorable twists and the main theorems 96

9.1. Main base-case results 103

10. Base-case Selmer conditions 114
10.1. Dual modules 115
10.2. Selmer conditions 120
10.3. Some cancellable pairs 126
10.4. Main-term pairs 129
10.5. The space $\mathbf{Q}((q_s)_s)$ 132
11. Ignorable pairs 134
11.1. Characterizing non-ignorable pairs 135
11.2. Counting non-ignorable pairs 140
11.3. Bounding moments using non-ignorable pairs 144
11.4. Estimating moments using non-ignorable pairs 149

Part 4. The Base Case II: Gridding 153
12. Grids of twists 153
12.1. Grids of ideals 153
12.2. Grids of twists 158
12.3. The Chebotarev Density Theorem 164
13. Bad grids and the proof of Proposition 12.5 167
13.1. Preliminary results 167
13.2. The proof of Proposition 12.5 169
14. Proofs of the base-case theorems 177
14.1. The parity of Selmer ranks in grids 177
14.2. Moment estimates on good grids of twists 180
14.3. The proofs of the base-case Selmer rank theorems 185
References 191

ACKNOWLEDGEMENTS

I would like to thank my advisors, Noam Elkies and Mark Kisin, for their support in my development as a mathematician.

I would also like to thank Melanie Matchett Wood, Shou-Wu Zhang, Dorian Goldfeld, and Andrew Granville for their encouragement and guidance from outside the Harvard mathematics department.

I want to acknowledge Dimitris Koukoulopoulos, Peter Koymans, Adam Morgan, Jesse Thorner, and David Yang for specific insights that had a major impact on this work.

I would like to thank the many people who have had comments on previous versions of this work, including Stephanie Chan, Brian Conrad, Djordjo Milovic, Carlo Pagano, Ye Tian, and Boya Wen.

I would like to thank George Boxer, Jordan Ellenberg, Wei Ho, Barry Mazur, Hector Pasten, Karl Rubin, Bjorn Poonen, Peter Sarnak, Frank Thorne, Richard Taylor, Nicholas Triantafillou, Ila Varma, and Xinyi Yuan for helpful discussion over the course of this project.

I would also like to thank Morgan, Geoff, Sarah, Greg, and Jill.

1. INTRODUCTION

Goldfeld's Conjecture. Given an abelian variety A defined over a number field F, the Mordell-Weil theorem states that the group of F-rational points of A is a finitely-generated abelian group. There is then a well-defined nonnegative integer r called the *rank* of A over F so that there some isomrphism

$$A(F) \cong \mathbb{Z}^r \oplus A(F)_{\text{tor}}$$

of abelian groups, where $A(F)_{\text{tor}}$ denotes the subgroup of points of finite order in $A(F)$. There is no proven algorithm for calculating the rank of an abelian variety, and understanding the behavior of the ranks of abelian varieties, and in particular of elliptic curves, constitutes one of the most fundamental problems in arithmetic geometry.

There are two close analogues of rank that are of interest to us:

- We define the *analytic rank* of A/F, denoted $r_{\text{an}}(A/F)$, to be the order of vanishing of the L-function associated to E/F at $s = 1$. For $F = \mathbb{Q}$ and A an elliptic curve, this rank is well-defined; for some higher number fields and higher dimensional abelian varieties, its existence is conjectural.
- For any rational prime p, we define the p^∞-*Selmer corank* of A/F, denoted $r_{p^\infty}(A/F)$, to be the limit of the sequence

  $$r_p(A/F),\ r_{p^2}(A/F),\ r_{p^3}(A/F), \ldots,$$

  where r_n denotes the n-Selmer rank of A/F, a nonnegative integer we will define in greater detail later.

Conjecturally, we should always have

$$r_{\text{an}}(A/F) = \text{rank}(A/F) = r_{2^\infty}(A/F) = r_{3^\infty}(A/F) = r_{5^\infty}(A/F) = \ldots.$$

The equality of rank and analytic rank is the celebrated conjecture of Birch and Swinnerton-Dyer (the BSD conjecture), and the equality of rank and the p^∞-Selmer coranks would follow as a consequence of the conjectured finiteness of the Shafarevich-Tate group $Ш(A/F)$ (the Shafarevich-Tate conjecture). For now, we note the following, easily-provable estimate; for p a rational prime and $k \geq 1$, we always have

$$r_p(A/F) \geq r_{p^2}(A/F) \geq \cdots \geq r_{p^k}(A/F) \geq r_{p^\infty}(A/F) \geq \text{rank}(A/F). \tag{1.1}$$

In 1979, Goldfeld conjectured the following:

Conjecture 1.1 ([13])**.** *Given an elliptic curve $E/\mathbb{Q}$ with narrow Weierstrass form*

$$y^2 = x^3 + ax + b,$$

and given a nonzero integer d, take E^d to be the elliptic curve over $\mathbb{Q}$ with narrow Weierstrass form

$$E^d : y^2 = x^3 + d^2ax + d^3b.$$

This curve is a quadratic twist of E, and is isomorphic to E over $\mathbb{Q}(\sqrt{d})$.

Then, for $r \geq 0$,

$$\lim_{N\to\infty} \frac{\#\left\{d \,:\, 0 < |d| \leq N \;\; \textit{and} \;\; r_{\text{an}}(E^d/\mathbb{Q}) = r\right\}}{2N} = \begin{cases} 1/2 & \textit{for } r = 0 \\ 1/2 & \textit{for } r = 1 \\ 0 & \textit{for } r \geq 2. \end{cases}$$

In particular, if both the BSD conjecture and Goldfeld's conjecture hold, 100% of the curves in the quadratic twist family of a given $E/\mathbb{Q}$ will have rank at most one.

Between this dissertation and some work in preparation, we will prove an analogue of Goldfeld's conjecture for 2^∞-Selmer coranks. For technical reasons, we need to place certain restrictions on the elliptic curves we consider. These restrictions vary depending on the structure of the 2-torsion subgroup $E(\mathbb{Q})[2]$ of $E(\mathbb{Q})$.

Assumption 1.2. An elliptic curve $E/\mathbb{Q}$ obeys the assumptions of Theorem 1.3 if one of the following holds:

(1) $E(\mathbb{Q})[2] = 0$; or

(2) $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$ and, writing $\phi : E \to E_0$ for the unique isogeny of degree 2 over $\mathbb{Q}$, we have

$$\mathbb{Q}(E_0[2]) \neq \mathbb{Q} \quad \text{and} \quad \mathbb{Q}(E_0[2]) \neq \mathbb{Q}(E[2]); \quad \text{or}$$

(3) $E(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$ and E has no cyclic degree 4 isogeny defined over $\mathbb{Q}$.

We note that a "generic" elliptic curve over $\mathbb{Q}$ satisfies $E(\mathbb{Q})_{\text{tor}} = 0$, fitting it into the first case given above.

Theorem 1.3. *Suppose $E/\mathbb{Q}$ is an elliptic curve satisfying Assumption 1.2. Then, for $r \geq 0$,*

$$\lim_{N\to\infty} \frac{\#\left\{d \,:\, 0 < |d| \leq N \;\; \textit{and} \;\; r_{2^\infty}(E^d/\mathbb{Q}) = r\right\}}{2N} = \begin{cases} 1/2 & \textit{for } r = 0 \\ 1/2 & \textit{for } r = 1 \\ 0 & \textit{for } r \geq 2. \end{cases}$$

This theorem was previously shown by the author for elliptic curves within the third case of Assumption 1.2. We note the following corollaries of this statement:

Corollary 1.4. *Take $E/\mathbb{Q}$ to be an elliptic curve satisfying Assumption 1.2.*

(1) 100% of the quadratic twists of E have rank at most one.

(2) Suppose the BSD conjecture holds for 100% of the quadratic twists of E. Then Goldfeld's conjecture also holds for E, and the Shafarevich-Tate conjecture holds for 100% of the twists of E.

(3) Suppose that we have

$$r_{2^\infty}(E^d/\mathbb{Q}) = 0 \;\; \textit{or} \;\; 1 \quad \Longrightarrow \quad r_{\text{an}}(E^d/\mathbb{Q}) = r_{2^\infty}(E^d/\mathbb{Q})$$

for all nonzero integers d outside of a set of density zero. Then the BSD conjecture holds for 100% of the quadratic twists of E, and the previous part of this corollary applies.

Proof assuming Theorem 1.3. Part (1) is immediate from the fact that the 2^∞-Selmer corank is an upper bound for the rank.

Next, it is known from work of Gross and Zagier [15] and Kolyvagin [28, 27] that, for any elliptic curve $E/\mathbb{Q}$, we have

$$r_{\text{an}}(E/\mathbb{Q}) = 0 \text{ or } 1 \implies r_{\text{an}}(E/\mathbb{Q}) = \text{rank}(E/\mathbb{Q}) \quad \text{and} \quad \#Ш(E/\mathbb{Q}) < \infty. \tag{1.2}$$

Assuming BSD, the 2^∞-Selmer corank of E is an upper bound for the analytic rank of E; under the assumptions of this part, Theorem 1.3 implies

$$r_{\text{an}}(E^d/\mathbb{Q}) = \text{rank}(E^d/\mathbb{Q}) = r_{2^\infty}(E^d/\mathbb{Q}) \quad \text{and} \quad \#Ш(E/\mathbb{Q}) < \infty$$

for 100% of the quadratic twists of E.

Part (3) again follows from the above results of Gross, Zagier, and Kolyvagin. □

Statements of the form

$$r_{p^\infty}(E/\mathbb{Q}) = 0 \text{ or } 1 \implies r_{\text{an}}(E/\mathbb{Q}) = r_{p^\infty}(E/\mathbb{Q}) \tag{1.3}$$

are known as *p-converse theorems*, as the direction of the implication is the opposite of the results of Kolyvagin. These sorts of results are known in a variety of settings, with [57, Theorem 1.4] giving a broad example. Most such results explicitly rule out application for $p = 2$, with one major exception provided by the congruent number curves.

Definition 1.5. A positive integer d is called a *congruent number* if any of the following equivalent conditions is satisfied:

- There is a right triangle whose side lengths are all rational and whose area is d;

- There is a rational square number x^2 such that both $x^2 - d$ and $x^2 + d$ are also rational squares;
- The elliptic curve

$$E_{\text{CN}}^d : y^2 = x^3 - d^2 x$$

has positive rank over the rational numbers.

In the first and second guises, congruent numbers have been studied since the Islamic golden age [6], with recent attention to the problem coming from its connection to the theory of elliptic curves [56].

The curve E_{CN}^1 satisfies the third part of Assumption 1.2, so Theorem 1.3 applies to it. Furthermore, recent work of Kriz [31] gives that (1.3) holds for the curves of the form $E_{\text{CN}}^d/\mathbb{Q}$ when $p = 2$. As a consequence, Goldfeld's conjecture holds for the curve E_{CN}^1, and the BSD and Shafarevich-Tate conjectures hold for 100% of the curves in its quadratic twist family. Furthermore, from 2-Selmer rank parity considerations of Monsky [18], we have the following:

Corollary 1.6. *Among the positive integers equal to* 1*,* 2*, or* 3 *mod* 8*,* 0% *are congruent numbers.*

Further, among the positive integers equal to 5*,* 6*, or* 7 *mod* 8*,* 100% *are congruent numbers.*

Selmer ranks. Our results for r_{2^∞} are consequences of distributional results on the Selmer ranks $r_2, r_4, r_8 \ldots$. We start by defining these ranks.

Definition 1.7. Suppose A is an abelian variety over a number field F and suppose that n is a positive integer. Writing G_F for the absolute Galois group of F, the set of algebraic points on A forms a G_F-module. Writing $A[n]$ for the n-torsion of A, we have an exact sequence

$$0 \to A[n] \to A \xrightarrow{\cdot n} A \to 0.$$

From the associated long exact sequence in group cohomology, we have an exact sequence

$$0 \to A(F)/nA(F) \to H^1(G_F, A[n]) \to H^1(G_F, A).$$

Given a place v of F, write G_v for the absolute Galois group of a completion F_v. We define

$$\text{Sel}^n(A/F) = \ker\left(H^1(G_F, A[n]) \to \prod_{v \text{ of } F} H^1(G_v, A)\right),$$

so we have a natural inclusion

$$A(F)/nA(F) \hookrightarrow \text{Sel}^n(A/F).$$

We then define the n-*Selmer rank* $r_n(A/F)$ to be the maximal r so there is some injection

$$(\mathbb{Z}/n\mathbb{Z})^r \hookrightarrow \text{Sel}^n(A/F)\Big/\text{im}(A(F)_{\text{tor}}).$$

Remark 1.8. In the literature, it is typical to leave out the correction for $A(F)_{\text{tor}}$ in the above definition. We have included it because it simplifies our theorem statements slightly and because this definition still satisfies

$$r_n(A/F) \geq \text{rank}(A/F).$$

Next, we give the probabilities that will appear in our main results

Definition 1.9. Given $n \geq j \geq 0$, take

$$P^{\text{Alt}}(j \mid n)$$

to be the probability that a a uniformly selected alternating $n \times n$ matrix with entries in $\mathbb{F}_2$ has kernel of rank exactly j. The is zero unless j and n have the same parity.

We also will define

$$P^{\text{Alt}}(j \mid 2\infty + b) = \lim_{n\to\infty} P^{\text{Alt}}(j \mid 2n + b) \quad \text{and}$$
$$P^{\text{Alt}}(j \mid \infty) = \frac{1}{2}\left(P^{\text{Alt}}(j \mid 2\infty) + P^{\text{Alt}}(j \mid 2\infty + 1)\right).$$

Theorem 1.10. *Suppose $E/\mathbb{Q}$ is an elliptic curve that fits into either the first or third case of Assumption 1.2. Given $k \geq 1$ and any sequence of integers*

$$r_2 \geq r_4 \geq \cdots \geq r_{2^k} \geq 0,$$

we have

$$\lim_{N\to\infty} \frac{\#\{d \,:\, 0 < |d| < N,\ r_2(E^d) = r_2,\ \dots\ r_{2^k}(E^d) = r_{2^k}\}}{2N}$$
$$= P^{\text{Alt}}(r_{2^k} \big| r_{2^{k-1}}) \cdot P^{\text{Alt}}(r_{2^{k-1}} \big| r_{2^{k-2}}) \cdot \cdots\cdot P^{\text{Alt}}(r_4 \big| r_2) \cdot P^{\text{Alt}}(r_2 \big| \infty).$$

To put it another way, as d varies, the sequence $(r_2(E^d_{\text{CN}}), r_4(E^d_{\text{CN}}), \dots)$ behaves like a time homogeneous Markov chain, and we give a representation of this Markov chain in the left part of Figure 1. The probability of starting in an even state is 50%, and the probability of starting in an odd state is 50%. The terminal states of this process are 0 and 1, and we derive the first and third cases of Theorem 1.3 as a consequence.

We also note that this result is consistent with the BKLPR heuristics for 2^∞-Selmer groups [1]. For general $k \geq 1$, the above statement is proved by the author in [48] for elliptic curves in the third case.

In this dissertation, we will fully prove this statement in the case $k = 1$. We can phrase this more explicitly as follows:

Theorem. *Suppose $E/\mathbb{Q}$ is an elliptic curve that fits into either the first or third case of Assumption 1.2. Given $r_2 \geq 0$, we have*

$$\lim_{N\to\infty} \frac{\#\{d \,:\, 0 < |d| < N,\ r_2(E^d) = r_2\}}{2N} = \alpha \cdot \frac{2^{r_2}}{(2^{r_2} - 1)(2^{r_2-1} - 1)\dots(2^1 - 1)},$$

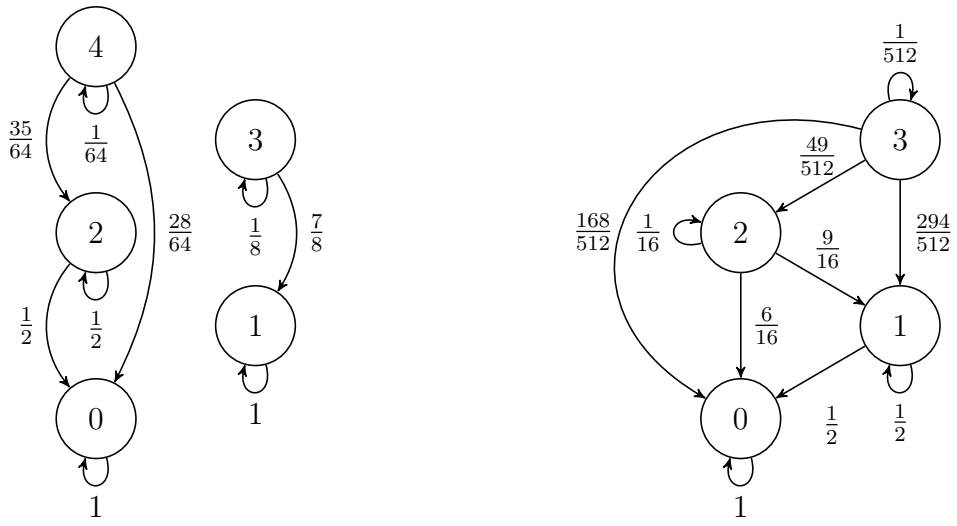

FIGURE 1. Diagrams for the Markov chains that model 2^k-Selmer ranks (on the left) and 2^k-class ranks (on the right). Each diagram omits infinitely many possible higher-rank states.

where we have taken

$$\alpha = \frac{1}{2} \cdot \prod_{i=0}^{\infty} \left(1 - 2^{-2i-1}\right) \approx .2097.$$

This was proved by Kane for curves in the third case of Assumption 1.2 [22].

We have a similar but more complicated result for elliptic curves with partial rational 2-torsion; this result will suffice to prove Theorem 1.3 for curves in the second case. We will give this result as Theorem 9.19.

Class ranks. We start with our result on the 2-primary class torsion of imaginary quadratic fields.

Notation 1.11. Given an imaginary quadratic field K, take $r_2(K) \geq r_4(K) \geq \dots$ to be the unique sequence of nonnegative integers satisfying

$$\mathrm{Cl}\, K[2^\infty] \;\cong\; (\mathbb{Z}/2\mathbb{Z})^{r_2(K)-r_4(K)} \oplus (\mathbb{Z}/4\mathbb{Z})^{r_4(K)-r_8(K)} \oplus \dots$$

and $\lim_{k\to\infty} r_{2^k}(K) = 0$.

As before, we need some notation for our probability distribution. We have no alternating restriction this time, which will be consistent with the fact that every class group is finite

Definition 1.12. For $n \geq j \geq 0$, take

$$P^{\text{Mat}}(j \mid n)$$

to be the probability that a uniformly selected $n \times n$ matrix with entries in $\mathbb{F}_2$ has kernel of rank exactly j.

We also use the notation

$$P^{\text{Mat}}(j \mid \infty) = \lim_{n \to \infty} P^{\text{Mat}}(j \mid n).$$

Theorem 1.13. *Given $k \geq 2$ and any sequence of integers*

$$r_4 \geq \cdots \geq r_{2^k} \geq 0,$$

we have

$$\lim_{N \to \infty} \frac{\#\left\{0 < d < N \,:\, r_4\left(\mathbb{Q}(\sqrt{-d})\right) = r_4,\, \ldots,\, r_{2^k}(\mathbb{Q}(\sqrt{-d})) = r_{2^k}\right\}}{N}$$
$$= P^{\text{Mat}}(r_{2^k} \big| r_{2^{k-1}}) \cdot P^{\text{Mat}}(r_{2^{k-1}} \big| r_{2^{k-2}}) \cdot \cdots \cdot P^{\text{Mat}}(r_8 \big| r_4) \cdot P^{\text{Mat}}(r_4 \big| \infty).$$

The distribution of sequences of 2^k-class ranks is again given by a Markov chain, and we give a representation of this Markov chain in the right part of Figure 1. In the case $k = 2$, the above theorem is a consequence of work of Fouvry and Klüners in [9]. Theorem 1.13 is consistent with what is predicted by Gerth's extension of the Cohen-Lenstra heuristic for the distribution of class groups [12, 4]. It is the third major result towards proving this heuristic for imaginary quadratic fields, after the result of Davenport-Heilbronn on 3-torsion [5] and the result of Fouvry and Klüners on 4-class groups.

We note that $\mathrm{Cl}\,\mathbb{Q}(\sqrt{-d})[2]$ has unbounded average size, per Gauss's genus theory, which is why we remove it from consideration above. A similar consideration explains our notation below.

Notation 1.14. Take F to be a number field, take ℓ to be a rational prime, and take K to be a degree ℓ Galois extension of F. Then $\mathrm{Cl}\,K$ is a $\mathrm{Gal}(K/F)$ module. Take ζ to be a primitive ℓ^{th} root of unity, and choose some isomorphism from $\langle\zeta\rangle$ to $\mathrm{Gal}(K/F)$. Under this isomorphism,

$$\mathrm{Cl}\,K/(\mathrm{Cl}\,K)^{\mathrm{Gal}(K/F)}$$

is a $\mathbb{Z}[\zeta]$ module. Writing $\omega = 1-\zeta$, there is a unique sequence of nonnegative integers

$$r_\omega(K) \geq r_{\omega^2}(K) \geq \dots$$

with limit zero for which there is some isomorphism

$$\mathrm{Cl}\,K[\ell^\infty]/(\mathrm{Cl}\,K[\ell^\infty])^{\mathrm{Gal}(K/F)} \;\cong\; (R/\omega R)^{r_\omega(K)-r_{\omega^2}(K)} \oplus (R/\omega^2 R)^{r_{\omega^2}(K)-r_{\omega^3}(K)} \dots,$$

where R is taken to be $\mathbb{Z}_\ell[\zeta]$. This defines the sequence of ω^k-class ranks of our field extension.

For this more general situation, we will need more general notation for our distribution.

Definition 1.15. Given nonnegative integer j and n, and given an integer u and a rational prime ℓ, take

$$P_{u,\ell}^{\mathrm{Mat}}(j \mid n)$$

to be the probability that a uniformly selected $n \times (n+u)$ matrix with entries in $\mathbb{F}_\ell$ has kernel of rank exactly j.

We also use the notation

$$P_{u,\ell}^{\mathrm{Mat}}(j \mid \infty) = \lim_{n\to\infty} P_{u,\ell}^{\mathrm{Mat}}(j \mid n).$$

Theorem 1.16. *Take F to be a number field with r_1 real embeddings and r_2 conjugate pairs of complex embeddings. Take ℓ to be a rational prime such that*

$$\mu_{2\ell} \not\subset F.$$

If $\ell = 2$, take r_1' to be an integer satisfying $0 \leq r_1' \leq r_1$. If $\ell > 2$, take $r_1' = r_1$. We define

$$u = -r_2 - r_1'.$$

For $H > 0$, define

$$X_{F,\ell,r_1'}(H) = \Big\{K/F \text{ Gal. of deg. } \ell \,:\, |\Delta_K| \leq H,\ K/F \text{ splits at exactly } r_1' \text{ real places}\Big\},$$

where Δ_K denotes the discriminant of $K/\mathbb{Q}$.

Then, given $k \geq 1$ and any sequence of integers

$$r_\omega \geq r_{\omega^2} \geq \cdots \geq r_{\omega^k} \geq 0,$$

we have

$$\lim_{H\to\infty} \frac{\#\left\{K \in X_{F,\ell,r_1'}(H) \,:\, r_\omega(K) = r_\omega,\, \ldots,\, r_{\omega^k}(K) = r_{\omega^k}\right\}}{\#X_{F,\ell,r_1'}(H)}$$
$$= P_{u,\ell}^{Mat}(r_{\omega^k} \,|\, r_{\omega^{k-1}}) \cdot \cdots \cdot P_{u,\ell}^{Mat}(r_{\omega^2} \,|\, r_\omega) \cdot P_{u,\ell}^{Mat}(r_\omega \,|\, \infty),$$

where our notation comes from Notation 1.14.

Conditionally on GRH, this result was previously known for Galois extensions of $\mathbb{Q}$ due to work of Koymans and Pagano [30], building off base-case work of Klys that was also conditional on GRH [26]. In this dissertation, we will prove this result in the case that $k = 1$ in a way suitable for our proofs for $k > 1$.

1.1. **Outline of this work and its connection to ongoing work.** The main $k = 1$ results given above are consequences of Theorem 9.14 and Theorem 9.10, statements built out of

the notation of Sections 8 and Section 9.1. As we mention at the beginning of Section 8, the ω-Selmer groups considered in these sections are easier to control than other Selmer groups. This is ultimately a consequence of the following observation: given an abelian variety A/F, and given a quadratic twist A^d of this variety, the geometric isomorphism of A and A^d descends to an isomorphism

$$A[2] \cong A^d[2]$$

of finite group varieties over F. Because of this, the 2-Selmer groups of A and A^d can be viewed as subgroups of the same cohomology group $H^1(G_F, A[2])$.

This group is still infinite, which is nonideal for an ambient space where our objects of interest live. Our workaround is easiest to explain in the case of an elliptic curve $E/\mathbb{Q}$ with full rational 2-torsion. In this case, if we choose a basis e_1, e_2 of $E[2]$, we have an isomorphism

$$B_0 : \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \xrightarrow{\sim} \text{Hom}(G_F, E[2]) = H^1(G_F, E[2])$$

given by

$$(d_1, d_2) \mapsto \left(\sigma \mapsto e_1 \cdot \tfrac{\sigma(\sqrt{d_1})}{\sqrt{d_1}} \; + \; e_2 \cdot \tfrac{\sigma(\sqrt{d_2})}{\sqrt{d_2}}\right).$$

This parameterizes cocycles in $E[2]$ as pairs of squarefree integers.

Take $\mathscr{V}_0$ to be a finite set of places including 2, ∞, and all places where E has bad reduction. Write $\mathscr{D}(\mathscr{V}_0)$ for the set of squarefree integers divisible only by primes in $\mathscr{V}_0$. Given a sequence $p_1, \ldots, p_r$ of distinct primes outside $\mathscr{V}_0$, we can then define a map

$$B_{(p_i)_i} : \mathscr{D}(\mathscr{V}_0) \oplus \mathscr{D}(\mathscr{V}_0) \oplus \mathbb{F}_2^r \oplus \mathbb{F}_2^r \xrightarrow{\sim} \ker \left(H^1(G_F, E[2]) \to \prod_{\substack{v \notin \\ \mathscr{V}_0 \cup \{p_1, \ldots, p_r\}}} H^1(I_v, E[2]) \right)$$

by

$$B_{(p_i)_i}\Big(d_{01},\, d_{02},\, (v_{i1})_i,\, (v_{i2})_i\Big) \;=\; B_0\Big(d_{01} \cdot p_1^{v_{11}} \ldots p_r^{v_{r1}},\;\; d_{02} \cdot p_1^{v_{12}} \ldots p_r^{v_{r1}}\Big).$$

Write $V(r)$ for the domain of $B_{(p_i)_i}$. For any choice of d_0 in $\mathscr{D}(\mathscr{V}_0)$, if we take

$$d = d_0 \cdot p_1 \cdot \cdots \cdot p_r, \tag{1.4}$$

we find that

$$\text{Sel}^2 E^d \subseteq B_{(p_i)_i}(V(r)).$$

In particular, we can find the distribution of 2-Selmer groups of twists of the form (1.4) by instead considering the distribution of the sizes of the subgroups

$$B^{-1}_{(p_i)_i}(\text{Sel}^2 E^d) \subseteq V(r).$$

The vector space $V(r)$ is a more acceptable ambient space for our calculations.

Given this setup, it is particularly nice to find the distribution of 2-Selmer ranks over families of the form

$$X = \left\{ d = d_0 p_1 \dots p_r \ : \ (p_i)_i \in \prod_{i \leq r} X_i, \right\} \tag{1.5}$$

where d_0 is fixed and $X_1, \dots, X_r$ are disjoint sets of rational primes not meeting $\mathscr{V}_0$. We will call such a family a *grid* in this dissertation. Given $v \in V(r)$ and given $d = d_0 p_1 \dots p_r$, we can determine if $\text{Sel}^2 E^d$ contains $B_{(p_i)_i}(v)$ from the Legendre symbols

$$\left(\frac{p_i}{p_j}\right) \quad \text{for all } i < j \leq r,$$

in addition to the values of p_i mod $8d_0 \cdot \prod_{p \in \mathscr{V}_0} p$ for all $i \leq r$. As a consequence, given $m \geq 0$, we can decompose sums of the form

$$\sum_{d \in X} (\#\text{Sel}^2 E^d)^m \tag{1.6}$$

into terms of the form

$$\sum_{(p_i)_i \in \prod_i X_i} \prod_{i \leq k} \chi_i(p_i) \cdot \prod_{i,j \leq r} \left(\frac{p_i}{p_j}\right)^{a_{ij}} \tag{1.7}$$

where the χ_i are Dirichlet characters of modulus dividing $8d_0 \prod_{p \in \mathscr{V}_0} p$, and the a_{ij} are all either 0 or 1. But from work of Jutila [21], given distinct $i, j \leq r$, and assuming X_i and X_j are large enough, we can often prove excellent cancellation results about sums of the form

$$\sum_{p_i \in X_i} \left| \sum_{p_j \in X_j} c_{p_j} \left(\frac{p_i}{p_j} \right) \right|.$$

We will give a more detailed statement of Jutila's result in Section 6. From Jutila's result, many of the terms of the form (1.7) turn out to be negligible. By finding decent estimates on the terms that remain, we can then derive estimates for the sequence of moments (1.6). Together with parity data, the moments can be used to find the distribution of 2-Selmer ranks in such a grid. We will prove results for natural density by covering the set of twists up to a given height outside a statistically negligible set with a collection of non-overlapping grids.

Now, to find the 2-Selmer statistics for quadratic twists of elliptic curves without full 2-torsion, we need to find a generalization for each step in this procedure. First, given a grid X and a tuple of primes $(p_i)_i$ in the grid, we need to find a suitable parameterization of the portion of $H^1(G_F, E[2])$ ramified just at $\{p_1, \ldots, p_r\}$ and $\mathscr{V}_0$. We do this in a non-canoncial way via Tate duality and an application of Shapiro's lemma. Second, we need to find an analogue for Legendre symbols; we need a function $\{\}$ on pairs of primes from $p_1, \ldots, p_r$ so we can determine $\text{Sel}^2 E^d$, with $d = d_0 p_1 \ldots p_r$ in terms of the data

$$\left\{ \frac{p_i}{p_j} \right\} \quad \text{for } i < j \leq r.$$

Third, we need to prove an analogue of Jutila's bilinear character estimates that applies for these more general symbols. We then need to apply this bilinear estimate estimate to split (1.6) into a negligible piece and a main-term piece. Finally, we need to patch these results for grids together to a result for all twists up to a given height. This approach works with

far more generality, applying to give Selmer statistics for twists of fairly general Galois modules.

Higher Selmer results are currenty most easily proved on grids. The calculations for higher Selmer groups come from generalizations of the fact that $E[2] \cong E^d[2]$ for any squarefree integer d. Specifically, given a sequence of squarefree integers $d_1, d_2, \ldots$, we find that the G_F-module $E^{d_1 d_2}[4]$ is isomorphic to a subquotient of

$$E^{d_1}[4] \oplus E^{d_2}[4] \oplus E[4],$$

that $E^{d_1 d_2 d_3}[8]$ is isomorphic to a subquotient of

$$E^{d_1 d2}[8] \oplus E^{d_1 d_3}[8] \oplus E^{d_2 d_3}[8] \oplus E^{d_1}[8] \oplus E^{d_2}[8] \oplus E^{d_3}[8] \oplus E[8],$$

etc. In a grids of twists, the first result gives relations between the 4-Selmer groups corresponding to squarefree integers

$$d_0 p_1 p_2 p_3 \ldots p_r, \qquad d_0 p_1' p_2 p_3 \ldots p_r,$$
$$d_0 p_1 p_2' p_3 \ldots p_r, \qquad d_0 p_1' p_2' p_3 \ldots p_r.$$

Grids contain many squares of this form, giving good aggregate control over 4-Selmer ranks. The 8-Selmer results rely on grids containing many cubes, etc. In all cases, it is most natural to find higher Selmer statistics over grids.

For $k \geq 1$, the Cassels-Tate pairing defined on the Shafarevich-Tate group of the twist E^d gives an alternating pairing

$$\text{CTP}_{E^d,k} : 2^{k-1}\text{Sel}^{2^k} E^d \otimes 2^{k-1}\text{Sel}^{2^k} E^d \to \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

with kernel equal to $2^k\text{Sel}^{2^{k+1}} E^d$. We note that, modulo the image of torsion, the domain of this pairing has dimension equal to the $r_{2^k}(E^d)$, and the kernel of this pairing has dimension $r_{2^{k+1}}(E^d)$. We claim that this pairing behaves like a random alternating matrix. To make

this meaningful, take a grid X as in (1.5). For d in this grid corresponding to the tuple $(p_i)_{i\leq r}$, and for $k \geq 1$, take

$$V_{k,(p_i)_i} = B^{-1}_{(p_i)_i}\left(2^{k-1}\text{Sel}^{2^k}E^d\right) \subseteq V(r).$$

We note that $\text{CTP}_{E^d,k}$ can be used to define an alternating pairing

$$C_{k,(p_i)_i} : V_{k,(p_i)_i} \otimes V_{k,(p_i)_i} \to \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

with kernel $V_{k+1,(p_i)_i}$.

With this in mind, choose $m \geq 1$, choose a filtration

$$V_m \subseteq V_{m-1} \subseteq \cdots \subseteq V_1 \subseteq V(r),$$

and choose a sequence $C_1, \ldots, C_{m-1}$ of alternating pairings

$$C_j : V_j \otimes V_j \to \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

so C_j has kernel V_{j+1} for all $j < m$. Take Y to be the subset of $(p_i)_i$ corresponding to integers d in X so

$$V_j = V_{j,(p_i)_i} \quad \text{for all } j \leq m \text{ and}$$

$$C_{j,(p_i)_i} = C_j \quad \text{for all } j < m.$$

Our claim, which recovers the Markov-chain behavior of Theorem 1.10, is that, as $(p_i)_i$ varies through the subset Y of the grid X, the pairing

$$C_{m,(p_i)_i} : V_m \otimes V_m \to \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

is equidistributed among all alternating pairings killing the image of torsion; and we accomplish this by abusing the relationships between these pairings found over hypercubes in the grid, as suggested above.

We now go through the sections of this dissertation. In Section 2, we will generalize the parameterization of cocycles in terms of $V(r)$ to apply for abelian varieties A/F where $A[2]$ is a nontrivial G_F module, and will also find a substitute for Legendre symbols in situations where $A[2]$ is not a trivial module. The notion of spin of a prime ideal, as introduced in [10], arises naturally from these considerations.

One guiding philosophy of this dissertation is that most results about the Selmer groups of abelian varieties should extend to results about Selmer groups for general Galois modules. In Section 3, we show that the theta group of a symmetric line bundle defined on A/F can often be constructed from the Galois module structure of $A[\ell^\infty]$. In Section 4, we similarly de-geometrize the Cassels-Tate pairing, giving a form of the pairing that applies to short exact sequences of finite Galois modules over number fields. The proofs in this section do not require substantially new ideas, but the central duality result could potentially be of fundamental importance in the theory of Galois cohomology. Our work on higher Selmer ranks depends on this new Cassels-Tate pairing, but we also use the formalism to exhibit pieces of class groups as Selmer groups, per Proposition 8.8.

We need a generalization of Jutila's bilinear character bounds that apply for the analogues of Legendre symbols we produce in Section 2. This analytic work is done in Section 6, a section we also consider to be of independent interest. Contrasting with similar bilinear bounds in e.g. [29], the form of the bound we produce will explicitly depend on the underlying choice of field extension K/F. This sensitivity is not important in our base case work, but will become relevant for our higher Selmer results, where we need to understand the splitting of primes in certain metabelian extensions.

With this legwork done, we turn to defining twist families and Selmer groups in Section 8. In this section, we will find that equivariant isogenies can cause the Selmer group distributions to misbehave. Following [24], we explain this behavior in terms of Tamagawa ratios, with our main proposition being Proposition 8.10. In Section 9, we derive the necessary conditions for Selmer groups to avoid being affected by Tamagawa ratios. With

the terminology of this section in hand, we finally give our main base-case results in Section 9.1.

In Sections 10 and 11, we give the necessary linear algebra for computing the moments of base-case Selmer groups in certain grids. We do the necessary gridding in Section 12 and Section 13 before finishing the proofs of our main base-case theorems in Section 14.

1.1.1. *Some historical comments.* Gerth first observed that, in quadratic fields indexed by a certain kind of grid, the distribution of 4-class ranks could be computed with relative ease via linear algebra and an application of the bilinear character sum bounds of Jutila [12, 21]. The analogous work for 2-Selmer ranks of quadratic twists of elliptic curves with full rational 2-torsion was done by Swinnerton-Dyer in [50]. 2-Selmer statistics over grids of quadratic twists have also been found in the case that $\mathbb{Q}(E[2])/\mathbb{Q}$ is an S_3 extension [25].

For many years, work on 2-Selmer distributions over grid families and work on 2-Selmer results over more natural families proceeded independently. In natural families, the only known viable approach was to adapt an argument of Heath-Brown that gives the 2-Selmer rank distribution in the family of quadratic twists of the congruent number curve [18]. While still relying on certain bilinear character sum estimates, this work seems otherwise unconnected to results over grids. The prime decomposition of the involved squarefree integers plays little role, for example. Heath-Brown's approach has since been used to find distributions of 4-class ranks in quadratic fields [9].

The grid-based results and natural density results started to comingle in a paper of Kane [22]. In this work, Kane found the distribution of 2-Selmer ranks in the family of quadratic twists of any curve in the full rational 2-torsion case of Assumption 1.2. His approach uses a subtle induction argument, and grids still do not appear in a substantial way; but his work builds on the grid-based foundation set by Swinnerton-Dyer in [50], and he relies on the prime decomposition of the involved squarefree integers.

With the strategy outlined above, where we first decompose most of the twists up to a certain height into non-overlapping grids, and then prove our main distribution results on these grids, we have more fully merged finding 2-Selmer rank distributions in grid families and finding 2- Selmer rank distributions in natural families. In addition to being a better setup for higher Selmer rank results, this simplifies the overall strategy of finding 2-Selmer rank distributions.

Part 1. The Cassels-Tate pairing, Theta Groups, and 1-Cocycle Parameterization

2. Legendre symbols and spin

Notation 2.1. Given a number field F and a finite module M with a continuous G_F-action, we define

$$Ш_1(F, M) = \ker\left(H^1(G_F,\, M) \,\to \prod_{v \text{ of } F} H^1(G_v,\, M)\right).$$

Here, G_F denotes the absolute Galois group of F, and G_v denotes the absolute Galois group of F_v, the completion of F at v.

Given a finite set of places $\mathscr{V}$ of F and its subfields, we also define

$$\mathscr{S}_{M/F}(\mathscr{V}) = \ker\left(H^1(G_F, M) \to \prod_{\substack{v \text{ of } F \\ v \nmid \mathscr{V}}} H^1(I_v, M)\right) \Big/ Ш_1(F, M).$$

The base-case Selmer groups we are interested in will lie in spaces of the form $\mathscr{S}_{M/F}(\mathscr{V})$, with $\mathscr{V}$ changing with the twist and with M and F remaining constant. The first goal of this section is to give a way to parameterize $\mathscr{S}_{M/F}(\mathscr{V})$ in a way that behaves well as the set of places $\mathscr{V}$ is adjusted.

With that in mind, take $\mathfrak{p}$ to be a prime of F, and take $\mathscr{V}$ to be a set of places of F and its subfields so $\mathfrak{p}$ divides no prime of $\mathscr{V}$. Take $\overline{\mathfrak{p}}$ to be a prime of $\overline{F}$ over $\mathfrak{p}$. We then have an exact sequence

$$0 \to \mathscr{S}_{M/F}(\mathscr{V}_0) \to \mathscr{S}_{M/F}\big(\mathscr{V}_0 \cup \{\mathfrak{p}\}\big) \xrightarrow{\mathrm{fb}^*_{M,F,\overline{\mathfrak{p}}}} M(-1)^{G_{F,\overline{\mathfrak{p}}}}, \tag{2.1}$$

where $\mathrm{fb}^*_{M,F,\overline{\mathfrak{p}}}$ is a map defined in Section 5.2 that measures the ramification of a given cocycle class at $\mathfrak{p}$, where $M(-1)$ denotes the (-1)-Tate twist, and where the superscript $G_{F,\overline{\mathfrak{p}}}$ indicates that we are considering the set of invariants under the action of the absolute Galois group of the completion of F at $\overline{\mathfrak{p}}$.

To parameterize $\mathscr{S}_{M/F}(\mathscr{V})$, we will ultimately need a section to the final map of (2.1). This will rely on this final map being surjective, motivating the following definition:

Notation 2.2. We fix the following:

(1) An integer $e_0 \geq 2$,

(2) A Galois extension of number fields K/F, with K containing μ_{e_0}, and

(3) A finite set of places $\mathscr{V}_0$ of F.

We assume that the places $\mathscr{V}_0$ contain all archimedean places, all places where K/F is ramified, and all places dividing e_0. Furthermore, given any finite $\mathrm{Gal}(K/F)$-module M, we assume the sequence (2.1) is exact on the right for $\mathscr{V} = \mathscr{V}_0$ and any choice of $\mathfrak{p}$ outside $\mathscr{V}_0$. If these conditions are met, we say $\mathscr{V}_0$ *unpacks* the tuple $(K/F, e_0)$

Definition 2.3. For any set $\mathscr{V}$ of places of F, write $K(\mathscr{V})$ for the maximal abelian extension of K of exponent dividing e_0 that is ramified only over places in $\mathscr{V}$.

Giving primes $\overline{\mathfrak{p}}, \overline{\mathfrak{p}}_0$ of $\overline{F}$ not over $\mathscr{V}_0$, we say $\overline{\mathfrak{p}}$ and $\overline{\mathfrak{p}}_0$ have the same class and write $\overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0$ if

$$\mathrm{Frob}_F\overline{\mathfrak{p}} \equiv \mathrm{Frob}_F\overline{\mathfrak{p}}_0 \quad \text{in } \mathrm{Gal}(K(\mathscr{V}_0)/F).$$

Proposition 2.4. *Given e_0 and K/F as in Notation 2.2, we can find a finite set of places $\mathscr{V}_0$ unpacking $(K/F, e_0)$.*

We postpone the proof of this until the end of this section.

The map $\mathrm{fb}^*_{M,F,\overline{\mathfrak{p}}}$ is fairly natural, but giving a section for this map requires some ad-hoc choices. After some experimentation, we have opted for a definition that built from Shapiro's lemma as given in Section 5.1, but even this relies on some extra choices that we

make now. We make heavy use of the superscript nc to emphasize the noncanonical nature of these definitions.

Notation 2.5. Take $(K/F, e_0, \mathscr{V}_0)$ as in Notation 2.2, and take μ_{e_0} to be the group of e_0-roots of unity in K. For every intermediate field L of K/F such that K/L is cyclic, we choose a set-theoretic section s_L^{nc} of the projection

$$\bigoplus_{\substack{v \text{ of } L \\ v|\mathscr{V}_0}} H^1(G_v, \mu_{e_0}) \longrightarrow \bigoplus_{\substack{v \text{ of } L \\ v|\mathscr{V}_0}} H^1(G_v, \mu_{e_0}) \Big/ \operatorname{im}\left(\mathscr{S}_{\mu_{e_0}/L}(\mathscr{V}_0)\right).$$

From Shapiro's lemma, we have an isomorphism

$$\mathscr{S}_{N/L}(\mathscr{V}) \xrightarrow{\text{sh}} \mathscr{S}_{\text{Ind}_{G_F}^{G_L} N/F}(\mathscr{V}). \tag{2.2}$$

for any set of places $\mathscr{V}$ of F and any field L that is intermediate to K/F. We will give this isomorphism explicitly in Section 5.1. As a consequence, if $\mathscr{V}_0$ unpacks $(K/F, e_0)$, it unpacks $(K/L, e_0)$ for any intermediate field L of the extension K/F.

Definition 2.6. Given $(K/F, e_0, \mathscr{V}_0)$ as in Notation 2.2, given sections $(s_L^{\text{nc}})_L$ as in Notation 2.5, and given a finite $\text{Gal}(K/F)$ module M of exponent dividing e_0 and a prime $\overline{\mathfrak{p}}$ of $\overline{F}$ not over $\mathscr{V}_0$, we define a map

$$\mathfrak{B}^{\text{nc}}_{M,F,\overline{\mathfrak{p}}} : M(-1)^{G_{F,\overline{\mathfrak{p}}}} \longrightarrow \mathscr{S}_{M/F}(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}} \cap F\})$$

as follows:

First, take L minimal so K/L is inert at $\overline{\mathfrak{p}} \cap L$, and define

$$\mathfrak{B}^{\text{nc}}(\overline{\mathfrak{p}}) \in \mathscr{S}_{\mu_{e_0}/L}(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}} \cap L\}),$$

to be the unique element satisfying $\text{fb}^*_{\mu_{e_0},L,\overline{\mathfrak{p}}}(\mathfrak{B}^{\text{nc}}(\overline{\mathfrak{p}})) = 1/e_0$ whose restriction to

$$\bigoplus_{\substack{v \text{ of } L \\ v|\mathscr{V}_0}} H^1(G_v, \mu_{e_0})$$

is in the image of s_L^{nc}.

Next, choosing $m \in M(-1)^{G_{F,\overline{\mathfrak{p}}}}$, there is a unique G_F-homomorphism $\rho(m)$ from

$$\mathrm{Ind}_{G_F}^{G_L}\mu_{e_0} \cong \mathbb{Z}[G_F] \otimes_{\mathbb{Z}[G_L]} \mu_{e_0}$$

to M that takes $[1] \otimes \zeta$ to $m \otimes \zeta$ for all $\zeta \in \mu_{e_0}$. We then take $\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}}(m)$ to be the image of $\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})$ under the composition

$$\mathscr{S}_{\mu_{e_0}/L}(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}} \cap L\}) \xrightarrow{\mathrm{sh}} \mathscr{S}_{\mathrm{Ind}_{G_F}^{G_L}\mu_{e_0}/F}(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}} \cap F\}) \xrightarrow{\rho(m)_*} \mathscr{S}_{M/F}(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}} \cap F\}).$$

Remark 2.7. In the above situation, we can use (5.6) and Proposition 5.3 to verify that

$$M(-1)^{G_{F,\overline{\mathfrak{p}}}} \xrightarrow{\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}}} \mathscr{S}_{M/F}(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}} \cap F\}) \xrightarrow{\mathrm{fb}^*_{M,F,\overline{\mathfrak{p}}}} M(-1)^{G_{F,\overline{\mathfrak{p}}}}$$

is the identity map, so we have succeeded at finding a section of fb^*. There are three other properties that recommend this particular section.

(1) The map $\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}}$ is linear in $M(-1)^{G_{F,\overline{\mathfrak{p}}}}$.

(2) Given $\overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0$ and any

$$m \in M(-1)^{G_{F,\overline{\mathfrak{p}}}} = M(-1)^{G_{F,\overline{\mathfrak{p}}_0}},$$

the difference $\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}}(m) - \mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}_0}(m)$ is trivial at all places over $\mathscr{V}_0$.

(3) With m as above, take N to be the minimal G_F-submodule of M containing $m \otimes \zeta$ for all ζ in μ_{e_0}. Then $\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}}(m)$ is in the image of the map

$$\mathscr{S}_{N/F}(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}} \cap F\}) \longrightarrow \mathscr{S}_{M/F}(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}} \cap F\}).$$

Remark 2.8. We note that

$$Ш_1(F, \mu_{e_0})$$

is equal either to 0 or $\mathbb{Z}/2\mathbb{Z}$, with the latter case possible only if e_0 is divisible by 8. This is a consequence of the Grunwald-Wang theorem, which describes precisely the scenario when

this group equals $\mathbb{Z}/2\mathbb{Z}$. This counterintuitive result is what forced us to define $\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})$ as an element of $\mathscr{S}_{\mu_{e_0}/L}$ rather than as an element of $H^1(G_L, \mu_{e_0})$.

Definition 2.9. With the setup of Notation 2.2, take M and N to be finite $\mathrm{Gal}(K/F)$ modules of exponent dividing e_0. Take $\overline{\mathfrak{p}}, \overline{\mathfrak{q}}$ to be primes of $\overline{F}$ not over $\mathscr{V}_0$. Per Section 5.2, we have an isomorphism

$$\mathrm{inv}_{M\otimes N, F, \overline{\mathfrak{p}}} : H^2(G_F, M\otimes N) \xrightarrow{\sim} M \otimes N(-1)_{G_{F,\overline{\mathfrak{p}}}},$$

where $M \otimes N(-1)_{G_{F,\overline{\mathfrak{p}}}}$ denotes the set of $G_{F,\overline{\mathfrak{p}}}$ coinvariants of $M \otimes N(-1)$.

We then define

$$\mathfrak{L}^{\mathrm{nc}}_{M\otimes N/F}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}) \,:\, M(-1)^{G_{F,\overline{\mathfrak{p}}}} \otimes N(-1)^{G_{F,\overline{\mathfrak{q}}}} \longrightarrow M \otimes N(-1)_{G_{F,\overline{\mathfrak{p}}}}$$

by

$$\mathfrak{L}^{\mathrm{nc}}_{M\otimes N/F}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}})\big(m, n\big) \,=\, \mathrm{inv}_{M\otimes N, F, \overline{\mathfrak{p}}} \left(\overline{\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}}(m)} \,\cup\, \overline{\mathfrak{B}^{\mathrm{nc}}_{N,F,\overline{\mathfrak{q}}}(n)} \right). \tag{2.3}$$

Here, $\overline{\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}}(m)}$ denotes an element of $H^1(G_F, M)$ projecting to $\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}}(m)$, with the same notation on the N side. The resulting pairing does not depend on the choice of this element.

Further, suppose that $\overline{\mathfrak{p}}, \overline{\mathfrak{q}}$ are primes of $\overline{F}$ not over $\mathscr{V}_0$. Take L to be the minimal intermediate field of K/F so K/L is inert at $\overline{\mathfrak{p}} \cap L$, and take E to be the minimal intermediate field of K/F so K/E is inert at $\overline{\mathfrak{q}} \cap E$. Then, for $\tau \in G_F$, we define an element

$$a^{\mathrm{nc}}_{\tau}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}) \in (\mu_{e_0})_{G_{L+\tau E}}$$

by

$$a^{\mathrm{nc}}_{\tau}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}) = \mathrm{inv}_{\mu_{e_0}\otimes\mu_{e_0}, (L+\tau E), \overline{\mathfrak{p}}} \left(\mathrm{res}^{G_L}_{G_{L+\tau E}} \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})} \,\cup\, \tau_* \mathrm{res}^{G_E}_{G_{E+\tau^{-1}L}} \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})} \right),$$

where again $\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})}$ denotes an element of $H^1(G_L, \mu_{e_0})$ projecting to $\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})$.

Remark 2.10. Following Remark 2.8, we can think about the element $\mathfrak{B}^{\text{nc}}(\overline{\mathfrak{q}})$ as being an element of $E^{\times}/Ш \cdot (E^{\times})^{e_0}$, where Ш is either $\{1\}$ or $\{1, \alpha\}$ for some element with

$$\alpha^2 \in (E^{\times})^{e_0}.$$

Using this, the symbol $a_{\tau}^{\text{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}})$ can be thought of as a norm-residue symbol, or as a general form of a Legendre symbol. The precise behavior or these symbols depends on the choice of s^{nc}, but if $\overline{\mathfrak{q}} \sim \overline{\mathfrak{q}}_0$ in the sense of Notation 2.2 for some other prime $\overline{\mathfrak{q}}_0$, we can concretely say that the fraction

$$\frac{\mathfrak{B}^{\text{nc}}(\overline{\mathfrak{q}})}{\mathfrak{B}^{\text{nc}}(\overline{\mathfrak{q}}_0)} \in E^{\times}/Ш \cdot (E^{\times})^{e_0}$$

is the unique element that is both locally an e_0 power at all places of E over $\mathscr{V}_0$ and is also a generator for an ideal of the form $I^{e_0} \cdot \big(\overline{\mathfrak{q}}\overline{\mathfrak{q}}_0^{-1} \cap L\big)$.

In this paper, the $a_{\tau}^{\text{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}})$ will serve as generalizations of Legendre symbols, with the special case $a_{\tau}^{\text{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}})$ instead a generalization of the notion of the spin of a prime ideal, a concept first considered in [10]. These are the atomic objects that we will decompose Selmer conditions into, with the maps $\mathfrak{L}^{\text{nc}}$ appearing naturally as part of this decomposition. To aid such a decomposition, we have the following proposition.

Proposition 2.11. *Use the setup of Notation 2.2. Given primes $\overline{\mathfrak{p}}, \overline{\mathfrak{q}}$ of $\overline{F}$ not over $\mathscr{V}_0$, take L and E as in Definition 2.9. Take M and N to be finite* $\text{Gal}(K/F)$ *modules of exponent dividing e_0, and choose any*

$$m \in M(-1)^{G_{F,\overline{\mathfrak{p}}}} \quad \textit{and} \quad n \in N(-1)^{G_{F,\overline{\mathfrak{q}}}}.$$

Then, if $\overline{\mathfrak{p}} \cap F$ and $\overline{\mathfrak{q}} \cap F$ are distinct, we have

$$\mathfrak{L}^{\text{nc}}_{M\otimes N/F}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}})\big(m, n\big) = \sum_{\tau \in B} m \otimes \tau n \otimes a_{\tau}^{\text{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}),$$

where B is any set of representatives in G_F of the double coset

$$G_L \backslash G_F / G_E.$$

In addition, take B' to be B with the representative of the identity removed. Then we have

$$\begin{aligned}\mathfrak{L}^{\mathrm{nc}}_{M\otimes N/F}(\overline{\mathfrak{p}},\overline{\mathfrak{p}})\big(m,n\big) = &\sum_{\tau\in B} m\otimes \tau n\otimes a^{\mathrm{nc}}_{\tau}(\overline{\mathfrak{p}},\overline{\mathfrak{p}})\\ &-\sum_{\tau\in B'} \tau m\otimes n\otimes a^{\mathrm{nc}}_{\tau}(\overline{\mathfrak{p}},\overline{\mathfrak{p}}).\end{aligned}$$

Proof. We start without using the assumption that $\overline{\mathfrak{p}}\cap F$ and $\overline{\mathfrak{q}}\cap F$ are distinct. Write

$$M_0 = \mathrm{Ind}_{G_F}^{G_L}\mu_{e_0} \quad \text{and} \quad N_0 = \mathrm{Ind}_{G_F}^{G_E}\mu_{e_0}.$$

We calculate

$$\begin{aligned}&\mathfrak{L}^{\mathrm{nc}}_{M\otimes N/F}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})\big(m,n\big)\\ &\quad= \mathrm{inv}_{M\otimes N,F,\overline{\mathfrak{p}}}\left(\rho(m)_*\mathrm{cor}_{G_F}^{G_L}\left([1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})}\right)\cup\rho(n)_*\mathrm{cor}_{G_F}^{G_E}\left([1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})}\right)\right)\\ &\quad= (\rho(m)_*\otimes\rho(n)_*)\,\mathrm{inv}_{M_0\otimes N_0,F,\overline{\mathfrak{p}}}\left(\mathrm{cor}_{G_F}^{G_L}\left([1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})}\right)\cup\mathrm{cor}_{G_F}^{G_E}\left([1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})}\right)\right)\end{aligned}$$

from (5.18). It then suffices to calculate

$$\mathrm{inv}_{M_0\otimes N_0,F,\overline{\mathfrak{p}}}\left(\mathrm{cor}_{G_F}^{G_L}\left([1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})}\right)\cup\mathrm{cor}_{G_F}^{G_E}\left([1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})}\right)\right).$$

From (5.11) followed by Proposition 5.3 and the double coset formula, this equals

$$\begin{aligned}&\mathrm{inv}_{M_0\otimes N_0,F,\overline{\mathfrak{p}}}\circ\mathrm{cor}_{G_F}^{G_E}\left(\mathrm{res}_{G_E}^{G_F}\circ\mathrm{cor}_{G_F}^{G_L}\left([1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})}\right)\cup[1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})}\right)\\ &\quad=\sum_{\tau\in B}\mathrm{inv}_{M_0\otimes N_0,F,\overline{\mathfrak{p}}}\circ\mathrm{cor}_{G_F}^{G_E}\left(\mathrm{cor}_{G_E}^{G_{E+\tau^{-1}L}}\circ\tau_*^{-1}(\psi_\tau)\cup[1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})}\right)\\ &\quad=\sum_{\tau_1\in B}\sum_{\tau\in B}\tau_1\,\mathrm{inv}_{M_0\otimes N_0,E,\tau_1^{-1}\overline{\mathfrak{p}}}\left(\mathrm{cor}_{G_E}^{G_{E+\tau^{-1}L}}\circ\tau_*^{-1}(\psi_\tau)\cup[1]\otimes\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})}\right),\end{aligned}\tag{2.4}$$

where we have taken

$$\psi_\tau = [1] \otimes \mathrm{res}^{G_L}_{G_{\tau E + L}} \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})}.$$

This element is only ramified at $\overline{\mathfrak{p}} \cap (\tau E + L)$ and places over $\mathscr{V}_0$. If we now assume that $\overline{\mathfrak{p}} \cap F$ and $\overline{\mathfrak{q}} \cap F$ are distinct, we find that (2.4) equals

$$\begin{aligned}
&\sum_{\tau \in B} \tau \, \mathrm{inv}_{M_0 \otimes N_0, E, \tau^{-1}\overline{\mathfrak{p}}} \left(\mathrm{cor}^{G_{E+\tau^{-1}L}}_{G_E} \circ \tau_*^{-1}(\psi_\tau) \cup [1] \otimes \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})} \right) \\
&\quad = \sum_{\tau \in B} \tau \, \mathrm{inv}_{M_0 \otimes N_0, E+\tau^{-1}L, \tau^{-1}\overline{\mathfrak{p}}} \left(\tau_*^{-1}(\psi_\tau) \cup [1] \otimes \mathrm{res}^{G_E}_{G_{E+\tau^{-1}L}} \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})} \right) \\
&\quad = \sum_{\tau \in B} \mathrm{inv}_{M_0 \otimes N_0, \tau E + L, \overline{\mathfrak{p}}} \left(\psi_\tau \cup [\tau] \otimes \tau_* \mathrm{res}^{G_E}_{G_{E+\tau^{-1}L}} \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})} \right) \\
&\quad = \sum_{\tau \in B} [1] \otimes [\tau] \otimes a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}).
\end{aligned}$$

This gives the first part of the proposition.

Now suppose that $\overline{\mathfrak{q}} = \overline{\mathfrak{p}}$. In this case, (2.4) splits into two pieces: a sum over (τ, τ_1) with $\tau = \tau_1$; and a sum over $(\tau, 1)$, excepting the already-counted representative of $(1, 1)$. The first piece can be evaluated as before. The second piece takes the form

$$\begin{aligned}
&\sum_{\tau \in B'} \mathrm{inv}_{M_0 \otimes N_0, L, \overline{\mathfrak{p}}} \left(\mathrm{cor}^{G_{L+\tau^{-1}L}}_{G_L} \circ \tau_*^{-1}(\psi_\tau) \cup [1] \otimes \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})} \right) \\
&\quad = \sum_{\tau \in B'} \mathrm{inv}_{M_0 \otimes N_0, L+\tau^{-1}L, \overline{\mathfrak{p}}} \left(\tau_*^{-1}(\psi_\tau) \cup [1] \otimes \mathrm{res}^{G_L}_{G_{L+\tau^{-1}L}} \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})} \right) \\
&\quad = - \sum_{\tau \in B'} t \, \mathrm{inv}_{N_0 \otimes M_0, L+\tau^{-1}L, \overline{\mathfrak{p}}} \left([1] \otimes \mathrm{res}^{G_L}_{G_{L+\tau^{-1}L}} \overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})} \cup \tau_*^{-1}(\psi_\tau) \right) \\
&\quad = - \sum_{\tau \in B'} [\tau^{-1}] \otimes [1] \otimes a^{\mathrm{nc}}_{\tau^{-1}}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}).
\end{aligned}$$

Here, we have made use of (5.10), with t taken as in that equation. We then have the proposition.

□

We have described the norm residue symbols $a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})$ as the atoms from which the Selmer conditions we are interested in are constructed. Not all these atoms are needed, with the next proposition giving all the redundancies we need to consider.

Proposition 2.12. *In the situation of Notation 2.2, choose primes $\overline{\mathfrak{p}},\overline{\mathfrak{q}},\overline{\mathfrak{p}}_0,\overline{\mathfrak{q}}_0$ of $\overline{F}$ not over $\mathscr{V}_0$ so that $\overline{\mathfrak{p}}\sim\overline{\mathfrak{p}}_0$ and $\overline{\mathfrak{q}}\sim\overline{\mathfrak{q}}_0$. Write L for the minimal extension of F so K/L is inert at $\overline{\mathfrak{p}}\cap L$, and write E for the analogous extension for $\overline{\mathfrak{q}}$. Take $\tau\in G_F$. We then have the following:*

(1) For $\sigma\in G_L$, we have $a_{\sigma\tau}^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})=a_{\sigma\tau}^{\mathrm{nc}}(\sigma\overline{\mathfrak{p}},\overline{\mathfrak{q}})=\sigma a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})$.

(2) For $\sigma\in G_E$, we have $a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}},\sigma\overline{\mathfrak{q}})=a_{\tau\sigma}^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})=a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})$.

(3) Writing a^{nc} for a_1^{nc}, we have

$$a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})-a^{\mathrm{nc}}(\overline{\mathfrak{p}},\tau\overline{\mathfrak{q}})\;=\;a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}}_0,\overline{\mathfrak{q}}_0)-a^{\mathrm{nc}}(\overline{\mathfrak{p}}_0,\tau\overline{\mathfrak{q}}_0).$$

(4) We have

$$\tau a^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})-a^{\mathrm{nc}}(\tau\overline{\mathfrak{p}},\tau\overline{\mathfrak{q}})\;=\;\tau a^{\mathrm{nc}}(\overline{\mathfrak{p}}_0,\overline{\mathfrak{q}}_0)-a^{\mathrm{nc}}(\tau\overline{\mathfrak{p}}_0,\tau\overline{\mathfrak{q}}_0).$$

(5) If

$$\overline{\mathfrak{p}}\cap(L+E)\neq\overline{\mathfrak{q}}\cap(L+E)\quad\textit{and}\quad\overline{\mathfrak{p}}_0\cap(L+E)\neq\overline{\mathfrak{q}}_0\cap(L+E),$$

we have

$$a^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})-a^{\mathrm{nc}}(\overline{\mathfrak{q}},\overline{\mathfrak{p}})=a^{\mathrm{nc}}(\overline{\mathfrak{p}}_0,\overline{\mathfrak{q}}_0)-a^{\mathrm{nc}}(\overline{\mathfrak{q}}_0,\overline{\mathfrak{p}}_0).$$

(6) If e_0 is odd, we have

$$a^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{p}})=1.$$

Otherwise, take ζ to be the unique element of order two in $(\mu_{e_0})_{G_L}$. Then

$$a^{\mathrm{nc}}(\overline{\mathfrak{p}},\overline{\mathfrak{p}})=\begin{cases}1 & \textit{if } x^{e_0}+1=0 \textit{ has a solution } x\in F_{\overline{\mathfrak{p}}\cap F}\\ \zeta & \textit{otherwise.}\end{cases}$$

If $\overline{\mathfrak{p}}_0 \cap L \neq \overline{\mathfrak{p}} \cap L$, we also have

$$a^{\mathrm{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}_0) - a^{\mathrm{nc}}(\overline{\mathfrak{p}}_0, \overline{\mathfrak{p}}) = a^{\mathrm{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}).$$

(7) Suppose τ represents the same class as τ^{-1} in

$$G_L \backslash G_F / G_L.$$

Then

$$a^{\mathrm{nc}}(\overline{\mathfrak{p}}, \tau\overline{\mathfrak{p}}) - a^{\mathrm{nc}}(\overline{\mathfrak{p}}_0, \tau\overline{\mathfrak{p}}_0) \in \left((\mu_{e_0})_{G_{L+\tau L}}\right)^2.$$

Proof. For σ in G_E, we have

$$\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}}) = \mathfrak{B}^{\mathrm{nc}}(\sigma\overline{\mathfrak{q}}) = \sigma_* \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}}).$$

Part 2 follows. For σ in G_L, (5.12) and (5.17) give

$$\sigma a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}) = a_{\sigma\tau}^{\mathrm{nc}}(\sigma\overline{\mathfrak{p}}, \overline{\mathfrak{q}}).$$

Applying this and part 2 for σ in G_K gives

$$a_\tau^{\mathrm{nc}}(\sigma\overline{\mathfrak{p}}, \overline{\mathfrak{q}}) = a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}).$$

Since $\sigma\overline{\mathfrak{p}} = \overline{\mathfrak{p}}$ for σ in $G_{F,\overline{\mathfrak{p}}}$, we then have this equality for σ in G_L, and part 1 follows.

Part 3 is a consequence of

$$\mathrm{res}^{G_{\tau E}}_{G_{L+\tau E}} \mathfrak{B}^{\mathrm{nc}}(\tau\overline{\mathfrak{q}}) - \tau_* \mathrm{res}^{G_E}_{G_{E+\tau^{-1}L}} \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{q}})$$

only being ramified over $\mathscr{V}_0$, which can be proven from (5.17). This result and (5.12) give part 4 as well.

Part 5 follows from skew commutativity of cup product and Hilbert reciprocity, in the form of (5.22) for the field $L + E$. For part 6, if we take χ to be the image of -1 under the

natural boundary map

$$L^\times/(L^\times)^{e_0} \longrightarrow H^1(G_L, \mu_{e_0}),$$

the symbol properties of a^{nc} give

$$a^{\mathrm{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}) = \mathrm{inv}_{\mu_{e_0}\otimes\mu_{e_0}, L, \overline{\mathfrak{p}}} \left(\overline{\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})} \cup \chi \right).$$

This has order dividing 2, giving the result for odd e_0. For even e_0, this symbol is either nontrivial, in which case it must equal ζ, or is trivial. As a norm residue symbol, it is the former only if -1 is an e_0 power at $\overline{\mathfrak{p}} \cap F$. This gives the first statement of the part, and the second statement follows from Hilbert reciprocity.

This just leaves part 7, which is substantially harder. The statement is a generalization of a previous result on involution spin [10, Section 12]. In that paper, it was proved using the theory of ray class fields. We will prove it instead as a consequence of our theory of theta groups; see Proposition 3.6. □

The obvious next question is whether this last proposition has identified all the redundancies between our Legendre symbol analogues $a^{\mathrm{nc}}_\tau(\overline{\mathfrak{p}}, \overline{\mathfrak{q}})$. For the symbols $a^{\mathrm{nc}}_\tau(\overline{\mathfrak{p}}, \overline{\mathfrak{p}})$, this is a difficult unresolved question about the spin of prime ideals. When $\overline{\mathfrak{p}}$ and $\overline{\mathfrak{q}}$ are different, the situation is much more straightforward.

Proposition 2.13. *In the situation of Notation 2.2, choose primes $\overline{\mathfrak{q}}, \overline{\mathfrak{p}}_0$ of $\overline{F}$ not over $\mathscr{V}_0$. Take L and E to be the minimal fields over F such that K/L is inert at $\overline{\mathfrak{p}}_0 \cap L$ and K/E is inert at $\overline{\mathfrak{q}} \cap E$. Write $\mathfrak{q}$ for $\overline{\mathfrak{q}} \cap F$. We assume $\overline{\mathfrak{p}}_0$ does not divide $\mathfrak{q}$.*

Take B to be a set of representatives in G_F for

$$G_L \backslash G_F / G_E$$

and take π to be the natural projection from $\mathrm{Gal}(K(\mathscr{V}_0 \cup \{\mathfrak{q}\})/F)$ *to* $\mathrm{Gal}(K(\mathscr{V}_0)/F)$. *Given σ_1, σ_2 in $\pi^{-1}(\mathrm{Frob}_F \overline{\mathfrak{p}}_0)$, we say the elements are equivalent if one equals the other*

conjugated by an element of $G_{K(\mathscr{V}_0)}$, and we write $\pi^{-1}(\mathrm{Frob}_F\overline{\mathfrak{p}}_0)_\sim$ for the set of equivalence classes under this relation.

There is then a unique isomorphism

$$\pi^{-1}(\mathrm{Frob}_F\overline{\mathfrak{p}}_0)_\sim \xrightarrow{\sim} \bigoplus_{\tau\in B}(\mu_{e_0})_{G_{L+\tau E}}$$

so that, for all primes $\overline{\mathfrak{p}}$ not over $\mathscr{V}_0\cup\{\mathfrak{q}\}$ satisfying $\overline{\mathfrak{p}}\sim\overline{\mathfrak{p}}_0$, we have

$$\mathrm{Frob}_F\overline{\mathfrak{p}} \longmapsto \big(a^{\mathrm{nc}}(\overline{\mathfrak{p}},\tau\overline{\mathfrak{q}}) \,:\, \tau\in B\big). \tag{2.5}$$

Proof. Take C to be the trivial G_F module $\mathbb{Z}/e_0\mathbb{Z}$. For a set of places of $\mathscr{V}$ of L or any subfield of L, take $L(\mathscr{V})$ to be the maximal abelian extension of L of exponent dividing e_0 ramified only over places of $\mathscr{V}$. We have a set of isomorphisms

$$\begin{aligned}\mathrm{Gal}\left(K(\mathscr{V}_0)L\Big(\mathscr{V}_0\cup\{\mathfrak{q}\}\Big)\Big/K(\mathscr{V}_0)\right)&\\ \cong \mathrm{Gal}\left(L\Big(\mathscr{V}_0\cup\{\mathfrak{q}\}\Big)\Big/L(\mathscr{V}_0)\right)&\\ \cong \mathrm{Hom}\left(\frac{\mathscr{S}_{C/L}\big(\mathscr{V}_0\cup\{\tau\overline{\mathfrak{q}}\cap L \,:\, \tau\in B\}\big)}{\mathscr{S}_{C/L}(\mathscr{V}_0)},\ \mathbb{Q}/\mathbb{Z}\right)&\\ \cong \bigoplus_{\tau\in B}(\mu_{e_0})_{G_{L+\tau E}}.&\end{aligned} \tag{2.6}$$

This set of isomorphisms takes $\mathrm{Frob}_F\overline{\mathfrak{p}}(\mathrm{Frob}_F\overline{\mathfrak{p}}_0)^{-1}$ to

$$\big(a^{\mathrm{nc}}(\overline{\mathfrak{p}},\tau\overline{\mathfrak{q}}) - a^{\mathrm{nc}}(\overline{\mathfrak{p}}_0,\tau\overline{\mathfrak{q}}) \,:\, \tau\in B\big).$$

To finish the proof, it then suffices to show that the map

$$\pi^{-1}(\mathrm{Frob}_F\overline{\mathfrak{p}}_0)_\sim \longrightarrow \mathrm{Gal}\left(K(\mathscr{V}_0)L\Big(\mathscr{V}_0\cup\{\mathfrak{q}\}\Big)\Big/K(\mathscr{V}_0)\right)$$

given by multiplication by $(\mathrm{Frob}_F\overline{\mathfrak{p}}_0)^{-1}$ is an isomorphism. This starts by noting that this map is well-defined, which follows from the definition of our equivalence relation, and surjective. We just need to show injectivity.

Call elements σ_1, σ_2 of $\mathrm{Gal}\left(K(\mathscr{V}_0 \cup \{\mathfrak{q}\})/K(\mathscr{V}_0)\right)$ equivalent if

$$\tau\sigma_1\tau^{-1} \cdot \mathrm{Frob}_F\overline{\mathfrak{p}}_0 = \sigma_2 \cdot \mathrm{Frob}_F\overline{\mathfrak{p}}_0 \quad \text{in} \quad K(\mathscr{V}_0 \cup \{\mathfrak{q}\})$$

for some τ in $G_{K(\mathscr{V}_0)}$. Equivalently, σ_1 and σ_2 are equivalent if they differ by an element of

$$\left[G_L, G_{K(\mathscr{V}_0)}\right].$$

Using a subscript $\sim$ to denote the corresponding set of equivalence classes, we have

$$\pi^{-1}(\mathrm{Frob}_F\overline{\mathfrak{p}}_0)_\sim \cong \mathrm{Gal}\left(K(\mathscr{V}_0 \cup \{\mathfrak{q}\})/K(\mathscr{V}_0)\right)_\sim.$$

We have an isomorphism of G_F modules

$$\mathrm{Gal}\left(K(\mathscr{V}_0 \cup \{\mathfrak{q}\})/K(\mathscr{V}_0)\right) \cong \mathrm{Hom}\left(\frac{\mathscr{S}_{C/K}(\mathscr{V}_0 \cup \{\mathfrak{q}\})}{\mathscr{S}_{C/K}(\mathscr{V}_0)},\ \mathbb{Q}/\mathbb{Z}\right),$$

where τ acts by conjugation on the first term and by τ^* on the second. We have isomorphisms

$$\frac{\mathscr{S}_{C/K}(\mathscr{V}_0 \cup \{\mathfrak{q}\})}{\mathscr{S}_{C/K}(\mathscr{V}_0)} = \frac{\mathscr{S}_{C/K}(\mathscr{V}_0 \cup \{\tau\overline{\mathfrak{q}} \cap K\ :\ \tau \in G_F/G_E\})}{\mathscr{S}_{C/K}(\mathscr{V}_0)} \cong C(-1) \otimes \mathbb{Z}[G_F/G_E],$$

with the latter isomorphism being

$$\phi \mapsto \sum_{\tau \in G_F/G_E} \mathrm{fb}^*_{C,K,\tau\overline{\mathfrak{q}}}(\phi) \otimes [\tau].$$

This is an isomorphism by the hypothesis of unpacking, and it respects the G_F structure of both modules by (5.17). The Pontryagin dual of it is the G_F-module

$$\mu_{e_0} \otimes \mathbb{Z}[G_F/G_E].$$

The set of G_L covariants of this module is isomorphic to the final term of the chain (2.6). At the same time, it has the same cardinality as $\pi^{-1}(\mathrm{Frob}_F\overline{\mathfrak{p}}_0)_\sim$ from the above argument. Injectivity of the map of the proposition then follows from surjectivity. $\square$

Finally, we check that a set of places unpacking $(K/F, e_0)$ can always be found.

Proof of Proposition 2.4. Take $\mathscr{V}_2$ to contain all archimedean, all places where K/F ramifies, and all places dividing $[K : F]$ or e_0. Then

$$\ker\left(H^1(G_K, \mathbb{Z}/e_0\mathbb{Z}) \to \prod_{v|\mathscr{V}_2} H^1(G_v, \mathbb{Z}/e_0\mathbb{Z}) \times \prod_{v\nmid\mathscr{V}_2} H^1(I_v, \mathbb{Z}/e_0\mathbb{Z})\right)$$

can be identified with a subset of

$$\mathrm{Hom}\big(\mathrm{Cl}\, K,\ \mathbb{Z}/e_0\mathbb{Z}\big).$$

By adding at most $\log_2 |\mathrm{Cl}\, K|$ places to $\mathscr{V}_1$, we can then make this kernel trivial. Call this new set $\mathscr{V}_1$.

Next, for every conjugacy class of $\mathrm{Gal}(K/F)$, choose a prime $\mathfrak{p}$ of F outside $\mathscr{V}_1$ so, for any $\overline{\mathfrak{p}}$ of $\overline{F}$ over $\mathfrak{p}$, we have that $\mathrm{Frob}_F\overline{\mathfrak{p}}$ represents the conjugacy class. $\mathscr{V}_0$ will consist of these primes and those places in $\mathscr{V}_1$.

Now, choose a finite $\mathrm{Gal}(K/F)$-module M of exponent dividing e_0, and suppose $\phi \in H^1(G_F, M)$ vanishes locally at every place in $\mathscr{V}_0$. Consider the inflation-restriction exact sequence

$$0 \to H^1(\mathrm{Gal}(K/F),\ M) \to H^1(G_F, M) \to H^1(G_K, M).$$

Since ϕ vanishes locally at all places in $\mathscr{V}_1$, the same is true when restricted to G_K. But M over G_K is a direct sum of submodules of $\mathbb{Z}/e_0\mathbb{Z}$, so the above assumptions force ϕ to have zero restriction to G_K.

It then is the inflation of an element ϕ_0 of $H^1(\mathrm{Gal}(K/F),\ M)$. This ϕ_0 vanishes at all the bad places of $\mathscr{V}_2$, and it also vanishes on all cyclic subgroups of $\mathrm{Gal}(K/F)$. This is enough to say that ϕ_0 vanishes locally everywhere, so it lies in $Ш_1(F, M)$. This gives that

$$\ker\left(H^1(G_F, M) \to \prod_{v|\mathscr{V}_0} H^1(G_v, M)\right) = Ш_1(F, M),$$

and Poitou-Tate duality implies that (2.1) is surjective on the right for the module $M^\vee$. We then get the proposition. □

3. Theta groups

A heuristic of Poonen and Rains [44] suggests that p-Selmer groups of abelian varieties can be modeled as the intersection of randomly-selected maximal isotropic spaces in a large quadratic space over $\mathbb{F}_p$. Given an abelian variety A defined over a field of characteristic not equal to p, and given a principal polarization on A defined over F, there is a well-known natural nondegenerate alternating pairing

$$A[p] \otimes A[p] \to \mu_p$$

called the Weil pairing, and their heuristic is based on the fact that this pairing is the bilinear form associated to a certain quadratic form on $A[p]$. This is a trivial observation when p is odd, but relies on a geometric object called the theta group when $p = 2$.

In this section we show that, in a wide set of cases, the theta group of a line bundle and its Galois structure can be recovered from higher Weil pairings. In particular, these objects can be constructed for arbitrary 2-divisible Galois modules with alternating structure. As an application of this more-general theory, we will prove the final part of Proposition 2.12, generalizing a previous result on involution spin [10, Theorem 12.2].

I'd like to thank Adam Morgan for his help with this section, and in particular for finding the construction of $\mathcal{H}$ given below.

Definition 3.1. Suppose we have the following data:

- A group G, G-modules M and N, and a G-equivariant isogeny λ with domain M satisfying

$$2M[2\lambda] = M[\lambda]$$

- An alternating G-equivariant pairing

$$P_1 : M[2\lambda] \otimes M[2\lambda] \to N$$

- A G-equivariant map $e : M[2] \to N$ satisfying

$$e(x+y) - e(x) - e(y) = P_1(x,y) \quad \text{for all } x, y \in M[2].$$

Under these circumstances, there is a unique pairing

$$P_0 : M[\lambda] \otimes M[\lambda] \to N$$

satisfying

$$P_0(2m, 2n) = 2P_1(m,n) \quad \text{for all } m, n \in M[\lambda]$$

This pairing is alternating and G-equivariant since P_1 is.

Following the construction of [43], we can then define a group U to be the set

$$N \times (M[2\lambda])$$

with the same associated G-action but with group operation

$$(n,m) \cdot (n',m') \;=\; \big(n + n' + P_1(m,m'),\, m + m'\big).$$

For any (n,m) and (n',m') in this group, we calculate

$$(n,m)^{-1} = \big(-n,\, -m\big) \quad \text{and}$$

$$(n,m)(n',m')(n,m)^{-1} = \big(n' + 2P_1(m,m'),\, m'\big).$$

From these basic properties, we can verify that

$$\big\{(e(m),\, m) \in U \;:\; m \in M[2]\big\}$$

is a normal subgroup K of U. We then define

$$\mathcal{H}_{\lambda,e,P_1}(M) \,=\, U/K.$$

We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & U & \longrightarrow & M[2\lambda] & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle \times 2} & & \\ 1 & \longrightarrow & N & \longrightarrow & \mathcal{H}_{\lambda,e,P_1}(M) & \longrightarrow & M[\lambda] & \longrightarrow & 1. \end{array} \tag{3.1}$$

The groups U and $\mathcal{H}$ are typically non-abelian, and we can consider the commutator pairings on either of the rows of (3.1). From the calculation

$$(0,m)\cdot(0,m')\cdot(0,m)^{-1}\cdot(0,m')^{-1} = \big(2P_1(m,m'),0\big),$$

we see that this pairing takes the form $(m,\, m') \mapsto 2P_1(m,m')$ for the top row. On the bottom row, this pairing is then given by $(m,\, m') \mapsto P_0(m,m')$.

Proposition 3.2. *Take*

$$q : H^1\big(G,\, M[\lambda]\big) \to H^2(G,N)$$

to be the connecting map coming from the second row of (3.1)*, and write*

$$\cup : H^1\big(G,\, M[\lambda]\big) \otimes H^1\big(G,\, M[\lambda]\big) \to H^2(G,N).$$

for the cup product induced by P_0. Then, for any $\phi, \psi \in H^1\big(G,\, M[\lambda]\big)$, we have

$$q(\phi+\psi) - q(\phi) - q(\psi) = -\phi\cup\psi.$$

We also have

$$q(a\phi) = a^2 q(\phi)$$

for any integer a.

Proof. Given our calculation of the commutator pairing above, the first claim here is a consequence of [43, Proposition 2.9].

To prove the second statement, note that the equivariant homomorphism

$$(n, m) \mapsto (a^2 n, am)$$

of U descends to $\mathcal{H}_{\lambda,e,P_1}(M)$. We then get a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & \mathcal{H}_{\lambda,e,P_1}(M) & \longrightarrow & M[\lambda] & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \times a^2} & & \downarrow & & \downarrow{\scriptstyle \times a} & & \\ 1 & \longrightarrow & N & \longrightarrow & \mathcal{H}_{\lambda,e,P_1}(M) & \longrightarrow & M[\lambda] & \longrightarrow & 1. \end{array}$$

from which the result follows.

□

Proposition 3.3. *Suppose we are in the situation of the above proposition. Choose a positive integer $k \geq 1$. We assume that*

$$2^{k+1} M[2^{2k+1}\lambda] = M[2^k \lambda]$$

and that there is a G-equivariant pairing

$$P_{k+1} : M[2^{k+1}\lambda] \otimes M[2^{k+1}\lambda] \to N$$

satisfying

$$2^k P_{k+1}(m, m') = P_1(2^k m, 2^k m') \quad \textit{for} \quad m, m' \in M\left[2^{k+1}\lambda\right].$$

Then q is zero on all elements in the image of the connecting map

$$H^0\big(G,\, M[2^k\lambda]/M[\lambda]\big) \to H^1\big(G,\, M[\lambda]\big)$$

coming from the exact sequence

$$0 \to M[\lambda] \to M[2^k\lambda] \to M[2^k\lambda]/M[\lambda] \to 0.$$

Proof. Choose $x_k \in M[2^k\lambda]$ so x_k is invariant under G mod $M[\lambda]$. Our goal is to prove that

$$\phi_k(\sigma) = \sigma x_k - x_k \in H^1(G, M[\lambda])$$

maps to zero under q.

Choose $x_{k+i} \in M[2^{k+i}\lambda]$ for i equal to $1, k+1$ so that

$$x_{k+1} = 2^k x_{2k+1} \quad \text{and} \quad x_k = 2^{k+1} x_{2k+1}.$$

We can then take

$$\phi_{k+i} = \sigma x_{k+i} - x_{k+i} \quad \text{in} \;\; H^1(G, M[2^i\lambda]).$$

for $i = 1, k+1$. From the diagram (3.1) and Corollary 2.8 of [43], we have

$$q(\phi_k) = \phi_{k+1} \cup_{P_1} \phi_{k+1},$$

where the cup product is with respect to the pairing P_1. This then equals

$$(2^k \phi_{2k+1}) \cup_{P_{k+1}} \phi_{2k+1},$$

where the $\cup_{P_{k+1}}$ denotes the cup product on $H^1(G, M[2^{k+1}\lambda])$ coming from P_{k+1}. But $2^k x_{2k+1}$ lies in $M[2^{k+1}\lambda]$, so $2^k\phi_{2k+1}$ is a coboundary. This cup product is then zero, and we have the proposition. □

3.1. **Theta groups of abelian varieties.** Take F to be a field of characteristic other than 2, take A to be an abelian variety over the field F, and take L to be a symmetric line bundle over A also defined over F with associated isogeny $\lambda : A \to \widehat{A}$. We assume the degree of L is not divisible by the characteristic of F.

For $x \in A(\overline{F})$, take $\tau_x : A \to A$ to be the translation by x map. We can then define a group

$$\mathcal{H}(L) = \left\{(x, \phi) \,:\, x \in A[\lambda],\ \phi : L \xrightarrow{\sim} \tau_x^* L\right\}$$

with a natural G_F action. This group is the theta group, or Mumford group, and our main references for its properties are [44] and [38]. We note that it fits in an exact sequence.

$$1 \to \overline{F}^\times \to \mathcal{H}(L) \to A[\lambda] \to 1. \tag{3.2}$$

Proposition 3.4. *In the above situation, take $G = G_F$, take N to equal $\overline{F}^\times$, and take P_1 to be the multiplicative inverse of the Weil pairing associated to $L^2 = L \otimes L$. Finally, let e be the quadratic form*

$$e_*^L : A[2] \to \pm 1$$

defined in [38, p. 304].

Then there is a canonical isomorphism

$$\eta : \mathcal{H}_{\lambda, e, P_1}(A) \to \mathcal{H}(L)$$

of groups with a G_F-action so that (3.2) *and* (3.1) *fit in a commutative diagram*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N & \longrightarrow & \mathcal{H}_{\lambda,e,P_1}(A) & \longrightarrow & A[\lambda] & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle \eta} & & \| & & \\
1 & \longrightarrow & \overline{F}^\times & \longrightarrow & \mathcal{H}(L) & \longrightarrow & A[\lambda] & \longrightarrow & 1.
\end{array}$$

Proof. Using the fact that L is a symmetric line bundle, Mumford defines canonical homomorphisms

$$\delta_{-1} : \mathcal{H}(L^2) \to \mathcal{H}(L^2) \quad \text{and} \quad \eta_2 : \mathcal{H}(L^2) \to \mathcal{H}(L)$$

fitting into the commutative diagrams

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{F}^\times & \longrightarrow & \mathcal{H}(L^2) & \longrightarrow & A[2\lambda] & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \delta_{-1}} & & \downarrow{\scriptstyle \times -1} & & \\ 1 & \longrightarrow & \overline{F}^\times & \longrightarrow & \mathcal{H}(L^2) & \longrightarrow & A[2\lambda] & \longrightarrow & 1 \end{array}$$

and

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{F}^\times & \longrightarrow & \mathcal{H}(L^2) & \longrightarrow & A[2\lambda] & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle x\mapsto x^2} & & \downarrow{\scriptstyle \eta_2} & & \downarrow{\scriptstyle \times 2} & & \\ 1 & \longrightarrow & \overline{F}^\times & \longrightarrow & \mathcal{H}(L) & \longrightarrow & A[\lambda] & \longrightarrow & 1, \end{array}$$

with the appearance of $A[2\lambda]$ explained by [38, Proposition 4, p. 310].

Given x in $A[2\lambda]$, there is some $\psi(x)$ in $\mathcal{H}(L^2)$ projecting to x satisfying $\psi(x)^{-1} = \delta_{-1}(\psi(x))$. This element is determined up to sign; in particular, $\eta' = \eta_2 \circ \psi$ is canonically defined on $A[2\lambda]$, and we have a commutative diagram

$$\begin{array}{ccccccccc} & & & & & & A[2\lambda] & & \\ & & & & & \swarrow^{\eta'} & \downarrow{\scriptstyle \times 2} & & \\ 1 & \longrightarrow & \overline{F}^\times & \longrightarrow & \mathcal{H}(L) & \longrightarrow & A[\lambda] & \longrightarrow & 1. \end{array}$$

For $x, y \in A[2\lambda]$, we have

$$\delta_{-1}\big(\psi(x)\psi(y)\big) = \psi(x)^{-1}\psi(y)^{-1} = \big(\psi(x)^{-1}\psi(y)^{-1}\psi(x)\psi(y)\big) \cdot \big(\psi(x)\psi(y)\big)^{-1}.$$

$$= e^{L^2}(x,y)\big(\psi(x)\psi(y)\big)^{-1},$$

with our notation and definition of the Weil pairing e^{L^2} as in Mumford's article. Correcting for this, we find

$$\psi(x+y) \in \pm\frac{1}{\sqrt{e^{L^2}(x,y)}} \cdot \psi(x)\psi(y),$$

so we have

$$\eta'(x+y) = P_1(x,y) \cdot \eta'(x)\eta'(y).$$

This agrees with the multiplication in U as in (3.1), and we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \overline{F}^{\times} & \longrightarrow & U & \longrightarrow & A[2\lambda] & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle \times 2} & & \\ 1 & \longrightarrow & \overline{F}^{\times} & \longrightarrow & \mathcal{H}(L) & \longrightarrow & A[\lambda] & \longrightarrow & 1, \end{array}$$

where the central map sends $(\zeta, x) \in \overline{F}^{\times} \times A[2\lambda]$ to $\zeta \cdot \eta'(x)$.

To prove the proposition, we just need to verify that the kernel of this map is the set of $\big(e_*^L(x), x\big)$, with x ranging through the two-torsion points. Given the above diagram, it is clear that the kernel should be the set of $\big(\eta'(x), x\big)$, where $\eta'(x) \in \mathcal{H}(L)$, which projects to 0 in $A[\lambda]$, is instead considered in $\overline{F}^{\times}$. We thus just need that

$$\eta'(x) = e_*^L(x) \quad \text{for all} \quad x \in A[2].$$

But this is a consequence of [38, Proposition 6], and we have the proposition. □

Remark 3.5. For this example, the hypotheses of Proposition 3.3 can be shown to be satisfied using the Weil pairings for L^4, L^8, ..., so both Proposition 3.2 and 3.3 hold in this case. This was already established in [44], with Proposition 3.3 being shown for the Kummer map associated with the exact sequence

$$0 \to A[\lambda] \to A \to \widehat{A} \to 0.$$

The key element of this elegant proof was the use of the Poincaré bundle on $A \times \widehat{A}$ to define a certain set acted on freely by $\mathcal{H}(L)$. For Proposition 3.3, we used higher divisibility of M as a stand-in for this geometry, and accepted that the end result would necessarily be weaker.

The advantage of our approach is that it opens up the possibility of working with theta groups not coming from abelian varieties. We turn to one such example next.

3.2. **Involution spin.** Take F to be a field of characteristic not equal to 2 and choose an element α of $F^{\times}$. We assume that α is not a root of unity and that α is not in $(F^{\times})^2$, so

$K = F(\sqrt{\alpha})$ is a quadratic extension. Fixing $k > 1$, we consider the quotient group

$$M_k = \left\{x \in \overline{F}^\times \ : \ x^{2^k} = \alpha^i \text{ for some } i \in \mathbb{Z}\right\} \Big/ \left\{\alpha^j \ : \ j \in \mathbb{Z}\right\},$$

where these sets are abelian groups with multiplication as their operation. Given x in this quotient, take $v(x)$ to be an integer so some representative of the class of x satisfies

$$x^{2^k} = \alpha^{v(x)}.$$

This integer is defined mod 2^k, and we have an alternating G_F-equivariant pairing

$$P_{k-1} : M_k \otimes M_k \longrightarrow \mu_{2^k} \subseteq \overline{F}^\times$$

defined by

$$P_{k-1}(x, y) = \frac{y^{v(x)}}{x^{v(y)}} \quad \text{for } \ x, y \in M.$$

We can then define the theta group $\mathcal{H}_{2,0,P_1}(M_k)$, and we consider the map

$$q_H : H^1(H, M_k[2]) \to H^2(H, \mu_4)$$

defined in Proposition 3.2. Here, H is any subgroup of G_F.

The module $M_k[2]$ is trivial over G_K, and the Kummer map associated to

$$0 \to M_k[2] \to M_k[4] \to M_k[2] \to 0$$

gives a map

$$\delta : M_k[2] \to H^1(G_K, M_k[2]).$$

Note that $\delta(x)$ is defined over $K(\mu_4, \sqrt[4]{\alpha})$.

From considering quadratic twists and using Proposition 3.3, we find that, for any $\chi \in H^1(G_K, \mathbb{F}_2)$ and any x in $H^0(G_K, M_k[2])$, we have

$$q_{G_K}(\delta(x) + x \cup \chi) = 0. \tag{3.3}$$

We calculate

$$\delta([\sqrt{\alpha}]) = [-1] \cup \chi_{\sqrt{\alpha}} \quad \text{and} \quad \delta([-1]) = [-1] \cup \chi_{-1},$$

where χ_b denotes the quadratic character associated to $K(\sqrt{b})/K$.

We can now finish the proof of Proposition 2.12.

Proposition 3.6. *Suppose we are in the situation of Notation 2.2 with $e_0 = 2$ and K/F a quadratic extension. Take τ to be an element of G_F projecting to the nontrivial element of* Gal(K/F). *Then, given primes $\overline{\mathfrak{p}}, \overline{\mathfrak{p}}_0$ of $\overline{F}$ not over $\mathscr{V}_0$, if $\overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0$, we have*

$$a_\tau^{\text{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}) = a_\tau^{\text{nc}}(\overline{\mathfrak{p}}_0, \overline{\mathfrak{p}}_0).$$

We first will show that this proposition implies Proposition 2.12, part 7. In the notation of that proposition, if τ shares a class with 1 in $G_L \backslash G_F / G_L$, we can apply the sixth part of the proposition. So suppose this is not the case. Writing σ for a generator of Gal(K/L), we must have

$$\sigma^k \tau = \tau^{-1} \sigma^j \quad \text{in Gal}(K/F)$$

for some integers k, j. By replacing τ with $\sigma^k \tau$ as needed, we may as well assume we have

$$\tau^2 = \sigma^{j+k} \quad \text{in Gal}(K/F).$$

Then σ^{j+k} is in both G_L and $G_{\tau L}$, but τ is in neither. We can then apply Proposition 3.6 with

$$K = L + \tau L \quad \text{and} \quad F = (L + \tau L)^\tau.$$

We now turn to the proof of the above proposition.

Proof of Proposition 3.6. We first claim that we can write $K = F(\sqrt{\alpha})$ with α not a root of unity so that $K(\mu_4, \sqrt[4]{\alpha})$ is a subfield of $K(\mathscr{V}_0)$. To see this, first choose any α so $K = F(\sqrt{\alpha})$. In F, we have a decomposition of ideals

$$(\alpha) = I_0 \cdot I^2$$

where I_0 is a product of primes of $\mathscr{V}_0$ and I is some other fractional ideal of K. But, since $\mathscr{V}_0$ unpacks μ_2 over F, we can write

$$I = (\beta) \cdot J_0 \cdot J^2$$

with β in F, J_0 a product of primes of $\mathscr{V}_0$, and J some other fractional ideal. We then replace α with α/β^2 unless this number is a root of unity, in which case we replace it with $4\alpha/\beta^2$.

From (5.3), we have

$$\mathrm{res}^{G_F}_{G_K} \mathfrak{B}^{\mathrm{nc}}_{M_1,F,\overline{\mathfrak{p}}}([\sqrt{\alpha}]) = [\sqrt{\alpha}] \cup \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}}) \ + \ [-\sqrt{\alpha}] \cup \tau_* \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}})$$

where the cup product is between $H^1(G_K, \mu_2)$ and $H^0(G_K, M_1)$. We can rewrite this as

$$\left(\mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}}) \cup [\sqrt{\alpha}] \ + \ \delta([\sqrt{\alpha}])\right) \ + \ \left(\tau_* \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}}) \cup [-\sqrt{\alpha}] \ + \ \delta([-\sqrt{\alpha}])\right) \ + \ \delta([-1]).$$

Using bilinearity and (3.3), we have

$$q_{G_K}(\mathfrak{B}^{\mathrm{nc}}_{M_1,F,\overline{\mathfrak{p}}}([\sqrt{\alpha}])) \ = \ \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}}) \cup \tau_* \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}}) \ + \ \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}}) \cup \chi_{\sqrt{\alpha}} \ + \ \tau_* \mathfrak{B}^{\mathrm{nc}}(\overline{\mathfrak{p}}) \cup \chi_{-\sqrt{\alpha}}.$$

where the cup pairing is the standrad one on $H^1(G_K, \mu_2)$. From the assumptions on α, $\overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0$ implies

$$\begin{aligned} &\mathrm{inv}_{\mu_4,F,\overline{\mathfrak{p}}} \left(q_{G_F}\left(\mathfrak{B}^{\mathrm{nc}}_{M_1,F,\overline{\mathfrak{p}}}([\sqrt{\alpha}])\right)\right) \ - \ a^{\mathrm{nc}}_{\tau}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}) \\ &\quad = \mathrm{inv}_{\mu_4,F,\overline{\mathfrak{p}}_0} \left(q_{G_F}\left(\mathfrak{B}^{\mathrm{nc}}_{M_1,F,\overline{\mathfrak{p}}_0}([\sqrt{\alpha}])\right)\right) \ - \ a^{\mathrm{nc}}_{\tau}(\overline{\mathfrak{p}}_0, \overline{\mathfrak{p}}_0). \end{aligned}$$

But Poitou-Tate reciprocity also gives us

$$\mathrm{inv}_{\mu_4,F,\overline{\mathfrak{p}}} \left(q_{G_F}\left(\mathfrak{B}^{\mathrm{nc}}_{M_1,F,\overline{\mathfrak{p}}}([\sqrt{\alpha}])\right)\right) \ = \ \sum_{v \in \mathscr{V}_0} \mathrm{inv}_{\mu_4,F,\overline{v}} \left(q_{G_F}\left(\mathfrak{B}^{\mathrm{nc}}_{M_1,F,\overline{\mathfrak{p}}}([\sqrt{\alpha}])\right)\right),$$

and this latter sum is determined by the class of $\overline{\mathfrak{p}}$ in $\mathrm{Gal}(K(\mathscr{V}_0)/F)$. This finishes the proof. $\square$

4. THE CASSELS-TATE PAIRING

The Cassels-Tate pairing is typically defined as a pairing between the Shafarevich-Tate group of an abelian variety over a global field and the Shafarevich-Tate group of the dual abelian variety, as per [51] or [36]. Flach later generalized the setup to handle Shafarevich-Tate groups coming from ℓ-divisible Galois modules defined over global fields [8].

However, the Cassels-Tate pairing is perhaps most easily defined and understood at the level of finite Galois modules. Because we think this simple reframing is of some independent interest, we will keep the notation for these results self-contained and prove them for general global fields.

Notation 4.1. Take F to be a global field (either a number field or a finite extension of the function field $\mathbb{F}_\ell[t]$ for some prime ℓ). Take S to be a set of places of F, take ${}^S F$ to be the maximal separable extension of F that is ramified only at the places of S, and write $G_{F,S}$ for the Galois group $\mathrm{Gal}({}^S F/F)$. For each place $v \in S$, take F_v to be the completion of F at v, fix a separable closure F_v^s of F_v, and fix an embedding ${}^S F \hookrightarrow F_v^s$. These embeddings induce homomorphisms $G_v \to G_{F,S}$, allowing us to view $G_{F,S}$ modules as G_v modules.

Take M to be a finite module with a continuous $G_{F,S}$ action. We assume that the characteristic of F does not divide the order of M. In addition, if F is a number field, we assume S contains all primes that divide the order of M and all archimedean primes.

For $v \in S$, choose a subgroup W_v of $H^1(G_v, M)$, where we use H^i to denote the standard continuous group cohomology. We assume that, for all but finitely many v, W_v is the set of unramified cocycle classes. We then take

$$\mathrm{Sel}\,(M, (W_v)_{v\in S}) = \ker\left(H^1(G_{F,S}, M) \to \prod_{v\in S} H^1(G_v, M)/W_v\right).$$

We will write $M^\vee$ for the module $\mathrm{Hom}\left(M, {}^S F^\times\right)$. Local Tate duality gives a perfect pairing

$$H^1(G_v, M) \times H^1(G_v, M^\vee) \to \mathbb{Q}/\mathbb{Z},$$

and we write $W_v^\perp$ for the orthogonal complement of W_v in $H^1(G_v, M^\vee)$.

Take

$$0 \to M_1 \xrightarrow{\iota} M \xrightarrow{\pi} M_2 \to 0 \tag{4.1}$$

to be an exact sequence of $G_{F,S}$ modules. The dual exact sequence has the form

$$0 \to M_2^\vee \xrightarrow{\pi^\vee} M^\vee \xrightarrow{\iota^\vee} M_1^\vee \to 0.$$

The Cassels-Tate pairing gives an answer to the following question: given M and $(W_v)_v$ as in Notation 4.1, and given the exact sequence (4.1), when can an element ϕ of $\text{Sel}(M_2, (\pi_*(W_v))_v)$ be lifted to an element of $\text{Sel}(M, (W_v)_v)$? We will first state our main result before giving an intuitive argument for why this result makes sense.

Proposition 4.2.

(1) With all notation as in Notation 4.1, including an exact sequence (4.1)*, the natural pairing*

$$\text{CTP}_{\iota,\pi} : \text{Sel}\left(M_2, (\pi_*(W_v))_v\right) \times \text{Sel}\left(M_1^\vee,\ \left(\iota_*^\vee(W_v^\perp)\right)_v\right) \to \mathbb{Q}/\mathbb{Z}$$

given in Definition 4.4 is well-defined and bilinear.

(2) Suppose we have

$$\phi \in \text{Sel}\left(M_2, (\pi_*(W_v))_v\right) \quad \textit{and} \quad \psi \in \text{Sel}\left(M_1^\vee,\ \left(\iota_*^\vee(W_v^\perp)\right)_v\right).$$

Taking β to be the standard isomorphism $(M_2^\vee)^\vee \xrightarrow{\sim} M_2$, we then have

$$\text{CTP}_{\iota,\pi}(\phi, \psi) \;=\; \text{CTP}_{\pi^\vee, \iota^\vee}(\psi, \beta_*(\phi)).$$

(3) The left and right kernels of $\text{CTP}_{\iota,\pi}$ are

$$\pi_*(\text{Sel}(M, (W_v)_v)) \quad \textit{and} \quad (\iota^\vee)_*(\text{Sel}(M^\vee, (W_v^\perp)_v)), \quad \textit{respectively}.$$

We now sketch the source of this pairing. There seem to be two distinct obstructions to lifting an element ϕ from $\text{Sel}(M_2, (\pi_*(W_v))_v)$ to $\text{Sel}(M, (W_v)_v)$. First, the long exact sequence for group cohomology gives us an exact sequence

$$H^1(G_{F,S}, M) \xrightarrow{\pi_*} H^1(G_{F,S}, M_2) \to H^2(G_{F,S}, M_1).$$

After considering local conditions, this gives an exact sequence

(4.2)

$$0 \to \pi_*(H^1(G_{F,S}, M)) \cap \text{Sel}(M_2, (\pi_*(W_v))_v) \to \text{Sel}(M_2, (\pi_*(W_v))_v) \to Ш_2(M_1),$$

where we have taken

$$Ш_2(M_1) = \ker\left(H^2(G_{F,S}, M_1) \to \prod_{v\in S} H^2(G_v, M_1)\right).$$

In particular, ϕ only lifts to $H^1(G_{F,S}, M)$ if its image in $Ш_2$ is zero

If ϕ lifts to a cocycle, it may still not lift to an element of $\text{Sel}(M, (W_v)_v)$. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} & & H^1(G_{F,S}, M_1) & \longrightarrow & H^1(G_{F,S}, M) & \longrightarrow & \ker\left(\begin{array}{l} H^1(G_{F,S}, M_2) \\ \to H^2(G_{F,S}, M_1)\end{array}\right) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod_{v\in S} \frac{H^1(G_v, M_1)}{\iota_*^{-1}(W_v)} & \longrightarrow & \prod_{v\in S} \frac{H^1(G_v, M)}{W_v} & \longrightarrow & \prod_{v\in S} \frac{H^1(G_v, M_2)}{\pi_*(W_v)}. \end{array}$$

The snake lemma then gives an exact sequence

$$\begin{aligned} (4.3) \qquad 0 \to \pi_*(\text{Sel}(M, (W_v)_v)) \to \ker\Big(\text{Sel}\big(M_2,\ (\pi_*(W_v))_v\big) \to Ш_2(M_1)\Big) \\ \to \text{cok}\left(H^1(G_{F,S}, M_1) \to \prod_{v\in S} \frac{H^1(G_v, M_1)}{\iota_*^{-1}(W_v)}\right). \end{aligned}$$

If ϕ maps to zero in this cokernel, we then get that it is of the form $\pi_*(\phi')$ for some ϕ' in $\text{Sel}(M, (W_v)_v)$. This cokernel then gives the second obstruction to finding a Selmer lift of the element ϕ.

The key observation about this situation is that, under Poitou-Tate duality, the group $Ш_2(M_1)$ is dual to

$$Ш_1(M_1^\vee) = \ker\left(H^1(G_{F,S}, M_1^\vee) \to \prod_{v\in S} H^1(G_v, M_1^\vee)\right),$$

and the final term of the sequence (4.3) is dual to

$$\ker\left(H^1(G_{F,S}, M_1^\vee) \to \prod_{v\in S} \frac{H^1(G_v, M_1^\vee)}{\iota_*^{-1}(W_v)^\perp}\right) \Big/ Ш_1(M_1^\vee).$$

We can then account for both obstructions using two filtered pieces of the Selmer group

$$\text{Sel}\left(M_1^\vee,\ \left(\iota_*^\vee(W_v^\perp)\right)_v\right).$$

This basic framework accounts for the form of the pairing in Proposition 4.2.

To define this pairing, we will work with cohomology groups using the language of inhomogeneous cocycles, so we first recall this notation.

Notation 4.3. Given a topological group G and a discrete module M with a continuous G action, and given $i \geq 0$, we take $C^i(G, M)$, or the set of i-cochains, to be the set of maps from G^i to M. For $i \geq 0$, we can define a coboundary operator

$$d : C^i(G, M) \to C^{i+1}(G, M)$$

by

$$\begin{aligned} df(\sigma_1, \ldots, \sigma_{i+1}) = &\sigma_1 f(\sigma_2, \sigma_3, \ldots, \sigma_{i+1}) \\ &+ \sum_{j=1}^{i} (-1)^j f(\sigma_1, \ldots, \sigma_{j-1}, \sigma_j\sigma_{j+1}, \sigma_{j+2}, \ldots, \sigma_{i+1}) \\ &+ (-1)^{i+1} f(\sigma_1, \ldots, \sigma_i). \end{aligned}$$

We call an i-cochain f a cocycle if $df = 0$, and we call it a coboundary if it is of the form dg for some $(i-1)$-cochain g. Writing Z^i for the set of i-cocycles and B^i for the set of i-coboundaries, we define

$$H^i(G, M) = Z^i(G, M)/B^i(G, M).$$

Finally, suppose we have discrete G-modules M_1, M_2, N and a bilinear G-equivariant pairing

$$P : M_1 \otimes M_2 \to N.$$

Given $f_1 \in C^i(G, M_1)$ and $f_2 \in C^j(G, M_2)$, we define an element $f_1 \cup_P f_2$ in $C^{i+j}(G, N)$ by

$$f_1 \cup_P f_2(\sigma_1, \ldots, \sigma_{i+j}) = P\left(f_1(\sigma_1, \ldots, \sigma_i), \sigma_1\sigma_2 \ldots \sigma_i f_2(\sigma_{i+1}, \ldots, \sigma_{i+j})\right).$$

The standard cohomological cup product is recovered by restricting this construction to cocycles [41, Proposition 1.4.8].

Definition 4.4 (Cassels-Tate pairing)**.** Given F, M, S, and $(W_v)_{v\in S}$ as in Notation 4.1, and given the exact sequence (4.1) of $G_{F,S}$ modules, we define a pairing

$$\text{CTP}_{\iota,\pi} : \text{Sel}\left(M_2, (\pi_*(W_v))_v\right) \times \text{Sel}\left(M_1^\vee, \left(\iota_*^\vee(W_v^\perp)\right)_v\right) \to \mathbb{Q}/\mathbb{Z}$$

as follows:

Suppose (ϕ, ψ) is in the domain of this map, and choose cocycles $\overline{\phi} \in Z^1(G_{F,S}, M_2)$ and $\overline{\psi} \in Z^1(G_{F,S}, M_1^\vee)$ representing this pair of Selmer elements. Choose $f : G_{F,S} \to M$ so

$$\overline{\phi} = \pi \circ f.$$

Then df lies in $Z^2(G_{F,S}, M_1)$. Take $\mathcal{O}_{F,S}^\times$ to be the subset of ${}^S F$ where the valuation at all places outside S is trivial. We have a standard perfect $G_{F,S}$-equivariant pairing

$$M_1 \otimes M_1^\vee \to \mathcal{O}_{F,S}^\times.$$

From Poitou-Tate duality [36], we have

$$H^3(G_{F,S},\, \mathcal{O}_{F,S}^\times) = 0,$$

so there is some

$$\epsilon : G_{F,S} \times G_{F,S} \to \mathcal{O}_{F,S}^\times$$

so that

$$d\epsilon = df \cup \overline{\psi} \quad \text{in } Z^3\left(G_{F,S},\, \mathcal{O}_{F,S}^\times\right).$$

Denoting the restriction to G_v by a subscript v, we can lift each $\overline{\phi}_v$ to an element $\overline{\phi}_{v,M}$ of $Z^1(G_v, M)$ that projects to W_v. Having done this, we find that

$$(f_v - \overline{\phi}_{v,M}) \cup \overline{\psi}_v - \epsilon_v$$

lies in $Z^2\left(G_v, \mathcal{O}_{F,S}^\times\right)$, and can define

$$\text{CTP}(\phi, \psi) = \sum_{v \in s} \text{inv}_v \left((f_v - \overline{\phi}_{v,M}) \cup \overline{\psi}_v - \epsilon_v \right),$$

where inv_v is the standard map $H^2(G_v, \overline{F_v}^\times) \to \mathbb{Q}/\mathbb{Z}$.

Proof of Proposition 4.2 (1). To prove the pairing is well-defined, we must prove it does not depend on the choice of the tuple

$$(\overline{\psi},\, \overline{\phi},\, f,\, (\overline{\phi}_{v,M})_v,\, \epsilon).$$

So suppose we have fixed one such tuple obeying the requirements of the definition.

- If $(\overline{\psi}, \overline{\phi}, f, (\overline{\phi}_{v,M})_v, \epsilon + \Delta)$ also obeys the requirements of the definition, we get that Δ is in $Z^2(G_F, \overline{F}^\times)$, and Poitou-Tate duality gives

  $$\sum_{v \in S} \text{inv}_v(\Delta_v) = 0.$$

  Thus, the choice of ϵ does not affect the result.
- If $(\overline{\psi}, \overline{\phi}, f, (\overline{\phi}_{v,M} + \Delta_v)_v)$ obeys the requirements of the definition, then so does the full tuple

  $$(\overline{\psi},\, \overline{\phi},\, f,\, (\overline{\phi}_{v,M} + \Delta_v)_v,\, \epsilon),$$

  and we may compute the pairing from this data instead without changing the value. The requirements of the definition force Δ_v to lie in $\iota_*^{-1}(W_v)$, so $\Delta_v \cup \psi_v$ is trivial in $H^2(G_v, \overline{F}^\times)$. The choice of $(\overline{\phi}_{v,M})_v$ thus does not affect the result.
- If $(\overline{\psi}, \overline{\phi}, f + \Delta)$ obeys the requirements of the definition, we get that Δ takes values in M_1. This partial tuple then extends to a full tuple

  $$\left(\overline{\psi},\, \overline{\phi},\, f + \Delta,\, (\overline{\phi}_{v,M})_v,\, \epsilon + \Delta \cup \overline{\psi}\right).$$

  This tuple gives an identical result to the orginal tuple, so the choice of f has no effect.
- If $(\overline{\psi}, \overline{\phi} + \Delta)$ obeys the requirements of the definition, we find that Δ can be written as dx_2 for some $x_2 \in M_2$. Choose $x \in M$ so $\pi(x) = x_2$. Then this partial tuple can be extended to a full tuple

  $$\left(\overline{\psi},\, \overline{\phi} + \Delta,\, f + dx,\, ((dx)_v + \overline{\phi}_{v,M})_v,\, \epsilon\right).$$

This tuple gives an identical result to the orginal tuple, so the choice of f has no effect.

- If $(\overline{\psi} + \Delta)$ obeys the requirements of the definitionn, Δ can be written as dy_1 with y_1 in $M_1^\vee$. Choose y so $\iota^\vee(y) = y_1$. Then the partial tuple can be extended to the full tuple

$$(\overline{\psi} + \Delta,\, \overline{\phi},\, f,\, (\overline{\phi}_{v,M})_v,\, \epsilon + df \cup y).$$

  The difference between the result computed from this tuple and the original is given by

$$\sum_{v \in S} \text{inv}_v \left((f_v - \phi_{v,M}) \cup dy - df_v \cup y \right) = \sum_{v \in S} \text{inv}_v \left(-d \left((f_v - \phi_{v,M}) \cup y \right) \right) = 0,$$

  so the pairing does not depend on the choice of $\overline{\psi}$.

The bilinearity of the pairing is immediate, finishing the proof of the first part of the proposition. □

We will next turn to the proof of the second part of the proposition. In the context of Definition 4.4, choose $\epsilon' \in C^2(G_{F,S},\, \mathcal{O}_{F,S}^\times)$ so that

$$d\epsilon' = -\overline{\psi} \cup df.$$

We then claim that we have

$$\text{CTP}(\phi, \psi) = -\sum_{v \in s} \text{inv}_v \left(\overline{\psi}_v \cup (f_v - \overline{\phi}_{v,M}) - \epsilon'_v \right). \tag{4.4}$$

This can be proved directly by a coboundary calculation. First, define $h \in C^2(G_{F,S},\, \mathcal{O}_{F,S}^\times)$ by

$$h(\sigma, \tau) = \left\langle df(\sigma, \tau),\, \overline{\psi}(\sigma\tau) \right\rangle,$$

where the pairing is the natural one. We then have

$$\begin{aligned} dh(\sigma,\tau,\epsilon) &= \left\langle \sigma df(\tau,\epsilon),\, \sigma\overline{\psi}(\tau\epsilon)\right\rangle \,-\, \left\langle df(\sigma\tau,\epsilon),\, \overline{\psi}(\sigma\tau\epsilon)\right\rangle \\ &\quad + \left\langle df(\sigma,\tau\epsilon),\, \overline{\psi}(\sigma\tau\epsilon)\right\rangle \,-\, \left\langle df(\sigma,\tau),\, \overline{\psi}(\sigma\tau)\right\rangle \\ &= -\left\langle \sigma df(\tau,\epsilon),\, \overline{\psi}(\sigma)\right\rangle + \left\langle df(\sigma,\tau),\, \sigma\tau\overline{\psi}(\epsilon)\right\rangle \\ &= \left(df\cup\overline{\psi} - \overline{\psi}\cup df\right)(\sigma,\tau,\epsilon) = (d\epsilon + d\epsilon')(\sigma,\tau,\epsilon) \end{aligned}$$

with the second equality following from bilinearity and the relations

$$df(\sigma,\tau\epsilon) - df(\sigma\tau,\epsilon) = df(\sigma,\tau) - \sigma df(\tau,\epsilon) \quad \text{and}$$

$$\overline{\psi}(\sigma\tau\epsilon) = \sigma\overline{\psi}(\tau\epsilon) + \overline{\psi}(\sigma) = \sigma\tau\overline{\psi}(\epsilon) + \overline{\psi}(\sigma\tau).$$

We can then take $\epsilon' = h - \epsilon$. Per Proposition 4.2 (1), this will not change the value of the pairing.

To prove (4.4), we need to show

$$\sum_{v\in s} \mathrm{inv}_v\left(\overline{\psi}_v\cup(f_v-\overline{\phi}_{v,M}) + (f_v-\overline{\phi}_{v,M})\cup\overline{\psi}_v - h_v\right) = 0. \tag{4.5}$$

A similar calculation to the one given before gives

$$d\gamma_v = \overline{\psi}_v\cup(f_v-\overline{\phi}_{v,M}) + (f_v-\overline{\phi}_{v,M})\cup\overline{\psi}_v - h_v,$$

where $\gamma_v \in C^1(G_v, \overline{F_v}^{\times})$ is defined by

$$\gamma_v(\sigma) = -\left\langle \overline{\psi}_v(\sigma),\, (f_v-\overline{\phi}_{v,M})(\sigma)\right\rangle \quad \text{for } \sigma\in G_v.$$

Then each summand of (4.5) is zero, and we have (4.4).

Proof of Proposition 4.2 (2). Choose $(\overline{\psi},\, \overline{\phi},\, f,\, (\overline{\phi}_{v,M})_v,\, \epsilon)$ associated to $\mathrm{CTP}_{\iota,\pi}(\phi,\psi)$. Choose $g\in C^1(G_F, M^\vee)$ so $\iota^\vee\circ g$ equals $\overline{\psi}$. Finally, for $v\in S$, choose $\overline{\psi}_{v,M^\vee}$ in $Z^1(G_v, M^\vee)$

projecting to $W_v^\perp$ satisfying $\iota^\vee \circ \overline{\psi}_{v,M^\vee} = \overline{\psi}_v$. We have

$$d(f \cup g) = df \cup \overline{\phi} - \overline{\psi} \cup dg,$$

and (4.4) gives

$$\begin{aligned}
&\text{CTP}_{\iota,\pi}(\phi,\psi) - \text{CTP}_{\pi^\vee,\iota^\vee}(\psi, \beta_*(\phi)) \\
&\quad = \sum_{v\in S} \text{inv}_v \left(\left(f_v - \overline{\phi}_{v,M}\right) \cup \overline{\psi}_v \; + \; \overline{\phi}_v \cup \left(g_v - \overline{\psi}_{v,M^\vee}\right) - (f\cup g)_v \right) \\
&\quad = \sum_{v\in S} \text{inv}_v \left(- \left(f_v - \overline{\phi}_{v,M}\right) \cup \left(g_v - \overline{\psi}_{v,M^\vee}\right) \; - \; \overline{\phi}_{v,M} \cup \overline{\psi}_{v,M^\vee} \right)
\end{aligned}$$

The result then follows from the cochain relation

$$\left(f_v - \overline{\phi}_{v,M}\right) \cup \left(g_v - \overline{\psi}_{v,M^\vee}\right) = 0$$

and the orthogonality assumption

$$\text{inv}_v(\overline{\phi}_{v,M} \cup \overline{\psi}_{v,M^\vee}) = 0 \quad \text{for all } \; v \in S.$$

□

Proof of Proposition 4.2 (3). From part (2), it suffices to prove the statement for the left kernel. The claim then splits into the following two subclaims:

- Suppose ϕ lies in $\text{Sel}\,(M_2, (\pi_*(W_v))_v)$. Then ϕ can be written as $\pi_*(\phi')$ for some $\phi' \in H^1(G_{F,S}, M)$ if and only if $\text{CTP}(\phi,\psi) = 0$ for all

$$\psi \in Ш_1(M_1^\vee) = \ker\left(H^1(G_{F,S}, M_1^\vee) \to \prod_{v\in S} H^1(G_v, M_1^\vee) \right).$$

- If ϕ obeys the requirements of the first part, then it lies in $\pi_*\left(\text{Sel}(M, (W_v)_v)\right)$ if and only if $\text{CTP}(\phi,\psi) = 0$ for all ψ in $\text{Sel}\left(M_1^\vee,\ \left(\iota_*^\vee(W_v^\perp)\right)_v\right)$.

To prove the first claim, we note that the map $\phi \mapsto df$ induces the final map of the sequence (4.2). Therefore, our goal is to show that

$$\text{CTP}(\phi, \psi) = \text{PTP}(df, \psi) \quad \text{for } \psi \in Ш_1(M_1^\vee), \tag{4.6}$$

where PTP is the standard Poitou-Tate pairing of $Ш_2(M_2)$ and $Ш_1(M_1^\vee)$. To see this, we recall the construction of the latter pairing from Tate's paper [51]: given $f_{\text{Ta}} \in Z^2(G_{F,S}, M_1)$ representing a class of $Ш_2(M_1)$, and given $f'_{\text{Ta}} \in Z^1(G_{F,S}, M_1^\vee)$ representing a class of $Ш_1(M_1^\vee)$, we define

$$\text{PTP}(f_{\text{Ta}}, f'_{\text{Ta}}) = \sum_{v \in S} \text{inv}_v \left(g_{\text{Ta},v} \cup f'_{\text{Ta},v} - h_{\text{Ta},v} \right),$$

where $g_{\text{Ta},v} \in C^1(G_v, M_1)$ is chosen so $dg_{\text{Ta},v} = f_{\text{Ta},v}$, and where $h_{\text{Ta}} \in C^2(G_{F,S}, \mathcal{O}_{F,S}^\times)$ is chosen so

$$dh_{\text{Ta}} = f_{\text{Ta}} \cup f'_{\text{Ta}}.$$

Take $(\overline{\psi},\ \overline{\phi},\ f,\ (\overline{\phi}_{v,M})_v,\ \epsilon)$ to be a tuple for computing $\text{CTP}(\phi, \psi)$. Then (4.6) can be verified from the dictionary

$$f_{\text{Ta}} = df, \quad f'_{\text{Ta}} = \overline{\psi}, \quad g_{\text{Ta},v} = f_v - \overline{\psi}_{v,M}, \quad h_{\text{Ta}} = \epsilon.$$

This establishes the first claim.

To establish the second, suppose $\overline{\phi}$ can be written in the form $\pi_*(\overline{\phi'})$. We then can write

$$\text{CTP}(\phi, \psi) = \sum_{v \in S} \text{inv}_v \left(\left(\overline{\phi'}_v - \overline{\phi}_{v,M} \right) \cup \overline{\psi}_v \right).$$

From the construction in the snake lemma, the map

$$\phi \mapsto \left(\overline{\phi'}_v - \overline{\phi}_{v,M} \right)_{v \in S}$$

induces the final map of (4.3). The result then follows from Poitou-Tate duality. □

The following naturality property follows from the definition.

Proposition 4.5. *Fix a global field F and set of places S as in Notation 4.1, and suppose*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\iota_M} & M & \xrightarrow{\pi_M} & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_2} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{\iota_N} & N & \xrightarrow{\pi_N} & N_2 & \longrightarrow & 0 \end{array}$$

is a commutative diagram with exact rows in the category of finite $G_{F,S}$-modules. Choose a set of local conditions $(W_{v,M})_{v\in S}$ for N, and choose a set of local conditions $(W_{v,N})_{v\in S}$ for N so that

$$W_{v,N} \subseteq f_*(W_{v,M}) \quad \textit{for all } v \in S.$$

We assume M and N and these local conditions obey the requirements of Notation 4.1.

Then, for

$$\phi \in \text{Sel}\left(M_2,\, (\pi_{M*}(W_{v,M}))_v\right) \quad \textit{and} \quad \psi \in \text{Sel}\left(N_1^\vee,\, \left(\iota_{N*}^\vee(W_{v,N}^\perp)\right)_v\right),$$

we have

$$\text{CTP}_{\iota_M,\pi_M}\left(\phi,\, f_{1\,*}^\vee(\psi)\right) \,=\, \text{CTP}_{\iota_N,\,\pi_N}\left(f_{2*}(\phi), \psi\right).$$

4.1. **Antisymmetry.** The second part of Proposition 4.2 generalizes a result of Flach on the antisymmetry of the Cassels-Tate pairing [8, Theorem 2]. In a general context, suppose we have chosen F, S, M, and $(W_v)_{v\in S}$ as in Notation 4.1, and choose a $G_{F,S}$-submodule M_1 of M. Choose a $G_{F,S}$-equivariant homomorphism $f : M \to M^\vee$ so that

$$f_*(W_v) \subseteq W_v^\perp \;\text{ for all } v \in S \quad \text{and } \; f(M_1) \subseteq M_1^\perp.$$

The map f then fits into the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{\iota} & M & \xrightarrow{\pi} & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_2} & & \\ 0 & \longrightarrow & M_2^\vee & \xrightarrow{\pi^\vee} & M^\vee & \xrightarrow{\iota^\vee} & M_1^\vee & \longrightarrow & 0 \end{array} \tag{4.7}$$

Under this circumstance, we can define a pairing

$$\text{CTP}_{\iota,\pi,f} : \text{Sel}\,(M_2,\,(\pi_*(W_v))_v) \times \text{Sel}\,(M_2,\,(\pi_*(W_v))_v) \to \mathbb{Q}/\mathbb{Z}$$

by

$$\text{CTP}_{\iota,\pi,f}(\phi,\psi) = \text{CTP}_{\iota,\pi}\,(\phi,\,f_{2*}(\psi))\,,$$

By Proposition 4.2 (2) and the naturality of the Cassels-Tate pairing, we have

$$\text{CTP}_{\iota,\pi}\,(\phi,\,f_{2*}(\psi)) \;=\; \text{CTP}_{\pi^\vee,\iota^\vee}\,(f_{2*}(\psi),\beta_*(\phi)) \;=\; \text{CTP}_{\iota,\pi}\,(\psi,\,{f_1^\vee}_*(\phi))\,.$$

In particular, if $f = f^\vee$, so that the associated pairing $M \times M \to {\mathcal{O}_{\mathcal{F},\mathcal{S}}}^\times$ is symmetric, then $\text{CTP}_{\iota,\pi,f}$ is also symmetric. Similarly, in the case where $f = -f^\vee$, the pairing on M is antisymmetric, and $\text{CTP}_{\iota,\pi,f}$ is also antisymmetric.

This theory is most interesting when f is an isomorphism satisfying

$$f_*(W_v) = W_v^\perp \;\text{ for all } v \in S \quad \text{and } \; f(M_1) = M_1^\perp. \tag{4.8}$$

In this case, f_* and f_{2*} give isomorphisms of Selmer groups, and $\text{CTP}_{\iota,\pi,f}$ has both kernels equal to $\pi_*(\text{Sel}(M,(W_v)_v))$.

In the anti-self dual case, we can follow the lead of [45] and ask if the antisymmetric pairing $\text{CTP}_{\iota,\pi,f}$ is alternating. If it is not, we can try to characterize its diagonal entries. There is still a terrific amount of work still to be done here, but the following partial answer suffices for our work.

Proposition 4.6. *Take F, S, and M as in 4.1, and fix k a positive integer. We assume that $M[2]$ is nonzero and that $2M[2^a] = M[2^{a-1}]$ for $k+2 \geq a \geq 1$. We also assume there is a $G_{F,S}$-equivariant anti-self dual map*

$$f_{k+2} : M[2^{k+2}] \to M[2^{k+2}]^\vee.$$

Finally, for $v \in S$, choose a subgroup W_v of $H^1(G_v, M[2^{k+1}])$.

We take

$$P_{k+2} : M[2^{k+2}] \otimes M[2^{k+2}] \to \mathcal{O}_{F,S}^{\times}$$

to be the pairing associated to f_{k+2}. From this pairing, we can apply the construction of Definition 3.1 to get the exact sequence

$$0 \to \mathcal{O}_{F,S}^{\times} \to \mathcal{H}_{2^{k+1},0,P_{k+2}}(M[2^{k+1}]) \to M[2^{k+1}] \to 0.$$

Taking q to be the connecting map associated to this sequence, we assume $q(W_v) = 0$ for $v \in S$.

Taking S_{good} to be the set of places $v \in S$ not dividing two where the action of G_v on $M[2]$ is unramified, we also assume

$$\ker\left(H^1(G_{F,S}, M[2]) \to \prod_{v \in S_{\text{good}}} H^1(G_v, M[2])\right) = 0.$$

Take $f_{k+1} : M[2^{k+1}] \xrightarrow{\sim} M[2^{k+1}]^{\vee}$ to be the map given by the restriction of $2^{\vee} \circ f_{k+2}$. Then, defining a Cassels-Tate pairing with respect to

$$0 \to M[2] \xrightarrow{\iota} M[2^{k+1}] \xrightarrow{2} M[2^k] \to 0,$$

we have

$$\text{CTP}_{\iota,2,f_{k+1}}(\phi, \phi) = 0 \quad \textit{for all} \quad \phi \in \text{Sel}\big(M[2^k],\, 2_*(W_v)_v\big).$$

Proof. In the context of Definition 3.1, given a subgroup $M[\lambda]$ and a pairing

$$P : M[\lambda] \times M[\lambda] \to \mathcal{O}_{F,S}^{\times},$$

we will refer to the corresponding module U as U_P.

For $a \leq k+2$, we can define a perfect pairing

$$P_a : M[2^a] \otimes M[2^a] \to \mathcal{O}_{F,S}^{\times}$$

so $P_a(2^{k+2-a}x, 2^{k+2-a}y) = 2^{k+2-a}P_{k+2}(x,y)$ for $x, y \in M[2^{k+2}]$. We have an exact sequence

$$0 \to \mathcal{O}_{F,S}^{\times} \to U_{P_1} \to M[2] \to 0 \tag{4.9}$$

of Galois modules, with U_{P_1} notably an abelian module. We claim this exact sequence splits as a sequence of $G_{F,S}$-modules. First, for H a closed subgroup of $G_{F,S}$, an Ext spectral sequence argument (per [36, Theorem 0.3]) together with the fact that

$$\mathrm{Ext}^1_{\mathbb{Z}}(M[2], \mathcal{O}_{F,S}^{\times}) = 0$$

gives an isomorphism

$$\mathrm{Ext}^1_{\mathbb{Z}[H]}(M[2], \mathcal{O}_{F,S}^{\times}) \cong H^1(H, M[2]^{\vee}) \cong H^1(H, M[2]).$$

Take c_H to be the image in $H^1(H, M[2])$ of the element of Ext^1 corresponding to (4.9). We then find that $c_{G_v} = 0$ for all $v \in S_{\text{good}}$. We will prove this by following the argument of [43, Proposition 3.6a]. First, we note that P_1 has range defined over ± 1, so we may alternatively consider the subsequence

$$0 \to \pm 1 \to U'_{P_1} \to M[2] \to 0. \tag{4.10}$$

We can verify that $2U'_{P_1}$ equals zero. We have a set-theoretic $G_{F,S}$ equivariant lift from $M[2]$ to U'_{P_1}, so we find

$$\dim H^0(G_v, \pm 1) + \dim H^0(G_v, M[2]) = \dim H^0(G_v, U'_{P_1}).$$

Since G_v acts cyclically on $M[2]$, and hence on U'_{P_1}, this gives

$$1 \quad + \quad \dim H^0(G_v, M[2]^{\vee}) = \dim H^0(G_v, (U'_{P_1})^{\vee}).$$

In particular we find that there is an element of $H^0(G_v, (U'_{P_1})^\vee)$ that projects to the identity map in $\mathrm{Hom}(\pm 1, \pm 1) = (\pm 1)^\vee$, since this is the unique nontrivial element of $(\pm 1)^\vee$. This element gives a section of (4.10) defined over G_v, so $c_{G_v} = 0$. From the assumptions of the proposition, we then get that $c_{G_{F,S}}$ is also zero.

Write $\cup_a$ for the cup product associated to P_a, and write q_a for the connecting map associated to the exact sequence

$$0 \to \mathcal{O}_{F,S}^\times \to \mathcal{H}_{2^a,0,P_{a+1}}(M[2^a]) \to M[2^a] \to 0.$$

Given ϕ in $\mathrm{Sel}\big(M[2^{k+1}],\, (W_v)_v\big)$, we can find $\phi' \in H^1(G_{F,S},\, M[2^{k+1}])$ that satisfies $2_*\phi' = \phi$ by the first claim in the proof of Proposition 4.2 (3). Choosing $\phi_{v,k+1} \in W_v$ that satisfies $2_*\phi_{v,k+1} = \phi_v$ for $v \in S$, we then get

$$\begin{aligned}
&\mathrm{CTP}_{\iota,2,f_{k+1}}(\phi,\phi) \\
&= \sum_{v\in S} \mathrm{inv}_v\left((\phi'_v - \phi_{v,k+1}) \cup_1 2_*^{k-1}\phi_v\right) = \sum_{v\in S} \mathrm{inv}_v\left((\phi'_v - \phi_{v,k+1}) \cup_{k+1} \phi_{v,k+1}\right) \\
&= \sum_{v\in S} \mathrm{inv}_v\left(-q_{k+1}(\phi'_v) + q_{k+1}(\phi'_v - \phi_{v,k+1}) + q_{k+1}(\phi_{v,k+1})\right) \quad \text{by Proposition 3.2} \\
&= \sum_{v\in S} \mathrm{inv}_v\left(q_{k+1}(\phi'_v - \phi_{v,k+1}) + q_{k+1}(\phi_{v,k+1})\right) \quad \text{by global Poitou-Tate duality} \\
&= \sum_{v\in S} \mathrm{inv}_v\left(q_{k+1}(\phi'_v - \phi_{v,k+1})\right) \quad \text{since } q(W_v) = 0 \\
&= \sum_{v\in S} \mathrm{inv}_v\left(2^k q_1(\phi'_v - \phi_{v,k+1})\right) = \sum_{v\in S} \mathrm{inv}_v\left(2^{k-1}(\phi'_v - \phi_{v,k+1}) \cup_1 (\phi'_v - \phi_{v,k+1})\right) \\
&= \sum_{v\in S} 2^{k-1}\mathrm{inv}_v\left((\phi'_v - \phi_{v,k+1}) \cup_1 c_{G_v}\right) = 0.
\end{aligned}$$

□

5. Appendix: Review of Galois cohomology

5.1. **Review of group cohomology.** We start by collecting the facts we will need about group cohomology. Our main reference is [41].

Take G to be a profinite group, and take M to be a topological G-module. We will always think of $H^1(G, M)$ as the set of continuous crossed homomorphisms from G to M modulo the set of coboundaries.

Group change. Per [41, 1.5], given a homomorphism of profinite groups $G_1 \to G$, a G_1-module M_1, and a homomorphism $M \to M_1$ that is G_1 equivariant with respect to the induced action of G_1 on M, there is a canonical homomorphism

$$H^k(G, M) \to H^k(G_1, M_1) \tag{5.1}$$

for any $k \geq 0$. This construction can be used to define restriction, inflation, and conjugation maps.

We consider the last case in more detail. If H is a closed subgroup of G, and τ lies in G, we have an induced map

$$\tau_* : H^k(H,\, M) \to H^k(\tau H \tau^{-1},\, M)$$

for all $k \geq 0$. If τ is in H, this map is the identity map. Given a crossed homomorphism ϕ representing an element of $H^1(G, M)$, we can give $\tau_*\phi$ the explicit representative

$$\tau_*\phi(\sigma) = \tau\phi(\tau^{-1}\sigma\tau).$$

Corestriction. Suppose H has finite index in G. Given an acyclic resolution

$$0 \to M \to M_0 \to M_1 \to \dots,$$

of M, we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M^H & \longrightarrow & M_0^H & \longrightarrow & M_1^H & \longrightarrow & \dots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M^G & \longrightarrow & M_0^G & \longrightarrow & M_1^G & \longrightarrow & \dots
\end{array}$$

where all the columns are given by the norm map. Taking homology of these complexes then gives the corestriction maps

$$\text{cor}_G^H : H^k(H, M) \to H^k(G, M).$$

We also get the more easily defined restriction maps

$$\text{res}_H^G : H^k(G, M) \to H^k(H, M),$$

which can be defined using the inclusion maps $M_i^H \hookrightarrow M_i^G$ at the level of complexes. This definition makes sense for any closed subgroup H of G.

Using the complexes, it is easy to check that

$$\text{cor}_G^H \circ \text{res}_H^G(\phi) = [G : H] \cdot \phi \tag{5.2}$$

for ϕ in $H^k(G, M)$. If H is normal in G, we also have

$$\text{res}_H^G \circ \text{cor}_G^H(\phi) = \sum_{\tau \in G/H} \tau_* \phi \tag{5.3}$$

for ϕ in $H^k(H, M)$.

This last equation is a special case of the double coset formula, which we quote from [41]. Take U to be a closed subgroup of G, and take H to be a finite index subgroup of G. Choose a set of representatives B of the double cosets

$$U \backslash G / H$$

Then, given ϕ in $H^k(H, M)$, we have

$$\text{res}_U^G \circ \text{cor}_G^H(\phi) = \sum_{\tau \in B} \text{cor}_U^{U \cap \tau H \tau^{-1}} \circ \tau_* \circ \text{res}^H_{\tau^{-1} U \tau \cap H}(\phi). \tag{5.4}$$

In particular, we have a commutative diagram

$$\begin{array}{ccccc} H^k(H,M) & \xrightarrow{\text{cor}} & H^k(G,M) & \xrightarrow{\text{res}} & H^k(H,M) \\ \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} \\ \bigoplus_{\tau\in B} H^k(H_\tau,M) & \xrightarrow{\bigoplus \text{cor}\circ\tau_*} & H^k(U,M) & \xrightarrow{\bigoplus(\tau^{-1})_*\circ\text{res}} & \bigoplus_{\tau\in B} H^k(H_\tau,M) \end{array} \tag{5.5}$$

for $k \geq 0$, where H_τ is defined as $H \cap \tau^{-1}U\tau$.

Shapiro's lemma. If N is an H-module, we can consider the induced module

$$\text{Ind}_G^H N = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N.$$

We have an isomorphism

$$N^H \cong \left(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N\right)^G$$

given by

$$n \longmapsto \sum_{\sigma\in G/H} [\sigma] \otimes n$$

for n in N^H. This isomorphism can be written as the composition

$$N^H \to \left(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N\right)^H \to \left(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N\right)^G,$$

where the first map sends n to $[1] \otimes n$, and the second map is the norm map. We can write the inverse of this map in the form

$$\left(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N\right)^G \hookrightarrow \left(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N\right)^H \to N^H,$$

where the second map gives the $[1]$ component.

If we apply this to an acyclic resolution of N, we derive Shapiro's lemma, that we have an isomorphism

$$H^k(H,N) \cong H^k\left(G, \text{Ind}_G^H N\right)$$

given in one direction as the composition

$$H^k(H,N) \to H^k\left(H, \mathrm{Ind}_G^H N\right) \xrightarrow{\text{cor}} H^k\left(G, \mathrm{Ind}_G^H N\right) \tag{5.6}$$

with the first map sending n to $[1] \otimes n$, and in the other as the composition

$$H^k\left(G, \mathrm{Ind}_G^H N\right) \xrightarrow{\text{res}} H^k(H, \mathrm{Ind}_G^H N) \to H^k(H,N) \tag{5.7}$$

with the second map sending an element of $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N$ to its $[1]$ component.

Using these compositions, we find that the bottom row of (5.5) induces an isomorphism

$$\bigoplus_{\tau \in B} H^k(H_\tau, M) \cong H^k\left(U, \mathrm{Ind}_G^H N\right), \tag{5.8}$$

where U is a closed subgroup of G, B is a set of representatives of $U\backslash G/H$, and H_τ denotes $H \cap \tau^{-1} U \tau$.

If N is a G-module and H is a normal subgroup of G, the conjugation maps defined above give an action of G/H on $H^k(H,N)$. Given $\tau \in G/H$, we can define an isomorphism

$$\rho_\tau : \mathrm{Ind}_G^H N \longrightarrow \mathrm{Ind}_G^H N \tag{5.9}$$

of G_F modules by

$$\rho_\tau([\sigma] \otimes x) = [\sigma\tau^{-1}] \otimes \tau x.$$

We then have a commutaive square

$$\begin{array}{ccc} H^k(H,N) & \xrightarrow{\tau_*} & H^k(H,N) \\ \downarrow & & \downarrow \\ H^k\left(G, \mathrm{Ind}_G^H N\right) & \xrightarrow{(\rho_\tau)_*} & H^k\left(G, \mathrm{Ind}_G^H N\right) \end{array}$$

with columns given by the Shapiro isomorphism.

Cup product. Given G-modules M_1 and M_2, we have the natural cup product map

$$\cup : H^k(G, M_1) \otimes H^j(G, M_2) \to H^{k+j}(G, M_1 \otimes M_2).$$

Take

$$t : M_1 \otimes M_2 \to M_2 \otimes M_1$$

to be the map taking $m_1 \otimes m_2$ to $m_2 \otimes m_1$ for all m_1 in M_1 and m_2 in M_2. Then, given $\phi_1 \in H^k(G, M_1)$ and $\phi_2 \in H^j(G, M_2)$, we have the skew-commutativity relation, that

$$\phi_2 \cup \phi_1 = (-1)^{k \cdot j} \cdot t_*(\phi_1 \cup \phi_2); \tag{5.10}$$

see [41, 1.4.4]. If we instead take $\phi_1 \in H^k(H, M_1)$, we have

$$\mathrm{cor}_G^H \left(\phi_1 \cup \mathrm{res}_H^G(\phi_2)\right) = \mathrm{cor}_G^H(\phi_1) \cup \phi_2 \quad \text{in} \quad H^{k+j}(G, M_1 \otimes M_2). \tag{5.11}$$

If we take ϕ_1 in $H^k(U, M_1)$ and ϕ_2 in $H^j(U, M_2)$, and if we take τ in G, we find

$$\tau_* \left(\phi_1 \cup \phi_2\right) = \tau_* \phi_1 \cup \tau_* \phi_2 \quad \text{in} \quad H^{k+j}\big(\tau U \tau^{-1}, M_1 \otimes M_2\big). \tag{5.12}$$

These are proved in [41, 1.5.3].

Procyclic corestriction. Suppose M is a $\widehat{\mathbb{Z}}$-module, and take a to be a positive integer. Choose m in M, and take ϕ to be the crossed homomorphism from $a \cdot \widehat{\mathbb{Z}}$ to M sending a to m. Then, under the corestriction map

$$\mathrm{cor} : H^1\big(a \cdot \widehat{Z},\, M\big) \longrightarrow H^1(\widehat{Z},\, M), \tag{5.13}$$

the class $\mathrm{cor}(\phi)$ is represented by a crossed homomorphism sending 1 to m. This can be proved directly from the effect of corestriction on cochains, as given in [41, 1.5].

5.2. **Local bookkeeping.** Take F to be a number field, and choose an algebraic closure $\overline{F}$ of F. Given a G_F module M of exponent dividing e_0, and given $k \geq 0$, we take $M(k)$ to

be the Galois module

$$M \otimes (\mu_{e_0})^{\otimes k}$$

and we take $M(-k)$ to be the Galois module

$$M \otimes \text{Hom}\left(\mu_{e_0},\ \tfrac{1}{e_0}\mathbb{Z}/\mathbb{Z}\right)^{\otimes k}.$$

These modules are isomorphic to the typical Tate twists of M, but such isomorphisms usually rely on some choice of isomorphism

$$\mu_{e_0} \xrightarrow{\sim} \tfrac{1}{e_0}\mathbb{Z}/\mathbb{Z}.$$

There is a canonical element of

$$\mu_{e_0} \otimes \text{Hom}\left(\mu_{e_0},\ \tfrac{1}{e_0}\mathbb{Z}/\mathbb{Z}\right).$$

If ζ is any generator of μ_{e_0}, this element is ζ tensored with the map sending ζ to $\frac{1}{e_0}$. We can define a natural canonical map

$$M \xrightarrow{\sim} M(-1)(1)$$

by tensoring with this element. For duals, we will use the notation

$$M^\vee = \text{Hom}(M, \mu_{e_0}).$$

Take $\mathfrak{p}$ to be a prime of F, write $G_\mathfrak{p}$ for the absolute Galois group of $F_\mathfrak{p}$, and write $I_\mathfrak{p}$ for the inertia subgroup of $G_\mathfrak{p}$. If N is a finite $G_\mathfrak{p}$ module, we have a perfect pairing

$$H^{2-i}\big(G_\mathfrak{p},\ N\big) \times H^i\big(G_\mathfrak{p},\ \text{Hom}(N, \overline{F}_\mathfrak{p}^\times)\big) \xrightarrow{\cup} H^2(G_\mathfrak{p}, \overline{F}_\mathfrak{p}^\times) \xrightarrow{\text{inv}} \mathbb{Q}/\mathbb{Z}$$

from local Tate duality for $i = 0, 1, 2$. If N is unramified at $\mathfrak{p}$ and $\mathfrak{p}$ does not divide the order of M, the case $i = 1$ restricts to a well-defined, non-degenerate pairing

$$\text{inv}_{\mathfrak{p}} : H^1\big(I_{\mathfrak{p}},\, N\big)^{G_{\mathfrak{p}}/I_{\mathfrak{p}}} \times H^1\big(G_{\mathfrak{p}}/I_{\mathfrak{p}},\, \text{Hom}(N, \overline{F}_{\mathfrak{p}}^{\times})\big) \to \mathbb{Q}/\mathbb{Z} \tag{5.14}$$

coming from the inflation-restriction sequence

$$0 \to H^1(G_{\mathfrak{p}}/I_{\mathfrak{p}},\, N) \to H^1(G_{\mathfrak{p}},\, N) \to H^1(I_{\mathfrak{p}},\, N)^{G_{\mathfrak{p}}/I_{\mathfrak{p}}} \to 0.$$

The final surjection of this last sequence follows from the fact that $G_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \widehat{Z}$ has cohomological dimension one, which implies that $H^2(G_{\mathfrak{p}}/I_{\mathfrak{p}},\, M)$ is zero.

Choose an inclusion

$$\iota : \overline{F} \hookrightarrow \overline{F}_{\mathfrak{p}}.$$

This induces an inclusion

$$\iota^* : G_{\mathfrak{p}} \hookrightarrow G_F.$$

The image $\iota^* G_{\mathfrak{p}}$ is the decomposition group of a unique prime $\overline{\mathfrak{p}}$ of $\overline{F}$. Given such an $\overline{\mathfrak{p}}$, we write $G_{F,\overline{\mathfrak{p}}}$ for its decomposition group in G_F. Consider the composition

$$\text{inv}_{\iota} : H^2(\iota^* G_{\mathfrak{p}}, \overline{F}^{\times}) \to H^2(G_{\mathfrak{p}}, \overline{F}_{\mathfrak{p}}^{\times}) \to \mathbb{Q}/\mathbb{Z},$$

where the first map is the group change homomorphism (5.1) corresponding to (ι, ι^*). Given a second inclusion ι_1, we can find some τ in G_F so $\iota_1 = \iota \circ \tau$. We then always have a commutative diagram

$$\begin{array}{ccc} H^2(G_{F,\overline{\mathfrak{p}}}, \overline{F}^{\times}) & & \\ \Big\downarrow{\scriptstyle \tau_*} & \searrow^{\text{inv}_{\iota}} & \\ H^2(G_{F,\tau\overline{\mathfrak{p}}}, \overline{F}^{\times}) & \xrightarrow{\text{inv}_{\iota_1}} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

In particular, if $G_{F,\overline{\mathfrak{p}}} = G_{F,\tau\overline{\mathfrak{p}}}$, we find that the maps inv_{ι} and inv_{ι_1} coincide. We thus have a well-defined map

$$H^{2-i}\big(G_{F,\overline{\mathfrak{p}}}, M\big) \times H^i\big(G_{F,\overline{\mathfrak{p}}}, M^{\vee}\big) \to \mathbb{Q}/\mathbb{Z}$$

depending only on the choice of $\overline{\mathfrak{p}}$ and not on the specific choice of ι for evaluating inv.

Definition 5.1. From this pairing, we get an isomorphism

$$H^2(G_{F,\overline{\mathfrak{p}}}, M) \xrightarrow{\sim} \text{Hom}\left(H^0\left(G_{F,\overline{\mathfrak{p}}}, M^\vee\right), \mathbb{Q}/\mathbb{Z}\right) \cong M(-1)_{G_{F,\overline{\mathfrak{p}}}}.$$

We then define a map

$$\text{inv}_{M,F,\overline{\mathfrak{p}}} : H^2(G_F, M) \longrightarrow M(-1)_{G_{F,\overline{\mathfrak{p}}}}$$

as the composition of this map with the restriction map.

Given an archimedean place v of F, and given an associated decomposition group $G_{F,\overline{v}}$ in G_F, we can extend this definition to give maps

$$\text{inv}_{M,F,\overline{v}} : H^2(G_F, M) \longrightarrow M(-1)_{G_{F,\overline{v}}}.$$

Definition 5.2. The Frobenius element is a canonical topological generator for $G_{\mathfrak{p}}/I_{\mathfrak{p}}$. Write $\text{Frob}_F\overline{\mathfrak{p}}$ for its image in $G_{F,\overline{\mathfrak{p}}}/I_{F,\overline{\mathfrak{p}}}$. For τ in G_F, we have

$$\text{Frob}_F\tau\overline{\mathfrak{p}} = \tau \circ \text{Frob}_F\,\overline{\mathfrak{p}} \circ \tau^{-1} \quad \text{in} \quad G_F/I_{F,\tau\overline{\mathfrak{p}}}. \tag{5.15}$$

If L/F is a finite extension, we also have

$$\text{Frob}_L\,\overline{\mathfrak{p}} = (\text{Frob}_F\,\overline{\mathfrak{p}})^m, \tag{5.16}$$

where m is the degree of the extension of residue fields corresponding to $L_{\overline{\mathfrak{p}}\cap L}/F_{\mathfrak{p}}$. In particular, if this extension is unramified at $\mathfrak{p}$, then m is just $[L_{\overline{\mathfrak{p}}\cap L} : F_{\mathfrak{p}}]$.

Evaluation at $\text{Frob}_F\overline{\mathfrak{p}}$ defines an isomorphism

$$\ker\left(H^1(G_{F,\overline{\mathfrak{p}}}, M) \to H^1(I_{F,\overline{\mathfrak{p}}}, M)\right) \longrightarrow \left(M^{I_{F,\overline{\mathfrak{p}}}}\right)_{G_{F,\overline{\mathfrak{p}}}}.$$

We define a map

$$\mathrm{fb}_{M,F,\overline{\mathfrak{p}}} : \ker\left(H^1(G_F, M) \to H^1(I_{F,\overline{\mathfrak{p}}}, M)\right) \longrightarrow \left(M^{I_{F,\overline{\mathfrak{p}}}}\right)_{G_{F,\overline{\mathfrak{p}}}}$$

as the composition of the restriction map with this isomorphism.

Assume that M is unramified at $\mathfrak{p}$ and that $\mathfrak{p}$ does not divide the order of M. From (5.14), we have an isomorphism

$$H^1(I_{F,\overline{\mathfrak{p}}}, M) \xrightarrow{\sim} \mathrm{Hom}\left(H^1(G_{F,\overline{\mathfrak{p}}}/I_{F,\overline{\mathfrak{p}}}, M^\vee), \mathbb{Q}/\mathbb{Z}\right) \xrightarrow{\sim} M(-1)^{G_{F,\overline{\mathfrak{p}}}}.$$

We write

$$\mathrm{fb}^*_{M,F,\overline{\mathfrak{p}}} : H^1(G_F, M) \longrightarrow M(-1)^{G_{F,\overline{\mathfrak{p}}}}$$

for the composition of this with the restriction map. Note that this definition is prone to sign errors coming from the skew commutativity of cup product.

For K a finite extension of F and τ in G_F, we have the commutative diagrams

$$\begin{array}{ccc} \ker\left(\mathrm{fb}^*_{M,K,\overline{\mathfrak{p}}}\right) & \xrightarrow{\mathrm{fb}_{M,K,\overline{\mathfrak{p}}}} & M_{G_{K,\overline{\mathfrak{p}}}} \\ \downarrow{\scriptstyle \tau_*} & & \downarrow{\scriptstyle \tau} \\ \ker\left(\mathrm{fb}^*_{M,\tau K,\tau\overline{\mathfrak{p}}}\right) & \xrightarrow{\mathrm{fb}_{M,\tau K,\tau\overline{\mathfrak{p}}}} & M_{G_{K,\tau\overline{\mathfrak{p}}}} \end{array} \quad , \quad \begin{array}{ccc} H^1(G_K, M) & \xrightarrow{\mathrm{fb}^*_{M,K,\overline{\mathfrak{p}}}} & M(-1)^{G_{K,\overline{\mathfrak{p}}}} \\ \downarrow{\scriptstyle \tau_*} & & \downarrow{\scriptstyle \tau} \\ H^1(G_{\tau K}, M) & \xrightarrow{\mathrm{fb}^*_{M,\tau K,\tau\overline{\mathfrak{p}}}} & M(-1)^{G_{K,\tau\overline{\mathfrak{p}}}} \end{array} \tag{5.17}$$

and

$$\begin{array}{ccc} H^2(G_K, M) & \xrightarrow{\mathrm{inv}_{M,K,\overline{\mathfrak{p}}}} & M(-1)_{G_{K,\overline{\mathfrak{p}}}} \\ \downarrow{\scriptstyle \tau_*} & & \downarrow{\scriptstyle \tau} \\ H^2(G_{\tau K}, M) & \xrightarrow{\mathrm{inv}_{M,\tau K,\tau\overline{\mathfrak{p}}}} & M(-1)_{G_{K,\tau\overline{\mathfrak{p}}}}. \end{array}$$

Finally, given a homomorphism $\rho : M \to N$ of G_F modules, we note that we have a commutative diagram

$$\begin{array}{ccc} H^2(G_F, M) & \xrightarrow{\mathrm{inv}_{M,F,\overline{\mathfrak{p}}}} & M(-1)_{G_{F,\overline{\mathfrak{p}}}} \\ \downarrow{\scriptstyle \rho_*} & & \downarrow{\scriptstyle \rho \otimes \mathrm{Id}} \\ H^2(G_F, N) & \xrightarrow{\mathrm{inv}_{N,K,\overline{\mathfrak{p}}}} & N(-1)_{G_{F,\overline{\mathfrak{p}}}}, \end{array} \tag{5.18}$$

and we can write down simlar diagrams for fb and fb^*.

Proposition 5.3. *Take F to be a number field and take M to be a finite G_F-module. Take $\mathfrak{p}$ to be a prime of F so that M is unramified at $\mathfrak{p}$ and so the order of M is indivisible by $\mathfrak{p}$. Take K/F to be a finite extension that is unramified at $\mathfrak{p}$. Take $\overline{\mathfrak{p}}$ to be a prime of $\overline{F}$ over $\mathfrak{p}$, and take B to be a subset of G_F so that*

$$\sigma \mapsto \sigma\overline{\mathfrak{p}} \cap K$$

gives a bijection between B and the set of primes of K dividing $\mathfrak{p}$.

The canonical restriction map $H^1(G_F, M) \to H^1(G_K, M)$ and corestriction map $H^1(G_K, M) \to H^1(G_F, M)$ then fit into a commutative diagram

$$\begin{array}{ccccc} \ker\left(\text{fb}^*_{M,F,\overline{\mathfrak{p}}}\right) & \xrightarrow{\text{res}} & \bigcap_{\tau\in B} \ker\left(\text{fb}^*_{M,K,\tau\overline{\mathfrak{p}}}\right) & \xrightarrow{\text{cor}} & \ker\left(\text{fb}^*_{M,F,\overline{\mathfrak{p}}}\right) \\ \downarrow{\scriptstyle \text{fb}_{F,\overline{\mathfrak{p}}}} & & \downarrow{\scriptstyle \oplus_\tau \text{fb}_{K,\tau\overline{\mathfrak{p}}}} & & \downarrow{\scriptstyle \text{fb}_{F,\overline{\mathfrak{p}}}} \\ M_{G_{F,\overline{\mathfrak{p}}}} & \longrightarrow & \bigoplus_{\tau\in B} M_{G_{K,\tau\overline{\mathfrak{p}}}} & \longrightarrow & M_{G_{K,\overline{\mathfrak{p}}}}, \end{array} \tag{5.19}$$

where the τ component of the first map in the second row is

$$m \;\mapsto\; \tau\left(1 + \text{Frob}_F\overline{\mathfrak{p}} + \cdots + (\text{Frob}_F\overline{\mathfrak{p}})^{[K_{K\cap\tau\overline{\mathfrak{p}}}:F_{\mathfrak{p}}]-1}\right) m$$

and the τ component of the second map is

$$m \;\mapsto\; \tau^{-1}m.$$

We also have a commutative diagram

$$\begin{array}{ccccc} H^2(G_F, M) & \xrightarrow{\text{res}} & H^2(G_K, M) & \xrightarrow{\text{cor}} & H^2(G_F, M) \\ \downarrow{\scriptstyle \text{inv}_{M,F,\overline{\mathfrak{p}}}} & & \downarrow{\scriptstyle \oplus_\tau \text{inv}_{M,K,\tau\overline{\mathfrak{p}}}} & & \downarrow{\scriptstyle \text{inv}_{M,F,\overline{\mathfrak{p}}}} \\ M(-1)_{G_{F,\overline{\mathfrak{p}}}} & \longrightarrow & \bigoplus_{\tau\in B} M(-1)_{G_{K,\tau\overline{\mathfrak{p}}}} & \longrightarrow & M(-1)_{G_{F,\overline{\mathfrak{p}}}} \end{array} \tag{5.20}$$

whose bottom row is as in (5.19)*.*

Finally, we have a commutative diagram

$$\begin{array}{ccccc} H^1(G_F, M) & \xrightarrow{\text{res}} & H^1(G_K, M) & \xrightarrow{\text{cor}} & H^1(G_F, M) \\ \downarrow{\scriptstyle \text{fb}^*_{F,\overline{\mathfrak{p}}}} & & \downarrow{\scriptstyle \oplus_\tau \text{fb}^*_{K,\tau\overline{\mathfrak{p}}}} & & \downarrow{\scriptstyle \text{fb}^*_{F,\overline{\mathfrak{p}}}} \\ M(-1)^{G_{F,\overline{\mathfrak{p}}}} & \longrightarrow & \bigoplus_{\tau\in B} M(-1)^{G_{K,\tau\overline{\mathfrak{p}}}} & \longrightarrow & M(-1)^{G_{F,\overline{\mathfrak{p}}}} \end{array}$$

where the τ component of the first map is

$$m \;\mapsto\; \tau m$$

and the τ component of the second map is

$$m \;\mapsto\; \left(1 + \text{Frob}_F\overline{\mathfrak{p}} + \cdots + (\text{Frob}_F\overline{\mathfrak{p}})^{[K_{K\cap\tau\overline{\mathfrak{p}}}:F_{\mathfrak{p}}]-1}\right)\tau^{-1}m.$$

Proof. The form of the restriction map for fb is a consequence of (5.16) and (5.17). For corestriction, we turn to the double coset formula (5.4). We see that B is a set of representatives of

$$G_K\backslash G_F/G_{F,\overline{\mathfrak{p}}}.$$

We then have

$$\text{res}^{G_F}_{G_{F,\overline{\mathfrak{p}}}} \circ \text{cor}^{G_K}_{G_F}(\phi) = \sum_{\tau\in B} \text{cor}^{G_{F,\overline{\mathfrak{p}}}\cap G_{\tau^{-1}K}}_{G_{F,\overline{\mathfrak{p}}}} \circ \tau_*^{-1} \circ \text{res}^{G_K}_{G_{F,\tau\overline{\mathfrak{p}}}\cap G_K}(\phi).$$

The group $G_{F,\overline{\mathfrak{p}}}/I_{F,\overline{\mathfrak{p}}}$ is procyclic, so we can calculate this using (5.13), the inflation-restriction sequence, and the fact that inflation commutes with corestriction.

If K/F is inert at $\mathfrak{p}$, we have

$$\text{inv}\left(\text{cor}^{G_{K,\overline{\mathfrak{p}}}}_{G_{F,\overline{\mathfrak{p}}}}(\gamma)\right) = \text{inv}(\gamma) \quad \text{for} \quad \gamma \in H^2(G_{K,\overline{\mathfrak{p}}}, \overline{F_{\mathfrak{p}}}^\times).$$

We can apply (5.11) in the form of the identity

$$\text{inv}\left(\phi \cup \text{res}^{G_{F,\tau\overline{\mathfrak{p}}}}_{G_{K,\tau\overline{\mathfrak{p}}}}(\psi)\right) = \text{inv}\left(\text{cor}^{G_{K,\tau\overline{\mathfrak{p}}}}_{G_{F,\tau\overline{\mathfrak{p}}}}(\phi) \cup \psi\right) \tag{5.21}$$

for $\phi \in H^2(G_{K,\tau\overline{\mathfrak{p}}}, M)$ and $\psi \in H^0(G_{F,\tau\overline{\mathfrak{p}}}, M^\vee)$. Together with (5.17) and the double coset formula, the compatibility of inv with corestriction follows. The compatibility with the restriction map comes from considering the same identity with ϕ in $H^0(G_{K,\tau\overline{\mathfrak{p}}}, M^\vee)$ and ψ in $H^2(G_{F,\tau\overline{\mathfrak{p}}}, M)$.

Applying (5.21) for ϕ in $H^1(G_{K,\tau\overline{\mathfrak{p}}}, M)$ and ψ unramified at $\mathfrak{p}$ in $H^1(G_{F,\tau\overline{\mathfrak{p}}}, M^\vee)$ gives the form of corestriction on fb^* as a consequence of the form of restriction on fb and the double coset formula. We can similarly find the form of restriction of fb^*. □

5.3. **Poitou-Tate duality.** We collect the parts of the nine term Poitou-Tate exact sequence we need; see [51, Theorem 3.1] and [41, 8.6.10]. Take F to be a number field, and take M to be any finite G_F-module. For any place v of F, choose a corresponding subgroup G_v of G_F; if the place is a finite prime $\mathfrak{p}$, this equals $G_{F,\overline{\mathfrak{p}}}$ for some choice of $\overline{\mathfrak{p}}$ over $\mathfrak{p}$.

- Note that, when composed with the natural projection

$$M_{G_{F,\overline{\mathfrak{p}}}} \to M_{G_F},$$

the maps $\text{inv}_{M,F,\overline{\mathfrak{p}}}$ do not depend on the choice of $\overline{\mathfrak{p}}$ over $\mathfrak{p}$. Given

$$\gamma \in H^2(G_F, M),$$

we have that

$$\sum_{v \text{ of } F} \text{inv}_{M,F,\overline{v}}(\gamma) = 0 \quad \text{in } M_{G_F}. \tag{5.22}$$

- Consider the pairing

$$\prod_{v \text{ of } F}{}' H^1(G_v, M) \times \prod_{v \text{ of } F}{}' H^1(G_v, M^\vee) \to \mathbb{Q}/\mathbb{Z}$$

given by

$$\left((\phi_v)_v, (\psi_v)_v\right) \mapsto \sum_v \text{inv}_v\left(\phi_v \cup \psi_v\right),$$

where $\prod'$ denotes the restricted product with respect to unramified cohomology.

Then this pairing is nondegenerate, and the image under the restriction map of $H^1(G_F, M)$ in the left product is precisely the anihilator of the image of $H^1(G_F, M^\vee)$ in the right product.

- In particular, take $\mathscr{V}$ to be a finite set of places of F containing all infinite places, all places dividing the order of M, and all places for which I_v has nontrivial action on M. Choose a subgroup

$$W \subseteq \prod_{v \in \mathscr{V}} H^1(G_v,\, M).$$

The above pairing then allows us to define a surjection

$$\prod_{v \in \mathscr{V}} H^1(G_v,\, M^\vee) \longrightarrow \text{Hom}(W, \mathbb{Q}/\mathbb{Z}),$$

and this then gives a non-degenerate pairing

$$\ker\left(\frac{H^1(G_F,\, M)}{Ш_1(F, M)} \longrightarrow \frac{\bigoplus_{v \in \mathscr{V}} H^1(G_v, M)}{W} \times \bigoplus_{v \notin \mathscr{V}} H^1(I_v,\, M)^{G_v/I_v}\right)$$
$$\times\ \text{cok}\left(H^1(G_F,\, M^\vee) \longrightarrow \text{Hom}(W, \mathbb{Q}/\mathbb{Z}) \times \bigoplus_{v \notin \mathscr{V}} H^1(I_v,\, M^\vee)^{G_v/I_v}\right) \to \mathbb{Q}/\mathbb{Z}.$$

Part 2. Bilinear character sums

6. Main results for bilinear character sums

In this section, we give a general bilinear character sum estimate. Our starting point is the following result of Jutila [21, Lemma 3]: there is some absolute constant $C > 0$ so that, for any $N_1, N_2 \geq 3$, and for any sequence of complex coefficients a_d indexed by integers of magnitude at most one, we have

$$\sum_{\substack{0<e<N_1 \\ e \text{ odd, squarefree}}} \left| \sum_{\substack{|d|<N_2 \\ d \text{ squarefree}}} a_d \left(\frac{d}{e}\right) \right| \leq C \cdot \left(N_1 \cdot N_2^{\frac{1}{2}} + N_1^{\frac{3}{4}} \cdot N_2 \cdot \log^3 N_2\right), \tag{6.1}$$

where $\left(\frac{d}{e}\right)$ denotes the Jacobi symbol, the bimultiplicative generalization of the standard Legendre symbol. This bilinear estimate fits into the theory of large sieve inequalities, with the standard reference being [19, Chapter 7].

Jutila's result has been sharpened and generalized substantially since it first appeared. Thanks to work of Heath-Brown [17], the exponents on N_1 and N_2 on the right side of (6.1) can be lowered to within ϵ of the optimal values. Bilinear estimates of more general characters have also been found. Goldmakher and Louvel [14] directly extended Heath-Brown's work to quadratic Hecke families, which are certain collections of order-two Hecke characters defined over a general number field F. Follow-up work generalized this to higher-order characters [3].

In parallel, Friedlander et al. found that estimates of bilinear sums of characters over number fields could be combined with estimates of short character sums to find the spin distribution of prime ideals in that number field [10, Proposition 5.1]. As part of this program, several bilinear character sum estimates have been derived over the last few years, with a particularly streamlined form of the argument given in [29, Proposition 3.6].

The result we give in this section is an adaptation of the argument in [10] to our more general framework. Usually, such estimates do not make the dependence on the underlying fields (in our case, the field extension K/F) explicit. In our case, making this dependence explicit is worthwhile, as this stronger form of the result has an application to our work in later sections.

This section is largely self-contained, though we will make use of Notation 2.2 and Propositions 2.4 and 2.13.

Notation 6.1. Take K/F to be a Galois extension of number fields, and fix an integer $e_0 \geq 2$. We assume K contains μ_{e_0}.

For any set of places $\mathscr{V}$ of F, take $K(\mathscr{V})$ to be the maximal abelian extension of K of exponent dividing e_0 ramified only at places over $\mathscr{V}$.

Write Δ_K for the magnitude of the discriminant of K, write $n_{K/F}$ for the degree of K/F, and write n_F for the degree of $F/\mathbb{Q}$. Take n_K to be the degree of K over $\mathbb{Q}$.

Given a number field L and an ideal $\mathfrak{a}$ of L, we will denote the rational norm of $\mathfrak{a}$ by $N_L(\mathfrak{a})$.

Definition 6.2. Given a set of places $\mathscr{V}_0$ of F and a prime $\mathfrak{p}$ of F outside $\mathscr{V}_0$, a *tempered function* will be a real-valued class function

$$\phi : \text{Gal}\left(K(\mathscr{V}_0 \cup \{\mathfrak{p}\})/F\right) \to [-1, 1]$$

so that ϕ has zero mean value on cosets of

$$\text{Gal}\left(K(\mathscr{V}_0 \cup \{\mathfrak{p}\})/K(\mathscr{V}_0)\right).$$

Given a function tempered $\phi_\mathfrak{p}$ for $(\mathfrak{p}, \mathscr{V}_0)$ and another prime $\mathfrak{q}$ of F, we define

$$\phi_\mathfrak{p}(\mathfrak{q}) = \begin{cases} 0 & \text{if } \mathfrak{q} \in \mathscr{V}_0 \cup \{\mathfrak{p}\} \text{ or } \mathfrak{p}|\Delta \\ \phi_\mathfrak{p}(\text{Frob}\,\mathfrak{q}) & \text{otherwise.} \end{cases}$$

Theorem 6.3. *There is some absolute constant $C > 0$ so we have the following:*

Take K/F, e_0, Δ_K, n_K, n_F, and $n_{K/F}$ as in Notation 6.1. Take $\mathscr{V}_0$ to be a set of places obeying the conditions of Notation 2.2. For each prime $\mathfrak{p}$ of F outside $\mathscr{V}_0$, take $\phi_\mathfrak{p}$ to be a tempered function for $(\mathfrak{p}, \mathscr{V}_0)$.

Then, given $N_1, N_2 > 1$, we have

$$\sum_{\substack{\mathfrak{p} \notin \mathscr{V}_0 \\ N_1 \leq N_F(\mathfrak{p}) \leq 2N_1}} \left| \sum_{\substack{\mathfrak{q} \notin \mathscr{V}_0 \\ N_2 \leq N_F(\mathfrak{q}) \leq 2N_2}} \phi_\mathfrak{q}(\mathfrak{p}) \right| \leq A \cdot N_1 \cdot N_2 \cdot \left(N_1^{-\alpha} + N_2^{-\alpha}\right) \tag{6.2}$$

with

$$A = \left(e_0^{|\mathscr{V}_0|} \cdot \log 2\Delta_K\right)^{C \cdot n_K} \cdot \Delta_K^C$$

and

$$\alpha = \begin{cases} 1/4 & \textit{if } n_{K/F} = 1 \\ 1/(3n_{K/F}+2) & \textit{if } n_{K/F} \textit{ is even} \\ 1/(3n_{K/F}+3) & \textit{otherwise.} \end{cases}$$

Remark 6.4. If $\mathscr{V}_0$ does not obey the conditions of Notation 2.2, we can add at most

$$C \cdot \log \Delta_K$$

places to it so it does, per the proof of Proposition 2.4.

We will adopt some notation of Weiss.

Definition 6.5 ([54])**.** Given a number field L and a nonzero integral ideal $\mathfrak{b}$ of L, take $I(\mathfrak{b})$ to be the set of ideals of L coprime to $\mathfrak{b}$ and take $P(\mathfrak{b})$ to be the set of principal ideals represented by a totally positive element equal to 1 mod $\mathfrak{b}$. A Dirichlet character mod $\mathfrak{b}$ will then be a homomorphism from $I(\mathfrak{b})/P(\mathfrak{b})$ to $\mathbb{C}^\times$.

Example 6.6. Suppose we are in the situation of Notation 2.2. Choose primes $\overline{\mathfrak{q}}, \overline{\mathfrak{p}}_0$ outside $\mathscr{V}_0$, and take L to be the subfield of K on which $\mathrm{Frob}_F \overline{\mathfrak{p}}_0$ acts trivially. Take k to be the minimal positive integer so

$$a^{\mathrm{nc}}(\overline{\mathfrak{p}}_0, \overline{\mathfrak{q}})^k$$

is a single root of unity, as opposed to a class of many roots of unity.

Then there is some Dirichlet character χ of L mod $\overline{\mathfrak{q}} \cap L$ and some complex constant c so that, for any prime $\overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0$ not over $\overline{\mathfrak{q}} \cap L$ or any prime of $\mathscr{V}_0$, we have

$$a^{\mathrm{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{q}})^k = c \cdot \chi(\overline{\mathfrak{p}} \cap L)$$

The above theorem will follow as a consequence of the following proposition.

Proposition 6.7. *There is some absolute $C > 0$ so we have the following:*

Take L to be a number field of degree n_L and of discriminant with magnitude Δ_L. Take F to be a subfield of L of degree n_F. For each prime $\mathfrak{p}$ of F , choose some nontrivial Dirichlet character $\chi_\mathfrak{p}$ of L mod $\mathfrak{p} \cdot \mathcal{O}_L$ and some complex constant $c_\mathfrak{p}$ of magnitude at most one. Then, for $N_1, N_2 > 1$, we have

$$\sum_{N_1 \leq N_L(\mathfrak{a}) \leq 2N_1} \left| \sum_{N_2 \leq N_F(\mathfrak{p}) \leq 2N_2} c_\mathfrak{p} \cdot \chi_\mathfrak{p}(\mathfrak{a}) \right|^2 \leq N_1 \cdot N_2 \cdot (C \cdot \log 2\Delta_L)^{n_L} + e^{C \cdot n_L} \cdot \Delta_L^{3/4} \cdot N_2^{2+\frac{3}{2} n_{L/F}}.$$

Here, the inner sum is over primes of F, and the outer sum is over integral ideals of L.

We will prove this by a smoothing argument. A previous version of our argument used a fairly complicated smoothing, producing a slightly larger α for $n_{K/F} > 1$. These improvements will not make our final result stronger, so we wil instead use as smoothing considered by Weiss. We would like to thank Jesse Thorner for pointing out the relevance of [54].

Proof. In [54, Section 3], Weiss chooses an absolute constant A, defines a function

$$\eta_1 : \mathbb{R} \to \mathbb{R} \quad \text{by} \quad \eta_1(x) = \begin{cases} \frac{1}{2}A & \text{if } |x| < A^{-1} \\ \frac{1}{4}A & \text{if } |x| = A^{-1} \\ 0 & \text{otherwise,} \end{cases}$$

and takes η_k to be the k^{th} convolution power of η_1. The functions $\eta_k(x)$ are symmetric and satisfy $\eta_k(x) \leq \eta_k(y)$ for $0 \leq y \leq x$, as can be proved inductively. The central limit theorem then gives that there is some absolute $c > 0$ so that, for $k \geq 1$, we have

$$\eta_k(x) \geq c \cdot k^{-1/2} \quad \text{for all } x \in [-c, c].$$

Weiss then defines $H_k(x)$ to be $\eta_k(\log x)$ for positive x.

From these estimates, [54, Lemma 3.4] implies there is some absolute $C > 0$ and some function

$$h : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$$

that is at least one on $[1/2, 1]$ so that, for any $y \geq 1$, any squarefree integral ideal $\mathfrak{b}$ of F, and any nontrivial Dirichlet character χ defined mod $\mathfrak{b}$, we have

$$\sum_{\mathfrak{a}} h\left(\frac{y}{N_L(\mathfrak{a})}\right)\chi(\mathfrak{a}) \;\leq\; \exp(Cn_L)\cdot 2^{\omega(\mathfrak{b})}\cdot \Delta_L^{3/4}\cdot N_L(\mathfrak{b})^{3/4} \quad \text{and}$$

$$\sum_{\mathfrak{a}} h\left(\frac{y}{N_L(\mathfrak{a})}\right) \;\leq\; \exp(Cn_L)\cdot \kappa(L)\cdot y \;+\; \exp(Cn_L)\cdot 2^{\omega(\mathfrak{b})}\cdot \Delta_L^{3/4}\cdot N_L(\mathfrak{b})^{3/4}.$$

Here, $\kappa(L)$ is defined to be the residue of the Dedekind zeta function for L at $s = 1$. From [33], we have the bound

$$\kappa(L) < (C\cdot \log 2\Delta_L)^{n_L}$$

for some absolute $C > 0$. Now, we can bound the expression of the Proposition by

$$\begin{aligned}
&\sum_{\mathfrak{a}} h\left(\frac{N_1}{N_L(\mathfrak{a})}\right)\left|\sum_{N_2\leq N_F(\mathfrak{p})\leq 2N_2} c_{\mathfrak{p}}\cdot\chi_{\mathfrak{p}}(\mathfrak{a})\right|^2 \\
&\quad\leq \sum_{N_2\leq N_F(\mathfrak{p}_1),N_F(\mathfrak{p}_2)\leq 2N_2}\left|\sum_{N_1\leq N_L(\mathfrak{a})\leq 2N_1} h\left(\frac{N_1}{N_L(\mathfrak{a})}\right)\chi_{\mathfrak{p}_1}(\mathfrak{a})\cdot\overline{\chi_{\mathfrak{p}_2}(\mathfrak{a})}\right| \\
&\quad\leq\; N_2\cdot N_1\cdot(C\cdot\log 2\Delta_L)^{n_L} \;+\; \exp(C\cdot n_L)\cdot\Delta_L^{3/4}\cdot N_2^{2+\frac{3n_L}{2n_F}},
\end{aligned}$$

where the first term in the sum comes from the diagonal terms and the second comes from the off-diagonal terms and the error term of the diagonal terms. This gives the theorem. □

We will need the following simple degree estimate for extensions of local fields.

Proposition 6.8. *Take p to be a prime number and take K_p to be a finite extension of $\mathbb{Q}_p$. Take r so the residue field of K_p has p^r elements. Take e_1 to be a positive integer indivisible by p, take s to be a nonnegative integer, and define e_0 to be $e_1 p^s$. Then, if L_p/K_p is an abelian extension of exponent dividing e_0, the inertia subgroup of* $\mathrm{Gal}(L_p/K_p)$ *has order*

dividing

$$e_0 \cdot p^{3rs}.$$

Proof. From local class field theory, we can write the inertia subgroup of L_p/K_p as a quotient of

$$\mathcal{O}_{K_p}^{\times}/(\mathcal{O}_{K_p}^{\times})^{e_0},$$

so we need only prove that $e_0 p^{3rs}$ is an upper bound on the size of this group. Taking k_p to be the residue field of K_p, we know that $k_p^{\times}/(k_p^{\times})^{e_0}$ has order dividing e_0. Now suppose a is an element of $\mathcal{O}_{K_p}^{\times}$ that maps to one in k_p. Hensel's lemma implies that

$$x^{e_0} - a = 0$$

has a solution for x in $\mathcal{O}_{K_p}$ if

$$a \equiv 1 \mod p^{3s};$$

see [7, Theorem 7.3], for example. This gives the proposition. □

From this result, we find that

$$[K(\mathscr{V}_0) : K(\emptyset)] \leq e_0^{n_{K/F}(3n_F + |\mathscr{V}_0|)}.$$

The degree of $K(\emptyset)$ over K is bounded by the size of the class group of K, which is bounded by

$$C \cdot \Delta_K^{1/2} \cdot (\log 2\Delta_K)^{n_K}$$

for some absolute C. This can be found by combining the upper bound of [33] with the lower bounds on regulators in [11]. We then get that

$$[K(\mathscr{V}_0) : F] \leq e_0^{Cn_K} \cdot \Delta_K^{1/2} \cdot (\log 2\Delta_K)^{n_K} \cdot e_0^{|\mathscr{V}_0| \cdot n_{K/F}}, \tag{6.3}$$

7. Proof of Theorem 6.3

For $N_1, N_2 > 1$, take $S_0(\mathscr{V}_0, N_1, N_2)$ to be the maximum value attained by the sum (6.2) over all sequences of tempered functions. Given a prime $\mathfrak{p}$ of F, $\overline{\mathfrak{p}}$ will be some fixed prime over $\mathfrak{p}$ in $\overline{F}$.

Take $S_1(\mathscr{V}_0, N_1, N_2)$ to be the maximal value of the sum

$$\sum_{\substack{N_1 \le N_F(\mathfrak{p}) \le 2N_1 \\ \overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0}} \left| \sum_{\substack{N_2 \le N_F(\mathfrak{q}) \le 2N_2 \\ \overline{\mathfrak{q}} \sim \overline{\mathfrak{q}}_0}} \phi_{\mathfrak{q}}(\mathfrak{p}) \right|$$

over all choices of primes $\overline{\mathfrak{p}}_0, \overline{\mathfrak{q}}_0$ outside $\mathscr{V}_0$ and not ramifying in K/F and over all choices of sequences of tempered function $\phi_{\mathfrak{q}}$. We have

$$S_0(\mathscr{V}_0, N_1, N_2) \;\le\; [K(\mathscr{V}_0) : F]^2 \cdot S_1(\mathscr{V}_0, N_1, N_2). \tag{7.1}$$

From (6.3), this implies

$$S_0(\mathscr{V}_0, N_1, N_2) \;\le\; e_0^{C \cdot |\mathscr{V}_0| \cdot n_K} \cdot \Delta_K \cdot (\log 2\Delta_K)^{n_K} \cdot S_1(\mathscr{V}_0, N_1, N_2).$$

Next, from Proposition 2.13 and using the fact that $\mathscr{V}_0$ obeys the conditions of Notation 2.2, we see that, if $\overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0$ and $\overline{\mathfrak{q}} \sim \overline{\mathfrak{q}}_0$, and assuming $\mathfrak{p} \neq \mathfrak{q}$, we can write $\phi_{\mathfrak{q}}(\mathfrak{p})$ as a linear combination of the symbols

$$a(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}) = \prod_{\tau \in \mathrm{Gal}(K/F)} a^{\mathrm{nc}}(\overline{\mathfrak{p}}, \tau\overline{\mathfrak{q}})^{\kappa(\tau)}$$

where κ varies over functions from $\mathrm{Gal}(K/F)$ to $\mathbb{Z}/e_0\mathbb{Z}$ for which $a^{\mathrm{nc}}(\overline{\mathfrak{p}}, \tau\overline{\mathfrak{q}})^{\kappa(\tau)}$ is a well-defined root of unity for all τ.

If a is any function of this type, we see that the average value of

$$\phi(\mathfrak{p}, \mathfrak{q}) a(\overline{\mathfrak{p}}, \overline{\mathfrak{q}})^{-1}$$

as $\mathfrak{p}$ varies has magnitude at most one. This allows us to conclude that the coefficient of any individual a has magnitude at most one. In addition, since ϕ is tempered, the coefficient of the trivial symbol is zero.

If we then take $S_2(\mathscr{V}_0, N_1, N_2)$ to be the maximal value of the sum

$$\sum_{\substack{N_1 \leq N_F(\mathfrak{p}) \leq 2N_1 \\ \overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0}} \left| \sum_{\substack{N_2 \leq N_F(\mathfrak{q}) \leq 2N_2 \\ \overline{\mathfrak{q}} \sim \overline{\mathfrak{q}}_0}} c_{\mathfrak{q}} \cdot a(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}) \right|$$

over all $\overline{\mathfrak{p}}_0, \overline{\mathfrak{q}}_0$, all nontrivial symbols a as above, and all sequences $c_{\mathfrak{q}}$ of complex coefficients of magnitude bounded by one, we get

$$S_1(\mathscr{V}_0, N_1, N_2) \leq e_0^{n_{K/F}} \cdot S_2(\mathscr{V}_0, N_1, N_2). \tag{7.2}$$

We then get

$$S_0(\mathscr{V}_0, N_1, N_2) \leq e_0^{C|\mathscr{V}_0|n_K} \cdot \Delta_K \cdot (\log 2\Delta_K)^{n_K} \cdot S_2(\mathscr{V}_0, N_1, N_2)$$

for some absolute choice of $C > 0$. From reciprocity on the terms a^{nc}, we also have

$$S_2(\mathscr{V}_0, N_1, N_2) = S_2(\mathscr{V}_0, N_2, N_1). \tag{7.3}$$

Given a positive integer t, take $S_{2,t}(\mathscr{V}_0, N_1, N_2)$ to be the maximal value of

$$\sum_{\substack{N_1 \leq N_F(\mathfrak{p}) \leq 2N_1 \\ \overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0}} \left| \sum_{\substack{N_2 \leq N_F(\mathfrak{q}) \leq 2N_2 \\ \overline{\mathfrak{q}} \sim \overline{\mathfrak{q}}_0}} c_{\mathfrak{q}} \cdot a(\overline{\mathfrak{p}}, \overline{\mathfrak{q}}) \right|^t.$$

Hölder gives

$$S_2(\mathscr{V}_0, N_1, N_2) \leq (2n_F N_1)^{\frac{t-1}{t}} \cdot S_{2,t}(\mathscr{V}_0, N_1, N_2)^{\frac{1}{t}}. \tag{7.4}$$

Take $S_3(\mathscr{V}_0, N_1, N_2)$ to be the maximal value of

$$\sum_{N_2 \leq N_L(\mathfrak{a}) \leq 2N_2} \left| \sum_{\substack{N_1 \leq N_F(\mathfrak{p}) \leq 2N_1 \\ \overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0}} c_{\mathfrak{p}} \cdot \chi_{\mathfrak{p}}(\mathfrak{a}) \right|^2$$

over all choices of the field L intermediate to K/F, all choices of nontrivial Dirichlet characters $\chi_{\mathfrak{p}}$ mod $\mathfrak{p} \cdot \mathcal{O}_L$, and all choices of the complex constants $c_{\mathfrak{p}}$ of magnitude at most one. The above proposition then gives

$$S_3(\mathscr{V}_0, N_1, N_2) \leq N_2 \cdot N_1 \cdot (C \cdot \log 2\Delta_K)^{n_K} \ + \ \exp(C \cdot n_K) \cdot \Delta_K^{3/4} \cdot N_1^{2+\frac{3}{2}n_{K/F}}$$

Take L to be the minimal extension of F for which $L \cap \overline{\mathfrak{p}}_0$ is inert. Via Example 6.6, there is some choice of sequence of Dirichlet characters $\chi_{\mathfrak{p}}$ defined mod $\mathfrak{p} \cdot \mathcal{O}_L$ and coefficients $c'_{\mathfrak{p}}$ of magnitude at most one so that

$$S_{2,t}(\mathscr{V}_0, N_1, N_2) \ = \sum_{\substack{\overline{\mathfrak{q}}_1, \ldots, \overline{\mathfrak{q}}_t \sim \overline{\mathfrak{q}}_0 \\ N_2 \leq N_F(\mathfrak{q}_1), \ldots, N_F(\mathfrak{q}_t) \leq 2N_2}} \left| \sum_{\substack{N_1 \leq N_F(\mathfrak{p}) \leq 2N_1 \\ \overline{\mathfrak{p}} \sim \overline{\mathfrak{p}}_0}} c'_{\mathfrak{p}} \cdot \chi_{\mathfrak{p}} \left(\overline{\mathfrak{q}}_1 \ldots \overline{\mathfrak{q}}_t \cap L \right) \right|.$$

Using Hölder a second time gives

$$S_{2,t}(\mathscr{V}_0, N_1, N_2) \ \leq \ (2N_2 n_F)^{t/2} \cdot \left(t! \cdot \sum_{k=0}^{t} S_3(\mathscr{V}_0, N_1, 2^k N_2^t) \right)^{1/2}.$$

Assuming $1 \leq t \leq 10 n_{K/F}$, we then have

$$S_{2,t}(\mathscr{V}_0, N_1, N_2) \leq (e_0 \cdot n_K)^{C \cdot n_K} \cdot (C \cdot \log 2\Delta_K)^{n_K/2} \cdot \Delta_K^{3/8} \cdot \left(N_2^t \cdot N_1^{1/2} \ + \ N_2^{t/2} \cdot N_1^{1+\frac{3}{4}n_{K/F}} \right).$$

Still assuming $1 \leq t \leq 10 n_{K/F}$, we have

$$S_2(\mathscr{V}_0, N_1, N_2) \ \leq \ \Delta_K^{\frac{3}{8}} \cdot (e_0 \cdot n_K \cdot \log 2\Delta)^{C \cdot n_F} \cdot N_1 \cdot N_2 \cdot \left(N_1^{-\frac{1}{2t}} + N_1^{\frac{1}{t} \cdot \frac{3}{4} n_{K/F}} \cdot N_2^{-\frac{1}{t} \cdot \frac{t}{2}} \right).$$

Using reciprocity to assume $N_2 \geq N_1$, the optimal choice of t is

$$t = \begin{cases} 2 & \text{if } n_{K/F} = 1 \\ \lceil 3n_{K/F} + 1 \rceil & \text{otherwise.} \end{cases}$$

With this, the theorem follows. □

Part 3. **The Base Case I: Linear Algebra**

8. TWISTABLE MODULES AND SELMER GROUPS

With current methods, it is far easier to control the distribution of 2-Selmer groups in quadratic twist families than the ℓ-Selmer group for any $\ell > 2$. Admirable progress has been made in other cases using methods from the geometry of numbers (see e.g. [2]), but determining the distribution of higher Selmer groups is largely an intractable problem.

The exception at 2 is a consequence of the fact that $+1$ and -1 are equal in fields of characteristic two but not in fields of any other characteristic. Because of this, if F is a number field, χ a homomorphism $G_F \to \pm 1$, and N a G_F module, when we define a quadratic twist N^χ and an isomorphism

$$\beta_\chi : N^\chi \xrightarrow{\sim} N$$

of abelian groups so that

$$\beta_\chi(\sigma n) = \chi(\sigma)\sigma\beta_\chi(n) \quad \text{for } \sigma \in G_F, n \in N^\chi,$$

we find that β_χ induces an isomoprhism

$$N^\chi[2] \cong N[2] \tag{8.1}$$

of G_F-modules. In particular, as χ varies, the 2-Selmer group of N^χ can be seen as a subgroup of the fixed ambient space

$$H^1(G_F, N[2])$$

for all χ. To find the distribution of 2-Selmer groups, we just need to understand how the portion of this space cut out by local conditions changes as the local conditions themselves change.

This can be generalized to twist families of higher degree. In general, for degree ℓ^k-twists, we can prove base case Selmer results about a portion of the ℓ-Selmer groups. We turn to the notation we need now.

Notation 8.1. Throughout this part, K/F will denote a fixed Galois extension of number fields, and ℓ^k will be a fixed power of a rational prime ℓ. We assume K contains μ_{ℓ^k}.

In addition, we will take $\mathscr{V}_0$ to be a set of places of F. We assume this set of places is large enough that the conditions of Notation 2.2 are satisfied for $(K/F, \ell^k, \mathscr{V}_0)$. In particular, we assume it contains all archimedean places and all places over ℓ.

$\mathbb{F}$ will denote a cyclic $\mathrm{Gal}(K/F)$-module of order ℓ^k.

Definition 8.2. Given Notation 8.1, a *twistable module* will consist of the following:

- A topological group N isomorphic to some finite power of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$,
- A continuous action of the absolute Galois group G_F of F on N that is ramified only at the places in $\mathscr{V}_0$, and
- An embedding of $\mathbb{F}$ into the group of continuous automorphisms of N so that the conjugation action of G_F on the automorphism group agrees with the action of G_F on $\mathbb{F}$. We assume that a generator ζ of $\mathbb{F}$ satisfies

$$(1 + \zeta^{\ell^{k-1}} + \zeta^{2\ell^{k-1}} + \cdots + \zeta^{(\ell-1)\ell^{k-1}})N = 0$$

Writing ω for the ideal generated by $(\zeta - 1)$ in $\mathbb{Z}[\mathbb{F}]$, we will assume that G_K has trivial action on $N[\omega^2]$.

Definition 8.3. Given $\chi \in H^1(G_F, \mathbb{F})$, the twist N^χ of N will be a topological group isomorphic to N under a non-equivariant isomorphism

$$\beta_\chi : N^\chi \xrightarrow{\sim} N$$

so that, for all $n \in N^\chi$ and $\sigma \in G_F$, we have

$$\beta_\chi(\sigma n) = \chi(\sigma)\sigma\beta_\chi(n).$$

We note that β_χ restricts to a G_F-equivariant isomorphism

$$N^\chi[\omega] \cong N[\omega],$$

generalizing (8.1).

We define the set of admissible twists

$$\mathbb{X}_F \subseteq H^1(G_F, \mathbb{F})$$

to be the set of χ so that, for all primes $\mathfrak{p}$ of F outside $\mathscr{V}_0$, χ is ramified at $\mathfrak{p}$ only if the image of χ under the natural map

$$H^1(G_F, \mathbb{F}) \to H^1(G_F, \mathbb{F}/\ell\,\mathbb{F}).$$

is ramified at $\mathfrak{p}$. If ζ has order ℓ, this set of twists is all of $H^1(G_F, \mathbb{F})$.

We represent the ramification of an element χ of $\mathbb{X}_F$ using the squarefree ideal

$$\mathfrak{h}_F(\chi) = \prod_{\substack{\mathfrak{p} \notin \mathscr{V}_0 \\ \chi \text{ is ramified at } \mathfrak{p}}} \mathfrak{p}.$$

There are many possible ways to order these ideals. Writing $N_{F/\mathbb{Q}}$ for the norm from F to $\mathbb{Q}$, we settle for the function

$$h_F(\chi) = N_{F/\mathbb{Q}}(\mathfrak{h}_F(\chi)).$$

Taking

$$\mathbb{F}(-1) = \text{Hom}(\mu_{\ell^k}, \mathbb{F}),$$

and taking $F(\mathbb{F}(-1))$ to be the minimal extension of F so $G_{F(\mathbb{F}(-1))}$ acts trivially on $\mathbb{F}(-1)$, we note that all primes dividing $\mathfrak{h}_F(\chi)$ split completely in $F(\mathbb{F}(-1))/F$ if χ is in $\mathbb{X}_F$.

For $H > 0$, we write $\mathbb{X}_F(H)$ for the subset of $\mathbb{X}_F$ of twists of height at most H.

A choice of *local twists* indexed by $\mathscr{V}_0$ will be a tuple $(\chi_v)_{v\in\mathscr{V}_0}$, where χ_v is chosen from from $H^1(G_v, \mathbb{F})$. Given a choice of local twists, we write $\mathbb{X}_F((\chi_v)_v)$ for the subset of $\mathbb{X}_F$ whose restriction to G_v gives χ_v for v in $\mathscr{V}_0$, and we take $\mathbb{X}_F(H, (\chi_v)_v)$ to be the set of twists in this set of height at most H.

Example 8.4. In the most important case of $\mathbb{F} = \pm 1$, we have

$$\mathbb{X}_F = H^1(G_F, \pm 1) \cong F^\times/(F^\times)^2.$$

In this setting, the height of d in $F^\times/(F^\times)^2$ is the product of the rational norms of all primes of F outside $\mathscr{V}_0$ where $F(\sqrt{d})/F$ ramifies.

In the specific case of $F = \mathbb{Q}$, we can represent any element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ by a square-free integer

$$d_0 \cdot p_1 \dots p_r,$$

where d_0 is divisible only by the primes in $\mathscr{V}_0$ and the $p_1 \dots p_r$ are distinct primes not in $\mathscr{V}_0$. The height of this twist is then $p_1 \dots p_r$.

In this context, a choice of local twists is equivalent to a choice of d_0, a choice of the value of $p_1 \dots p_r$ mod 8, and a choice of whether $p_1 \dots p_r$ is a quadratic residue or not at the odd primes in $\mathscr{V}_0$.

Definition 8.5. For each $v \in \mathscr{V}_0$ and each χ_v in $H^1(G_v, \mathbb{F})$, fix an ℓ-divisible $\mathbb{Z}[\mathbb{F}]$-submodule $W_v(\chi_v)$ of $H^1(G_v, N)$.

Now suppose χ is an element of $\mathbb{X}_F$. For each place v of F outside $\mathscr{V}_0$, define a subgroup $W_v(\chi)$ of $H^1(G_{F_v}, N)$ as follows:

- If χ ramifies at v, take
$$W_v(\chi) = 0.$$
- If χ does not ramify at v, take
$$W_v(\chi) = \mathrm{im}\Big(H^1(G_v/I_v, N) \to H^1(G_v, N)\Big).$$

We then define the Selmer group $\mathrm{Sel}(N^\chi,\ (W_v)_{v\in\mathscr{V}_0})$ by

$$\mathrm{Sel}(N^\chi,\ (W_v)_v)\ =\ \ker\left(H^1(G_F, N^\chi)\ \longrightarrow\ \prod_{v \text{ of } F}\frac{H^1(G_v, N^\chi)}{W_v(\chi)}\right),$$

and we supress the $(W_v)_v$ in this notation if it is clear what local conditions we are using (or if they do not matter).

For $m \geq 1$, we define the ω^m-Selmer group $\mathrm{Sel}^{\omega^m}(N^\chi,\ (W_v)_v)$ to be the subgroup of $H^1(G_F, N[\omega^m])$ mapping to $\mathrm{Sel}(N^\chi,\ (W_v)_v)$ under the natural map to $H^1(G_F, N^\chi)$.

Example 8.6. Given a topological group N isomorphic to some power of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, and given a continuous G_F-action on N that is ramified only over the set of places $\mathscr{V}_0$, we can define a twistable module $N \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell[\zeta]$, where ζ denotes a primitive ℓ^{th} root of unity. The geometry of this module and its generalizations is fairly well understood (see [34]). If L/F is a Galois degree ℓ-extension, if $\chi : \mathrm{Gal}(L/F) \to \langle\zeta\rangle$ is a nontrivial homomorphism, and if A is an abelian variety over F, we find that $(A \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell[\zeta])^\chi$ can be given the structure of an abelian variety A^χ over F of dimension $(\ell - 1)\dim A$, and that we always have

$$\mathrm{rank}(A/L) = \mathrm{rank}(A/F) + \mathrm{rank}\,(A^\chi/F)\,.$$

There are similar compatibilities between L-functions of A and its twists [35].

In this case, the limit of the standard ℓ^k-Selmer groups of A^χ can be written in the form

$$\text{Sel}\left((A^\chi[\ell^\infty]),\ (W_v)_v\right),$$

where

$$W_v = \ker\left(H^1(G_v, A^\chi[\ell^\infty]) \to H^1(G_v, A^\chi)\right) \quad \text{for } v \in \mathscr{V}_0.$$

Remark 8.7. In the next proposition, we will find that a certain portion of the ℓ^∞-Selmer group of a degree ℓ Galois extension of number fields can be written as the Selmer group of a twistable module. We hope to extend this to find statistics of the algebraic K-groups $K_{2i}\mathcal{O}_L$ as L varies through a similar family, giving evidence for the Cohen-Lenstra-esque conjectures of [20]. These objects are related to Selmer groups defined from Tate twists $\mathbb{Q}_\ell/\mathbb{Z}_\ell(m)$ [53], but the precise nature of their relationship will need to wait for future work.

Proposition 8.8. *Take L/F to be a degree ℓ Galois extension of number fields, and take χ to be a nontrivial homomorphism from* $\text{Gal}(K/F)$ *to $\mathbb{Z}[\zeta]$, where ζ denotes a primitive ℓ^{th} root of unity. Take*

$$\text{Cl}^\vee L = \text{Hom}\left(\text{Cl}\, L,\ \mathbb{Q}/\mathbb{Z}\right).$$

Take $N = \mathbb{Q}_\ell/\mathbb{Z}_\ell[\zeta]$ to be a twistable module with a trivial G_F action and with ζ acting via multiplication. For v a place of F, take

$$W_v = \begin{cases} H^1(G_v/I_v, N^\chi) & \text{if } L/F \text{ is unramified at } v \\ 0 & \text{otherwise.} \end{cases}$$

We assume that

$$\ker\left(H^1(G_F, \mu_\ell) \to \prod_{\substack{v \text{ of } F,\, v\nmid \ell\infty \\ v \text{ ram. in } L/F}} H^1(G_v, \mu_\ell) \times \prod_{\substack{v \text{ of } F,\, v\nmid \ell\infty \\ v \text{ unr. in } L/F}} H^1(I_v, \mu_\ell)\right) \tag{8.2}$$

is zero.

Then we have an exact sequence

$$0 \to (\mathrm{Cl}^\vee L[\ell^\infty])^{\mathrm{Gal}(L/F)} \to \mathrm{Cl}^\vee L[\ell^\infty] \to \mathrm{Sel}(N^\chi, (W_v)_v) \to 0$$

of $\mathrm{Gal}(L/F)$*-modules.*

Proof. Write $G = \mathrm{Gal}(L/F)$. From Shapiro's lemma, and specifically (5.8), we have an isomorphism

$$\mathrm{Cl}^\vee L[\ell^\infty] \cong \ker\left(H^1(G_F, N_0) \to \prod_{v \text{ of } F} \frac{H^1(G_v, N_0)}{H^1(G_v/I_v, N_0^{I_v})}\right),$$

of $\mathrm{Gal}(L/F)$ modules, where $N_0 = \mathbb{Q}_\ell/\mathbb{Z}_\ell[G]$. Choosing a generator σ of G, we have a map

$$N_0 \xrightarrow{(\sigma-1)} (\sigma-1)N_0 \cong N^\chi.$$

Call this composition π. We calculate

$$\pi_*\left(H^1\left(G_v/I_v,\, N_0^{I_v}\right)\right) = W_v$$

for all v in F. From (5.9), we have an exact sequence

$$0 \to \mathrm{Cl}^\vee L[\ell^\infty]^{\mathrm{Gal}(L/F)} \to \mathrm{Cl}^\vee L[\ell^\infty] \to \ker\left(H^1(G_F, N^\chi) \to \prod_{v \text{ of } F} \frac{H^1(G_v, N^\chi)}{\pi_*(H^1(G_v/I_v, N_0^{I_v}))}\right).$$

We then just need to prove this last sequence is surjective on the right.

To this end, we recall that we have a surjection

$$N_0 \xrightarrow{\text{Norm}} \mathbb{Q}_\ell/\mathbb{Z}_\ell$$

given by adding the coefficients of each $[\sigma^j]$. We then have an exact sequence

$$0 \to \mathbb{F}_\ell \xrightarrow{\iota} N_0 \xrightarrow{\pi \oplus \text{Norm}} \mathbb{Q}_\ell/\mathbb{Z}_\ell \oplus N^\chi \to 0.$$

For v not dividing ℓ or ∞, we get

$$(\iota_*)^{-1}(H^1(G_v/I_v, N_0^{I_v})) = \begin{cases} H^1(G_v/I_v, \mathbb{F}_\ell) & \text{if } L/F \text{ is unramified at } v \\ H^1(G_v, \mathbb{F}_\ell) & \text{otherwise.} \end{cases}$$

Surjectivity then follows as a consequence of the Cassels-Tate pairing and the assumption that (8.2) is zero. □

8.1. **Tamagawa ratios.** We wish to understand the distribution of the Selmer groups $\text{Sel}^\omega(N^\chi)$ as χ varies. As was observed in [24], the average size of these groups can tend to infinity as the number of prime divisors of $\mathfrak{h}_F(\chi)$ grows, with the authors showing this tendency for quadratic twists of elliptic curves over $\mathbb{Q}$ with one nonzero rational 2-torsion point. This is part of a general trend that necessitates us defining *Tamagawa ratios*.

Definition 8.9. Take T to be a G_F-submodule of $N[\omega]$. Given $\chi \in \mathbb{X}_F$, we define the Tamagawa ratio $\mathcal{T}_{N,T}(\chi)$ by

$$\mathcal{T}_{N,T}(\chi) = \prod_{\mathfrak{p} | \mathfrak{h}_F(\chi)} \frac{\#H^0(G_{F_\mathfrak{p}},\, N/T[\omega])}{\#H^0(G_{F_\mathfrak{p}},\, N[\omega])}.$$

Proposition 8.10. *Given $(K/F, \mathscr{V}_0, \mathbb{F})$ as in Notation 8.1, there is some $C > 0$ so we have the following:*

Suppose N is a twistable module defined with respect to $(K/F, \mathscr{V}_0, \mathbb{F})$. Given a G_F-submodule T of $N[\omega]$, take

$$\iota_{T,*} : H^1(G_F, T) \longrightarrow H^1(G_F, N[\omega])$$

to be the map coming from the inclusion of T in $N[\omega]$. Then, for χ in $\mathbb{X}_F$, we have

$$\left|\iota_{T,*}^{-1}\big(\text{Sel}^\omega(N^\chi)\big)\right| \;\geq\; \mathcal{T}_{N,T}(\chi) \cdot \left(\prod_{v \in \mathscr{V}_0} \#H^1(G_v, T)\right)^{-1} \tag{8.3}$$

Proof. Take $\mathscr{V}_1$ to be the set of primes of F dividing $\mathfrak{h}$. The space on the left hand side of (8.3) is at least as large as

$$\ker\left(\mathscr{S}_{T/F}(\mathscr{V}_0 \cup \mathscr{V}_1) \to \prod_{v\in\mathscr{V}_0} H^1(G_v, T) \times \prod_{v\in\mathscr{V}_1} H^1(G_v, N^\chi)\right). \tag{8.4}$$

For v in $\mathscr{V}_1$, we have an exact sequence

$$\begin{aligned} 0 \to H^0(G_v, T) \to H^0(G_v, N^\chi) \to H^0(G_v, N^\chi/T) \\ \to H^1(G_v, T) \to H^1(G_v, N^\chi). \end{aligned}$$

Writing U_v for the image of $H^1(G_v, T)$ in $H^1(G_v, N^\chi)$, we then find that

$$\#U_v = \frac{\#H^1(G_v, T)\cdot\#H^0(G_v, N[\omega])}{\#H^0(G_v, T)\cdot\#H^0(G_v, N/T[\omega])} = \#H^0(G_v, T(-1))\cdot\frac{\#H^0(G_v, N[\omega]}{\#H^0(G_v, N/T[\omega])}.$$

To prove the second equality, we note that the set of invariants $H^0(G_v, T)$ has the same size as the set of coinvariants $H^1(G_v/I_v, T)$ since G_v/I_v is procyclic.

We also have

$$\#\mathscr{S}_{T/F}(\mathscr{V}_0 \cup \mathscr{V}_1) \geq \prod_{v\in\mathscr{V}_1} H^0(G_v, T(-1))$$

by the unpacking hypothesis. We then get the proposition by comparing the size of the domain and image of the map in (8.4). □

In particular, we always have the lower bound

$$|\text{Sel}^\omega(N^\chi)| \;\geq\; c\cdot\max{}_T\mathcal{T}_{N,T}(\chi)$$

for the size of the Selmer group of N^χ, where the maximum is taken over all G_F-submodules of $N[\omega]$ and where c depends just on N.

This bound tends to be fairly sharp, in the sense of the next theorem.

Theorem 8.11. *Given $(K/F, \mathscr{V}_0, \mathbb{F})$ as in Notation 8.1, there is some $c, C > 0$ so we have the following:*

Suppose N is a twistable module of corank $g > 0$ defined with respect to $(K/F, \mathscr{V}_0, \mathbb{F})$. Then, for $H > 30$ a positive real number satisfying

$$g \leq c \cdot \log\log\log H,$$

we have

$$\sum_{\substack{\chi \in \mathbb{X}_F \\ h(\chi) \leq H}} \frac{\#\text{Sel}^{\omega}(N^{\chi})}{\max_T \mathcal{T}_{N,T}(\chi)} \leq \exp\left(Cg^2\right) \cdot \sum_{\substack{\chi \in \mathbb{X}_F \\ h(\chi) \leq H}} 1. \tag{8.5}$$

We will prove this theorem in Section 14.2.

Remark 8.12. We can rewrite Theorem 8.11 to give effective bounds on C that explicitly depend on K/F, $\mathscr{V}_0$, and $\mathbb{F}$. We have no particular use for this sensitivity in our applications, so we have opted for the easier form above and in the remaining theorems of this section.

On the other hand, we have a use for sensitivity in g. One of our main goals is to find the probability that $\text{Sel}^{\omega}(N^{\chi})$ has a certain rank as χ varies through a family. We will find this probability by computing the average size of

$$\text{Sel}^{\omega}(N^{\oplus m})^{\chi}$$

over this family, where m varies in some interval $\{0, \ldots, s\}$. In order for the error bounds on this rank distribution to decrease as H increases, we need to allow s to grow as some unbounded function in H. This forces us to keep track of the effect of g.

8.2. **Dual modules and base-case Selmer groups.** Fix a twistable module N defined with respect to $(K/F, \mathscr{V}_0, \mathbb{F})$. In this section, we will consider dual twistable modules.

Definition 8.13. The topological group

$$W = \text{Hom}\left(N, \mu_{\ell^{\infty}}\right).$$

has a G_F action defined by

$$t \mapsto \sigma\phi(\sigma^{-1}t) \quad \text{for } \sigma \in G_F.$$

We can also definie an action of $\mathbb{F}$ on W by

$$(\zeta\phi)(t) = \phi(\zeta^{-1}t).$$

Writing ζ^σ for the image of ζ under σ in $\mathbb{F}$, we can calculate

$$\sigma(\zeta(\phi)) = \zeta^\sigma(\sigma(\phi))$$

using the fact that the action of G_F on $\mathbb{F}$ agrees with the conjugation action of G_F on End N. The module W is a free $\mathbb{Z}_\ell$ module.

We define a corresponding torsion module by

$$N^\vee = (W \otimes \mathbb{Q}_\ell)/W. \tag{8.6}$$

The action of $\mathbb{F}$ on W extends to an obvious action on $W \otimes \mathbb{Q}_\ell$, and subsequently to an action on $N^\vee$. We then have that $N^\vee$ is a twistable module with respect to the $K/F, \mathbb{F}, \mathscr{V}_0$.

We will also need to consider the module

$$N' = N^\vee \big/ (N^\vee[\ell/\omega]).$$

If G_F acts trivially on $\mathbb{F}$, this module is isomorphic to N'.

We have a natural nondegenerate G_F-equivariant pairing

$$N[\omega] \times N'[\omega] \longrightarrow \mu_\ell. \tag{8.7}$$

We also have a natural map

$$N[\omega^2]/N[\omega] \otimes \mathbb{F}/\ell\,\mathbb{F} \xrightarrow{\sim} N[\omega]$$

given by $(x,\zeta)\mapsto(\zeta-1)x$. We will use this pairing in (8.9) below.

Notation 8.14. Take S to be a finite set. For $s\in S$, take $\mathfrak{p}_s$ to be a prime of F not over $\mathscr{V}_0$, and take $\overline{\mathfrak{p}}_s$ to be a prime of $\overline{F}$ over $\mathfrak{p}_s$. Any element of $H^1(G_F,\mathbb{F})/Ш_1(F,\mathbb{F})$ ramified only at $\mathscr{V}_0$ and the primes $\mathfrak{p}_s$ can be uniquely written in the form

$$\chi=\chi_0+\sum_{s\in S}\mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_s}(x_s), \tag{8.8}$$

where the x_s lie in $\mathbb{F}(-1)^{G_{F,\overline{\mathfrak{p}}_s}}$ and χ_0 lies in $\mathscr{S}_{\mathbb{F}/F}(\mathscr{V}_0)$. (We note that twisting by $Ш_1(F,\mathbb{F})$ does not affect local behavior, and hence has no effect on the structure on the ω-Selmer group of N^χ). For this twist to lie in $\mathbb{X}_F$, each x_s must either be zero or a generator of $\mathbb{F}(-1)$. In the former case, we can disregard $\mathfrak{p}_s$. So we assume the latter case, which forces us to assume

$$\big(\mathbb{F}(-1)\big)^{G_{F,\overline{\mathfrak{p}}_s}}\cong\mathbb{F}(-1)$$

for each $s\in S$. Write σ_s for the projection of $\mathrm{Frob}_F\overline{\mathfrak{p}}_s$ to the Galois group

$$G_1=\mathrm{Gal}\big(K(\mathscr{V}_0)/F(\mathbb{F}(-1))\big),$$

where $F(\mathbb{F}(-1))$ is the minimal extension of F for which $G_{F(\mathbb{F}(-1))}$ has trivial action on $\mathbb{F}(-1)$, and where $K(\mathscr{V}_0)$ is the maximal abelian extension of K of exponent dividing ℓ^k ramified only over $\mathscr{V}_0$.

The ω-Selmer group of N^χ evidently contains $Ш_1(F,N[\omega])$. Modulo this group, the Selmer group of N^χ with χ in the above form is a subgroup of

$$\mathscr{S}_{N[\omega]/F}\big(\mathscr{V}_0\cup\{\mathfrak{p}_s\ :\ s\in S\}\big),$$

and any element in this set can uniquely be written in the form

$$\phi=\phi_0+\sum_{s\in S}\mathfrak{B}^{\mathrm{nc}}_{N[\omega],F,\overline{\mathfrak{p}}_s}(q_s\cup_{\mathbb{F}}x_s), \tag{8.9}$$

where q_s is an element of $(N[\omega^2]/N[\omega])^{\sigma_s}$ and ϕ_0 lies in $\mathscr{S}_{N[\omega]/F}(\mathscr{V}_0)$.

Take

$$\delta'_\chi \in \text{Ext}^1_{G_F}(N'[\omega^2]/N'[\omega],\ N'[\omega])$$

to be the class of the extension

$$0 \to N'[\omega] \to (N')^\chi[\omega^2] \to N'[\omega^2]/N'[\omega] \to 0.$$

Taking the notation

$$\mathscr{R} = \bigoplus_{s\in S} H^0\left(\langle\sigma_s\rangle,\ N'[\omega^2]/N'[\omega]\right),$$

we then define a bilinear pairing

$$\langle\ ,\ \rangle_\chi : H^1(G_F, M) \otimes \mathscr{R} \longrightarrow \tfrac{1}{\ell}\mathbb{Z}/\mathbb{Z} \tag{8.10}$$

by

$$(\phi,\ (r_s)_s) \longmapsto \sum_{s\in S} \text{inv}_{\mu_\ell, F, \overline{\mathfrak{p}}_s}\left(\phi \cup \left(\text{res}_{G_{F,\overline{\mathfrak{p}}_s}} \delta'_\chi \cup r_s\right)\right),$$

where the outer product is the cup product from (8.7) and the inner is the Yoneda product.

Proposition 8.15. *Take all Selmer conditions as in Definition 8.5. Given ϕ in the form* (8.9) *and χ in the form* (8.8)*, and supposing ϕ obeys the local conditions at all places of $\mathscr{V}_0$, we find that*

$$\phi \in \text{Sel}^\omega N^\chi$$

if and only if

$$\langle\phi, (r_s)_s\rangle_\chi = 0 \quad \textit{for all } (r_s)_s \in \mathscr{R}.$$

We will prove this proposition in Section 10.2. Write

$$\mathscr{Q} = \bigoplus_{s\in S} H^0\left(\langle\sigma_s\rangle,\ N[\omega^2]/N[\omega]\right).$$

Via (8.9), we can think about the pairing defined above in the form

$$\langle\phi, (r_s)_s\rangle_\chi = \langle(q_s)_s,\ (r_s)_s\rangle_\chi + \langle\phi_0, (r_s)_s\rangle_{0,\chi}, \tag{8.11}$$

where the first pairing is defined on $\mathscr{Q} \otimes \mathscr{R}$, and the latter pairing is defined on $\mathscr{S}_{N[\omega]/F}(\mathscr{V}_0) \otimes \mathscr{R}$.

8.3. **Tuple sets of twists and moment estimates.** For fixed S and $(\sigma_s)_s$, we can choose a fixed basis for $\mathscr{Q}$, $\mathscr{R}$, and $\mathscr{S}_{N[\omega]/F}(\mathscr{V}_0)$, and consequently think about the pairings $\langle\ ,\ \rangle_\chi$ and $\langle\ ,\ \rangle_{0,\chi}$ as matrices that change with χ. To prove base-case Selmer results, we will need some kind of equidistribution statement about these matrices and their kernels.

More specifically, suppose $(x_s)_s$ is fixed in $\bigoplus_s \mathbb{F}(-1)$, and $(\sigma_s)_s$ is fixed as above. We will take X to be a nonempty set of tuples of primes

$$(\overline{\mathfrak{p}}_s)_{s\in S}, \quad \overline{\mathfrak{p}}_s \text{ a prime of } \overline{F} \text{ not over } \mathscr{V}_0 \text{ so that } \mathrm{Frob}_F \overline{\mathfrak{p}}_s = \sigma_s.$$

For each tuple $(\overline{\mathfrak{p}}_s)_s$ in X and each pair of distinct indices s_1, s_2 in S, we require $\overline{\mathfrak{p}}_{s_1}$ and $\overline{\mathfrak{p}}_{s_2}$ to be over distinct primes of F. Fixing χ_0, we then can consider the set of twists of the form (8.8), where $(\overline{\mathfrak{p}}_s)_s$ varies over the tuple set X. We will sometimes refer to this set of twists also with the symbol X.

Our main tool for proving rank distributions is to find estimates on sums of the form

$$\frac{1}{\#\mathscr{R}} \sum_{\chi\in X} \sum_{(q_s)_s\in\mathscr{Q}_1} \sum_{(r_s)_s\in\mathscr{R}} \exp\left(2\pi i \cdot \left(\left\langle \phi_0,\ (r_s)_s\right\rangle_\chi + \left\langle (q_s)_s,\ (r_s)_s\right\rangle_\chi\right)\right) \tag{8.12}$$

for certain subsets $\mathscr{Q}_1$ of $\mathscr{Q}$. It is most useful to this by fixing $((q_s)_s, (r_s)_s)$ and considering the sum

$$\sum_{\chi\in X} \langle (q_s)_s, (r_s)_s\rangle_\chi. \tag{8.13}$$

- In some cases, we can prove that (8.13) is negligible. In these circumstances, we will call $((q_s)_s, (r_s)_s)$ an *ignorable pair*.
- We can also find some subcollections of $\mathscr{Q}_1 \times \mathscr{R}$ where (8.13) has magnitude $\#X$ for any choice of $((q_s)_s, (r_s)_s)$, but there is substantial cancellation of these sums across the subcollection. In these case, we will call $((q_s)_s, (r_s)_s)$ a *cancellable pair*.

- In other cases, the choice of $((q_s)_s, (r_s)_s)$ may be from a subcollection of pairs where we have little control on the sums (8.13), where the size of the subcollection depends on $(\sigma_s)_s$ and is generically of negligible size. We will call these pairs *generically negligible*.
- Outside these cases, we find that (8.13) equals $\#X$. These give the *main-term pairs*, and estimating (8.12) amounts to counting the number of main-term pairs.

9. Favorable twists and the main theorems

Take K/F as in Notation 8.1, and take $G_0 = \mathrm{Gal}(K/F(\mathbb{F}(-1)))$. Recall the notation of Tamagawa ratios from Definition 8.9. Fix a twistable module N. We call a twist $\chi \in \mathbb{X}_F$ a *favored twist* of N if, for any G_F-submodule T of $N[\omega]$, we have

$$\mathcal{T}_{N,T}(\chi) \leq 1,$$

with equality if and only if

$$\dim H^0(\langle\sigma\rangle,\, N/T[\omega]) = \dim H^0(\langle\sigma\rangle,\, N[\omega]) \quad \text{for} \quad \sigma \in G_0. \tag{9.1}$$

We call T a *cofavored* submodule of $N[\omega]$ if (9.1) always holds. We will denote the set of favored twists of N by $\mathbb{X}^{\text{fav}}_{F,N}$, and those of height at most H by $\mathbb{X}^{\text{fav}}_{F,N}(H)$. Given local twists $(\chi_v)_{v\in\mathscr{V}_0}$, we define $\mathbb{X}^{\text{fav}}_{F,N}(H,\, (\chi_v)_v)$ as the subset of $\mathbb{X}^{\text{fav}}_{F,N}(H)$ restricting over $\mathscr{V}_0$ to $(\chi_v)_v$.

For favored twists, the Selmer group $\mathrm{Sel}^{\omega} N^{\chi}$ tends to be small, with its average size decomposing as a sum of terms indexed by cofavored modules. For this reason, we will restsrict our attention mostly to modules with a positive proportion of twists. The next definition is key.

Definition 9.1. Given a twistable module N as above, we call N *potentially favored* if

$$\lim_{H\to\infty} \frac{\#\mathbb{X}^{\text{fav}}_{F,N}(H)}{\#\mathbb{X}_F(H)} > 0.$$

Alternatively, we call N potentially favored if

- For any submodule T of $N[\omega]$ fixed by G_F, we have

$$\sum_{\sigma \in G_0} \dim H^0(\langle\sigma\rangle,\, N[\omega]) \geq \sum_{\sigma \in G_0} \dim H^0(\langle\sigma\rangle,\, (N/T)[\omega]),\ \text{and}$$

- There is some function

$$w : \text{Gal}(K/F(\mathbb{F}(-1))) \to \mathbb{R}$$

so that, for any submodule T of $N[\omega]$ fixed by G_F, we either have

$$\sum_{\sigma \in G_0} w(\sigma) \cdot \dim H^0(\langle\sigma\rangle,\, N[\omega]) > \sum_{\sigma \in G_0} w(\sigma) \cdot \dim H^0(\langle\sigma\rangle,\, (N/T)[\omega])$$

or

$$\dim H^0(\langle\sigma\rangle,\, N[\omega]) = \dim H^0(\langle\sigma\rangle,\, (N/T)[\omega]) \quad \text{for all } \sigma \in G_0.$$

We call the set of functions w that obey the second property the *superlatives* for N. N has a superlative if and only if it has a favored twist.

Remark 9.2. We will prove that these definitions are equivalent as part of Proposition 14.6.

Given an exact sequence

$$0 \to \mathbb{Z}^m \to \mathbb{Z}^n \to \mathbb{Z}^{n-m} \to 0,$$

we get an associated sequence of twistable modules

$$0 \to N^{\oplus m} \to N^{\oplus n} \to N^{\oplus n-m} \to 0$$

by tensoring with N. We call any such exact sequence a *basic exact sequence*.

I would like to thank David Yang for his help in finding the following proposition.

Proposition 9.3. *Suppose N_1 and N_2 are twistable modules. Then, if N_1 and N_2 are potentially favored, and if $w : G_0 \to \mathbb{R}^+$ is a superlative for both, then $N_1 \oplus N_2$ is potentially favored and has w as a superlative.*

Proof. Take N_1, N_2, and w as in the statement of the proposition, and take T to be a submodule of $N_1 \oplus N_2$. Taking the quotient of the exact sequence

$$0 \to N_1 \xrightarrow{\iota} N_1 \oplus N_2 \xrightarrow{\pi} N_2 \to 0$$

by T gives the exact sequence

$$0 \to N_1/\iota^{-1}(T) \to (N_1 \oplus N_2)/T \to N_2/\pi(T) \to 0.$$

The associated long exact sequence gives

$$\begin{aligned}&\dim H^0(\langle\sigma\rangle,\, (N_1 \oplus N_2)/T[\omega]) \\ &\qquad \le \dim H^0(\langle\sigma\rangle,\, N_1/\iota^{-1}(T)[\omega]) + \dim H^0(\langle\sigma\rangle,\, N_2/\pi(T)[\omega])\end{aligned}$$

for all σ in G_0. Then

$$\begin{aligned}&\sum_{\sigma\in G_0} w(\sigma)\cdot \dim H^0(\langle\sigma\rangle,\, (N_1 \oplus N_2)/T[\omega]) \\ &\le \sum_{\sigma\in G_0} w(\sigma)\cdot \dim H^0(\langle\sigma\rangle,\, N_1/\iota^{-1}(T)[\omega]) \;+\; \sum_{\sigma\in G_0} w(\sigma)\cdot \dim H^0(\langle\sigma\rangle,\, N_2/\pi(T)[\omega]) \\ &\le \sum_{\sigma\in G_0} w(\sigma)\cdot \dim H^0(\langle\sigma\rangle,\, N_1[\omega]) \;+\; \sum_{\sigma\in G_0} w(\sigma)\cdot \dim H^0(\langle\sigma\rangle,\, N_2[\omega]) \\ &= \sum_{\sigma\in G_0} w(\sigma)\cdot \dim H^0(\langle\sigma\rangle,\, (N_1 \oplus N_2)[\omega]).\end{aligned}$$

If the first and last entries in this sequence are equal, the positivity of w forces

$$\dim H^0(\langle\sigma\rangle,\, (N_1 \oplus N_2)/T[\omega]) = \dim H^0(\langle\sigma\rangle,\, (N_1 \oplus N_2)[\omega]) \quad \text{for } \sigma \in G_0.$$

So w is is a superlative for $N_1 \oplus N_2$. Applying this argument for the superlative $1+\epsilon w$ with ϵ approaching zero shows that $N_1 \oplus N_2$ is potentially favored, giving the proposition. $\square$

Remark 9.4. Given a twistable module N, a nonnegative integer a, and a G_F-submodule T of $N^{\oplus a}[\omega]$, we see that the logic of the above proposition gives that there is some sequence of G_F-submodules $T_1, \ldots, T_j$ of $N[\omega]$ and some sequence of nonnegative integers $a_1, \ldots, a_j$ with sum a so that

$$\dim H^0(\langle\sigma\rangle, N^{\oplus a}/T) \leq \sum_{i \leq j} a_i \cdot \dim H^0(\langle\sigma\rangle, N/T_i) \quad \text{for all } \sigma \in G_0.$$

This gives a useful upper bound for the function $\sigma \mapsto \dim H^0(\langle\sigma\rangle,\, N^{\oplus a}/T)$ in the case that T is not cofavored.

Given twistable modules N_1 and N_2, write δ_{σ,N_i} for the connecting map

$$\delta_{\sigma,N_i} : H^0(\langle\sigma\rangle, N_i[\omega^2]/N_i[\omega]) \to H^1(\langle\sigma\rangle, N_i[\omega])$$

coming from the exact sequence

$$0 \to N_i[\omega] \to N_i[\omega^2] \to N_i[\omega^2]/N_i[\omega] \to 0.$$

Given a G_F-equivariant map $\beta : N_1[\omega] \to N_2[\omega]$, we can lift β to an equivariant map

$$\overline{\beta} : N_1[\omega^2]/N_1[\omega] \longrightarrow N_2[\omega^2]/N_2[\omega]$$

via

$$\overline{\beta}(x) = \frac{1}{\zeta - 1}\beta((\zeta - 1)x).$$

We say β *commutes with the connecting maps* if we have

$$\delta_{\sigma,N_2} \circ \overline{\beta} = \beta_* \circ \delta_{\sigma,N_1} \quad \text{for } \sigma \in G_0. \tag{9.2}$$

Proposition 9.5. *Take N_1 and N_2 to be potentially favored modules sharing some superlative w. Suppose the only cofavored submodules of N_i are 0 and $N_i[\omega]$ for $i = 1, 2$. Then the cofavored submodules of $N_1 \oplus N_2$ are 0, $0 \oplus N_2[\omega]$, $(N_1 \oplus N_2)[\omega]$, and those modules of the form*

$$\{(x, \beta(x)) \ : \ x \in N_1[\omega]\}$$

where $\beta : N_1[\omega] \to N_2[\omega]$ runs over all the G_F-homomorphisms that commute with the connecting maps.

Proof. Choose a cofavored submodule T of $N_1 \oplus N_2$, and consider the standard exact sequence

$$0 \to N_2 \xrightarrow{\iota} N_1 \oplus N_2 \xrightarrow{\pi} N_1 \to 0.$$

From the argument of the previous proposition, we see that $\iota^{-1}(T)$ is cofavored in N_2 and $\pi(T)$ is cofavored in N_1. If $\iota^{-1}(T)$ is nonzero, it is $N_2[\omega]$, and we find that T is either $0 \oplus N_2[\omega]$ or $(N_1 \oplus N_2)[\omega]$. So we assume it is zero.

If $\pi(T)$ is also zero, T is zero, so we can assume $\pi(T)$ is $N_1[\omega]$. Then T is the graph of a map $\beta : N_1[\omega] \to N_2[\omega]$. This graph is a G_F-submodule if and only if β is linear and G_F-equivariant.

Following the logic of the previous proposition, we find that, since T is cofavored, the connecting map

$$H^0\big(\langle\sigma\rangle,\, N_1[\omega^2]/N_1[\omega]\big) \longrightarrow H^1\big(\langle\sigma\rangle,\, N_2[\omega]\big) \tag{9.3}$$

corresponding to the sequence

$$0 \to N_2[\omega] \to ((N_1 \oplus N_2)/T)[\omega] \to N_1[\omega^2]/N_1[\omega] \to 0$$

is zero for σ in G_0. To see this, take x in $N_1[\omega^2]/N_1[\omega]$ fixed by σ. Its preimage in $(N_1 \oplus N_2)/T[\omega]$ consists of all elements in the class of $(x, \overline{\beta}x)$. Applying $(\sigma - 1)$ to this

element yields the class

$$\sigma \mapsto (\sigma - 1)\overline{\beta}x - \beta(\sigma - 1)x,$$

which is trivial if and only if β commutes with the connecting map. So T is the graph of a function β that commutes with the connecting maps.

Conversely, we find that the graph of any G_F-homomorphism β that commutes with the connecting maps is cofavored in $N_1 \oplus N_2$, and we have the proposition. $\square$

Remark 9.6. In the context of the above proposition, we find that the kernel and image of any G_F-homomorphism that commutes with the connecting maps are cofavored. From the assumptions of the proposition, we find that the set of such homomorphisms consists of the zero map and isomorphisms.

In particular, the set of G_F endomorphisms of $N_1[\omega]$ that commute with connecting maps form a finite division ring, and hence a finite field of characteristic ℓ by Wedderburn's theorem. The set of G_F homomorphisms from $N_1[\omega]$ to $N_2[\omega]$ that commute with connecting maps is then either 0 or a one-dimensional vector space over this field.

Under some technical assumptions, we can now classify the cofavored submodules of modules of the form $N^{\oplus m}$. We will actually go a little further than this, proving the following proposition:

Proposition 9.7. *Take $N_1, \ldots, N_r$ to be potentially favored modules sharing some superlative. Suppose we have the following:*

- *For $i \leq r$, the only cofavored submodules of N_i are 0 and $N[\omega]$.*
- *For $i \leq r$, the only G_F-automorphisms of $N_i[\omega]$ that commute with the connecting maps are $0, 1, \ldots, \ell - 1$.*
- *For $i, j \leq r$ with $i \neq j$, there is no G_F-isomorphism of $N_i[\omega]$ and $N_j[\omega]$ that commutes with the connecting maps.*

Then, for $a_1, \ldots, a_r$ nonnegative integers, the cofavored submodules of

$$N_1^{\oplus a_1} \oplus \cdots \oplus N_r^{\oplus a_r} \tag{9.4}$$

are those of the form

$$A_1 \otimes N_1[\omega] \oplus \cdots \oplus A_r \otimes N_r[\omega], \tag{9.5}$$

where A_i is a vector subspace of $\mathbb{F}_\ell^{a_i}$ for $i \leq r$.

Proof. We work by induction on $\sum_i a_i$. From Proposition 9.5, the result holds for this sum at most two. Now take $a \geq 3$, and suppose every cofavored submodule of (9.4) takes the form (9.5) for $\sum_i a_i < a$. Then suppose $\sum_i a_i = a$, and take T to be a cofavored submodule of (9.4).

Suppose that $N_j = 0$ for some j where $a_j > 0$. Then the image of T under the map

$$\bigoplus_i N_i^{\oplus a_i} \xrightarrow{\sim} \bigoplus_{i \neq j} N_i^{\oplus a_i}$$

is cofavored, and takes the form (9.5) by the induction step. Thus T also takes this form. So we may assume the N_j are nonzero.

Choose any direct sum of basic exact sequences

$$0 \to \bigoplus_i N_i^{\oplus b_i} \xrightarrow{\iota} \bigoplus_i N_i^{\oplus a_i} \xrightarrow{\pi} \bigoplus_i N_i^{\oplus a_i - b_i} \to 0. \tag{9.6}$$

with $\sum_i a_i > \sum_i b_i > 0$. We claim that we can assume that $\iota^{-1}(T)$ is zero and that

$$\pi(T) = \bigoplus_i N_i^{\oplus a_i - b_i}[\omega]. \tag{9.7}$$

First, suppose $\iota^{-1}(T)$ is nonzero. It is cofavored, and hence can be written in the form (9.5) by the induction step. There is then some other direct sum of basic exact sequences

$$0 \to \bigoplus_i N_i^{\oplus c_i} \xrightarrow{\iota_c} \bigoplus_i N_i^{\oplus a_i} \xrightarrow{\pi_c} \bigoplus_i N_i^{\oplus a_i - c_i} \to 0 \tag{9.8}$$

with $\sum_i c_i > 0$ so that

$$\bigoplus_i N_i^{\oplus c_i}[\omega] = \iota_c^{-1}(T).$$

The module $\pi_c(T)$ is cofavored, and hence expressible in the form (9.5). T equals its preimage in $\bigoplus_i N_i^{\oplus a_i}[\omega]$, and is hence also expressible in this form.

Now suppose (9.7) fails to hold. The module $\pi(T)$ is cofavored, and hence expressible in the form (9.5). The same holds for the preimage $\pi^{-1}(\pi(T))[\omega]$. We now choose (9.8) so that

$$\iota_c\left(\bigoplus_i N_i^{\oplus c_i}\right) = \pi^{-1}(\pi(T))[\omega] \supseteq T.$$

Because (9.7) does not hold, we have that $\sum_i a_i > \sum_i c_i$, so $\iota_c^{-1}(T)$ is expressible in the form (9.5) by the induction step. But $T = \iota_c(\iota_c^{-1}(T))$, and hence is also expressible in this form.

We have now reduced to the case where, given any direct sum of basic exact sequences (9.6) satisfying $\sum_i a_i > \sum_i b_i > 0$, we have $\iota^{-1}(T) = 0$ and (9.7). But in this case, we must have

$$\dim T = \sum_i (b_i - a_i) \cdot \dim N_i[\omega]$$
$$\text{for all } b_1, \ldots, b_r \geq 0 \text{ so that } \sum_i a_i > \sum_i b_i > 0.$$

Since $\sum_i a_i$ is at least three and the $\dim N_i$ are all positive, it is easy to prove that this statement cannot hold. We have thus proved the proposition. □

9.1. **Main base-case results.** Our main results will be concentrated in two main cases, depending on whether N has an alternating structure.

Notation 9.8. Choose $(K/F, \mathscr{V}_0, \mathbb{F})$ as in Notation 8.1. *We assume that* $\mathbb{F}$ *is trivial as a* $\mathrm{Gal}(K/F)$*-module*. Fix a generator ζ of $\mathbb{F}$ and take $\omega = 1 - \zeta$.

Take N to be a potentially-favored twistable module, and choose local conditions $(W_v)_v$ as in Definition 8.5. We assume that these subgroups are ℓ-divisible and are preserved by the action of ζ_*.

We assume that the only cofavored submodules of N are 0 and $N[\omega]$; if this condition, we call N *uncofavored*. We also assume that the only G_F-automorphisms of $N[\omega]$ that commute with the connecting maps are $1, \dots, \ell - 1$.

For each $m > 0$, we have a natural nondegenerate pairing

$$P_m : N[\omega^m] \otimes N'[\omega^m] \to \mu_{\ell^\infty}$$

If there is no nonzero G_F-equivariant homomorphism $\beta_1 : N[\omega] \to N'[\omega]$ that commutes with the connecting maps, we say that N is in *the non-alternating case*.

Otherwise, suppose there is a G_F-equivariant isomorphism

$$\beta : N \to N'$$

of $\mathbb{Z}_\ell[\zeta]$ modules so that $P_m(x, \beta(x)) = 0$ for all $m > 0$ and all x in $N[\omega^m]$. If $\ell = 2$, we suppose there is some G_F-equivariant map $e : N[2] \to \pm 1$ that satisfies

$$e(x + y) = e(x)e(y)P_{m_0+1}(x, \beta y) \quad \text{for all } x, y \in N[2], \tag{9.9}$$

where m_0 is chosen so $N[\omega^{m_0}] = N[2]$. From this information, we can construct a quadratic form

$$q_H : H^1(H, N[\omega]) \to H^2(H, \overline{F}^\times) \tag{9.10}$$

for all closed subgroups H of G_F. This is the form given in Proposition 3.2 for $\ell = 2$, and can be defined as the cup product

$$q_H(\phi) = -\tfrac{1}{2}\phi \cup_{P_0} \beta_*\phi.$$

for $\ell \neq 2$.

Given this information, we say that N is in the *alternating case* if, for $v \in \mathscr{V}_0$ and $m > 0$, the preimage of W_v under

$$H^1(G_v, N[\omega^m]) \to H^1(G_v, N)$$

is its own orthogonal complement under the pairing

$$(\phi, \psi) \mapsto \phi \cup_{P_m} \beta_*(\psi).$$

Definition 9.9. For $m > 0$ and N and $(W_v)_v$ in the alternating or non-alternating case, we take $W_{v,m}$ to be the preimage of W_v under

$$H^1\left(G_v,\, N[\omega^m]\right) \to H^1\left(G_v,\, N\right).$$

Then, for $\chi_v \in H^1(G_v, \mathbb{F})$ chosen for $v \in \mathscr{V}_0$, we define

$$\begin{aligned}&\mathscr{S}^{\cap}(N,\, (\chi_v)_v)\\ &\quad = \ker\left(H^1(G_F, N[\omega]) \to \prod_{v \in \mathscr{V}_0} H^1(G_v, N[\omega])/W_{v,1}(\chi_v) \,\times \prod_{\sigma \in G_{F(\mu_{\ell^k})}} H^1(\langle\sigma\rangle,\, N[\omega])\right).\end{aligned}$$

We always have

$$\mathscr{S}^{\cap}(N,\, (\chi)_v) \,\subseteq\, \text{Sel}^{\omega}(N^{\chi}).$$

Supposing χ is ramified at at least one prime, the connecting map $\delta_{N^{\chi}}$ associated to

$$0 \to N[\omega] \to N^{\chi}[\omega^2] \to N[\omega] \to 0$$

gives an injection

$$\delta_{N^{\chi}, G_F} : H^0(G_F, N[\omega]) \to \omega_*^{m-1}\text{Sel}^{\omega^m}(N^{\chi}).$$

For $m > 0$, we take

$$r_{\omega^m}(N^\chi) = \dim_{\mathbb{F}_\ell} \omega_*^{m-1}\text{Sel}^{\omega^m}(N^\chi) - \dim_{\mathbb{F}_\ell} H^0(G_F, N[\omega]).$$

Choose $\chi \in \mathbb{X}_F$. Per an observation of Wiles [55], the formula

$$r_\omega\left(N^\chi\right) - r_\omega\left((N')^\chi\right) = \sum_{v\in\mathscr{V}_0} \dim W_{v,1}(\chi) - \dim H^0(G_v, N[\omega]) \tag{9.11}$$

follows from Poitou-Tate duality and the global Euler-Poincaré characteristic formula of Tate, with this particular statement a special case of [41, 8.7.9]. (We note that, in the enumeration of places, each pair of complex embeddings of F corresponds to one place in $\mathscr{V}_0$.)

The basic linear-algebraic idea of the various heuristics describing Selmer groups is that $\text{Sel}^\omega N^\chi$ and $\text{Sel}^\omega\left((N')^\chi\right)$ should behave like the kernel and cokernel of some large matrix with entries selected uniformly at random from $\mathbb{F}_\ell$. The difference in dimension between the kernel and cokernel of this matrix is of course the difference between the number of rows and columns of the matrix, so Wiles' formula frequently appears in these predictions.

Because $\text{Sel}^\omega N^\chi$ always contains $\mathscr{S}^\cap(N,\ (\chi)_v)$, we will need to adjust the matrix heuristics accordingly. So define

$$\begin{aligned} u_{\text{r/c}}(N, (\chi_v)_v) = &\dim \mathscr{S}^\cap(N',\ (\chi_v)_v) - \dim \mathscr{S}^\cap(N,\ (\chi_v)_v) \\ &+ \sum_{v\in\mathscr{V}_0} \left(\dim W_{v,1}(\chi_v) - \dim H^0(G_v, N[\omega])\right). \end{aligned}$$

Theorem 9.10. *Suppose N is a twistable module with local conditions $(W_v)_v$ in the non-alternating case. Given $\epsilon > 0$, there is then $C > 0$ so we have the following:*

Fix $(\chi_v)_v$, and take

$$r_0 = \dim \mathscr{S}^\cap(N,\ (\chi_v)_v).$$

We assume $\mathbb{X}_F(H,\ (\chi_v)_v)$ is nonempty for sufficiently large H.

Suppose $H > C$. Then, for $r \geq 0$, with notation as in Definition 1.15, the difference

$$\left| \frac{\#\left\{\chi \in \mathbb{X}^{\text{fav}}_{F,N}(H,\,(\chi_v)_v) \,:\, r_\omega(N^\chi) = r + r_0\right\}}{\#\mathbb{X}^{\text{fav}}_{F,N}(H,\,(\chi_v)_v)} \;-\; P^{\text{Mat}}_{\ell,\,u_{\text{r/c}}(N,(\chi_v)_v)}(r \mid \infty) \right| \tag{9.12}$$

has upper bound

$$(\log\log H)^{-1/4+\epsilon}.$$

If

$$\lim_{H\to\infty} \frac{\#\mathbb{X}^{\text{fav}}_{F,N}(H)}{\#\mathbb{X}_F(H)} = 1,$$

we can instead bound (9.12) *by*

$$\exp^{(2)}\left(\tfrac{1}{5}\log^{(3)} H\right)^{-1}.$$

We will prove this in Section 14.3.

Example 9.11. The case $k = 1$ of Theorem 1.16 follows as a consequence of this result and Proposition 8.8. Taking N as in that Proposition, we see that N is in the non-alternating case. $N[\omega]$ is one dimensional, so it is uncofavored and has no automorphisms besides scalar multiples. To apply the theorem to $\text{Sel}^\omega N^\chi$, we then just need to show that $N[\omega]$ and $N'[\omega]$ have no isomorphism commuting with boundary maps. But recall that we assumed that $\mu_{2\ell}$ does not lie in F. For ℓ odd, this implies $N[\omega]$ and $N'[\omega]$ are not isomoprhic. If $\ell = 2$, the unique isomorphism does not commute with the boundary maps.

We thus just need to show that (8.2) holds for 100% of twists of N. In light of the Grunwald-Wang theorem, this will be a consequence of Proposition 12.5, part 5.

We have a similar result for the alternating case, where $u_{\text{r/c}}$ is always zero. We require a little more notation:

Definition 9.12. Given N in the alternating case, we say N is in the *parity-invariant case* if, for some (or every) choice of local twists $(\chi_v)_v$ such that $\mathbb{X}_F(H,\,(\chi_v)_v)$ is nonempty

for sufficiently large H, the parity of $r_\omega(N^\chi)$ does not depend on the choice of χ from $\mathbb{X}_F(H,\,(\chi_v)_v)$.

We will consider parity invariance in greater detail in Section 14.1.

Definition 9.13. Given $n \geq j \geq 0$, take

$$P_\ell^{\text{Alt}}(j \mid n)$$

to be the probability that a a uniformly selected alternating $n \times n$ matrix with coefficients in $\mathbb{F}_\ell$ has kernel of rank exactly j. The is zero unless j and n have the same parity, in which case it equals

$$\frac{\ell^{\frac{1}{4}(j^2+2j-n^2-2nj)} \cdot (\ell^n-1)(\ell^{n-1}-1)\cdots(\ell-1)}{(\ell^j-1)(\ell^{j-1}-1)\cdots(\ell-1)\cdot(\ell^{n-j}-1)(\ell^{n-j-2}-1)\cdots(\ell^2-1)}.$$

We also will define

$$P_\ell^{\text{Alt}}(j \mid 2\infty+b) = \lim_{n\to\infty} P_\ell^{\text{Alt}}(j \mid 2n+b) \quad \text{and}$$
$$P_\ell^{\text{Alt}}(j \mid \infty) = \frac{1}{2}\left(P_\ell^{\text{Alt}}(j \mid 2\infty) + P_\ell^{\text{Alt}}(j \mid 2\infty+1)\right).$$

Theorem 9.14. *Suppose N is a twistable module with local conditions $(W_v)_v$ in the alternating case. Given $\epsilon > 0$, there is then $C > 0$ so we have the following:*

Fix $(\chi_v)_v$, and take

$$r_0 = \dim \mathscr{S}^\cap(N,\,(\chi_v)_v).$$

We assume $\mathbb{X}_F(H,\,(\chi_v)_v)$ is nonempty for sufficiently large H. In the parity-invariant case, take $k_0 \in \{0,1\}$ to be the parity of $r_\omega(N^\chi) - r_0$ for χ from this set of twists. For $r \geq 0$, define

$$P(r) = \begin{cases} P_\ell^{\text{Alt}}(r \mid 2\infty+k_0) & \textit{in the parity-invariant case} \\ P_\ell^{\text{Alt}}(r \mid \infty) & \textit{otherwise.} \end{cases}$$

Now suppose $H > C$. With notation as in Definition 1.15, the difference

$$\left| \frac{\#\left\{\chi \in \mathbb{X}_{F,N}^{\text{fav}}(H,\, (\chi_v)_v) \,:\, r_\omega(N^\chi) = r + r_0\right\}}{\#\mathbb{X}_{F,N}^{\text{fav}}(H,\, (\chi_v)_v)} \,-\, P(r) \right| \tag{9.13}$$

has upper bound

$$(\log\log H)^{-1/4+\epsilon}.$$

If

$$\lim_{H\to\infty} \frac{\#\mathbb{X}_{F,N}^{\text{fav}}(H)}{\#\mathbb{X}_F(H)} = 1,$$

we can instead bound (9.13) *by*

$$\exp^{(2)}\left(\tfrac{1}{5}\log^{(3)} H\right)^{-1}.$$

We will prove this in Section 14.3.

As a consequence, we get the case $k = 1$ of our main result for abelian varieties, which we state below. Here, we take the notation $r_{2^k}(A)$ from the introduction.

Theorem 9.15. *Take A to be an abelian variety over a number field F, and take $\mathscr{V}_0$ to be a set of places of F that include the archimedean places, the places dividing 2, and the places where A has bad reduction.*

We assume that A has a polarization defined over F of odd degree. We further assume that $A[2^\infty]$ is potentially favored and uncofavored, that $A[2]$ has no nonidentity automorphisms commuting with the connecting maps, and that we have an identity

$$\ker\left(H^1(G_F,\, A[2]) \to \prod_{\sigma\in G_F} H^1(\langle\sigma\rangle,\, A[2])\right) = 0. \tag{9.14}$$

Choose a set of local twists $(\chi_v)_{v\in\mathscr{V}_0}$. If A/F is parity invariant (see Section 14.1), take $b \in \{0,1\}$ so $r_2(A^d)$ has parity b for all χ in $\mathbb{X}_F((\chi_v)_v)$.

Then, given $k \geq 1$, and given any sequence of integers

$$r_2 \geq r_4 \geq \cdots \geq r_{2^k} \geq 0,$$

we have

$$\lim_{H\to\infty} \frac{\#\{\mathbb{X}^{\text{fav}}_{F,A}(H,\,(\chi_v)_v)\ :\ r_2(A^\chi)=r_2,\,\ldots\,r_{2^k}(A^\chi)=r_{2^k}\}}{\#\mathbb{X}^{\text{fav}}_{F,A}(H,\,(\chi_v)_v)}$$

$$= P^{\text{Alt}}(r_{2^k}\big|r_{2^{k-1}})\cdot P^{\text{Alt}}(r_{2^{k-1}}\big|r_{2^{k-2}})\cdot\ldots$$

$$\ldots\cdot P^{\text{Alt}}(r_4\big|r_2)\cdot\begin{cases} P^{\text{Alt}}(r_2\big|2\infty+b) & \textit{in the parity invariant case}\\ P^{\text{Alt}}(r_2\big|\infty) & \textit{otherwise.}\end{cases}$$

We will now apply this theorem in the special case of elliptic curves.

9.1.1. *Technical conditions for elliptic curves.* For our theorems to apply to an elliptic curve E over a number field F, we need E to be potentially favored, uncofavored, and we need that $E[2]$ has no nonidentity automorphism commuting with the connecting maps. In the case of $F=\mathbb{Q}$, we will find that these conditions are satisfied by the curves satisfying Assumption 1.2.

We can find c_1,c_2,c_3 in $F(E[2])^\times$ and a,b in F so that E is isomorphic over F to

$$y^2=x^3+ax+b=(x-c_1)(x-c_2)(x-c_3)$$

Take e_1 to be the point $(c_1,0)$, and take e_2 to be the point $(c_2,0)$. The connecting map

$$E[2]\to H^1(G_{F(E[2])},E[2])$$

can be given in the form

$$e_1\mapsto e_1\cdot\chi_{c_1-c_2}+e_2\cdot\chi_{(c_3-c_1)\cdot(c_2-c_1)}$$

$$e_2\mapsto e_1\cdot\chi_{(c_3-c_2)\cdot(c_1-c_2)}+e_2\cdot\chi_{c_2-c_1},$$

where $\chi_c\ :\ G_{F_1}\to\mathbb{F}_2$ denotes the quadratic character associated to $F_1(\sqrt{c})/F_1$; this calculation can be done directly, and is the content of [47, Proposition X.1.4].

We now split into cases.

Example 9.16. Suppose $F = F(E[2])$. We find that E is uncofavored if and only if none of the isogenous curves

$$E/\langle e_1 \rangle, \quad E/\langle e_2 \rangle, \quad E/\langle e_1 + e_2 \rangle$$

has full rational two torsion. This is equivalent to the condition that E has no rational cyclic 4-isogeny. Given the above form of the connecting map, this condition is equivalent to saying that none of

$$(c_3 - c_1) \cdot (c_2 - c_1), \quad (c_3 - c_2) \cdot (c_1 - c_2), \quad (c_1 - c_3) \cdot (c_2 - c_3) \tag{9.15}$$

are in $(F^\times)^2$. If E is not uncofavored, there is then $c \in F \backslash \{0, \pm 1\}$ and d in $F^\times$ so that E is isomorphic to

$$dy^2 = x(x-1)(x-c^2).$$

Equivalently, the non-uncofavored E have j-invariant in the set

$$\left\{ 2^8 \cdot \frac{(c^4 - c^2 + 1)^3}{c^4(c^2-1)^2} \ : \ F \backslash \{0, \pm 1\} \right\}.$$

We now check for a nonidentity automorphism commuting with the connecting maps. From Remark 9.6, we can restrict our attention to the isomorphism T sending e_1 to e_2 to $e_1 + e_2$ back to e_1. We calculate that this commutes with the connecting maps if and only if all three entries in (9.15) are all in $-(F^\times)^2$. Taking $c_1 = 0$, $c_2 = 1$, $c_3 = \lambda$, we must have $z_0, z_1 \in F^\times$ so

$$\lambda = -z_0^2, \quad 1 - \lambda = -z_1^2 \implies -z_0^2 - z_1^2 = 1.$$

This is impossible unless there are κ_0, κ_1 in F so $\kappa_0^2 + \kappa_1^2 = -1$ is solvable, so this case cannot happen for $F = \mathbb{Q}$. Suppose now that this equation has a solution over F. We can

then parameterize the F points of the conic $z_0^2 + z_1^2 = -1$, with the map

$$(t_0, t_1) \mapsto (z_0, z_1) = \left(\frac{-\kappa_0 t_0^2 + 2\kappa_1 t_0 t_1 + \kappa_0 t_1^2}{t_0^2 + t_1^2}, \ \frac{\kappa_1 t_0^2 + 2\kappa_0 t_0 t_1 - \kappa_1 t_1^2}{t_0^2 + t_1^2} \right)$$

giving a birational map from $\mathbb{P}^1(F)$ to this locus. We then find that the elliptic curves in this exceptional form are isomorphic to some curve of the form

$$dy^2 = x\,(x-1)\left(x + \frac{(-\kappa_0 t_0^2 + 2\kappa_1 t_0 t_1 + \kappa_0 t_1^2)^2}{(t_0^2 + t_1^2)^2} \right).$$

These curves are uncofavored unless F contains $\sqrt{-1}$, in which case none are uncofavored.

Example 9.17. Suppose $F(E[2])/F$ is a $\mathbb{Z}/3\mathbb{Z}$ extension. The only proper G_F-submodule of $E[2]$ is 0, so E is uncofavored. The isomorphism T is G_F-equivariant, so we need to check that it does not commute with the connecting maps. Taking σ to be a generator of $\mathrm{Gal}(F(E[2])/F)$, we note that any curve in this case can be written in the form

$$E : y^2 = \left(x - \tfrac{1}{3}\sigma^2\alpha + \tfrac{1}{3}\alpha\right)\left(x - \tfrac{1}{3}\alpha + \tfrac{1}{3}\sigma\alpha\right)\left(x - \tfrac{1}{3}\sigma\alpha + \tfrac{1}{3}\sigma^2\alpha\right) \tag{9.16}$$

with α an element of $F(E[2])$ of zero trace. We then find that T commutes with the connecting maps if and only if $\alpha/\sigma\alpha$ is a square in $F(E[2])$. As in the full 2-torsion case, this forces $\kappa_0^2 + \kappa_1^2 + 1 = 0$ to have a solution over $F(E[2])$, and hence over F from the theory of Hilbert symbols, eliminating the case $F = \mathbb{Q}$.

To give a particular example, take F to be a number field containing $\mathbb{Q}(\mu_3)$, and take b to be any element of $F^\times$ that is not a cube. Then, if we consider the elliptic curve

$$E : y^2 = x^3 + b,$$

we find that the extension $F(E[2])/F$ is of degree 3, and the map T commutes with the connecting maps. This corresponds to the choice $\alpha = -(\zeta - 1)\sqrt[3]{b}$ in (9.16), with ζ a primitive third root of unity, and we see that $\alpha/\sigma\alpha$ lies in μ_3 and is hence a square.

This exception is exceptional, of course, as this elliptic curve has complex multiplication by $\mathbb{Z}[\mu_3]$. If ζ is a primitive third root of unity in this order, we find that either ζ or ζ^2 restricts to T on $E[2]$.

Example 9.18. If $F(E[2])/F$ is quadratic, E can be given the equation

$$E : y^2 = x(x^2 + Ax + B).$$

Taking the quotient by $\langle (0,0) \rangle$ gives the isogenous curve

$$E_0 : y^2 = x(x^2 - 2Ax + (A^2 - 4B))$$

(see e.g. [23]). We have that E is uncofavored if and only if $F(E[2]) \neq F(E_0[2])$, which is equivalent to the condition

$$F\left(\sqrt{4B - A^2}\right) \neq F\left(\sqrt{-B}\right).$$

E is potentially favored if $E_0[2]$ is not a trivial G_F module, which occurs if $-B$ is not a square in F. We find that E_0 is potentially favored, and is uncofavored if E is also uncofavored.

In this case, the isomorphism T is non-equivariant. Then, under the partial two torsion case of Assumption 1.2, Theorem 9.15 and Proposition 14.6 give the $k = 1$ case of the following:

Theorem 9.19. *Suppose $E/\mathbb{Q}$ is an elliptic curve that fits into the second case of Assumption 1.2. That is, suppose we can find rational numbers A, B so that E can be given the equation*

$$E : y^2 = x(x^2 + Ax + B),$$

where we assume that none of $-B$, $A^2 - 4B$, $-B(A^2 - 4B)$ are rational squares. Take $\mathscr{V}_0$ to be a set of places including 2, ∞, and the places where E has bad reduction

Take $X^{\text{fav}}(H)$ to be the set of squarefree integers of the form $d_0 \cdot p_1 \dots p_r$ of magnitude at most H, where d_0 is divisible only by primes in $\mathscr{V}_0$, where $p_1, \dots, p_r$ are distinct primes outside $\mathscr{V}_0$, and where

$$\#\left\{i \le r \ : \ p_i \text{ splits in } \mathbb{Q}\left(\sqrt{A^2-4B}\right)/\mathbb{Q}\right\} > \#\left\{i \le r \ : \ p_i \text{ splits in } \mathbb{Q}(\sqrt{-B})/\mathbb{Q}\right\}.$$

Take $X_0^{\text{fav}}(H)$ to be the complement of $X^{\text{fav}}(H)$ in the set of squarefree integers of magnitude at most H.

Then we have

$$\lim_{H\to\infty} \frac{\#X^{\text{fav}}(H)}{\#X_0^{\text{fav}}(H)} = 1.$$

Further, for $1/2 > \epsilon > 0$, we have

$$\lim_{H\to\infty} \frac{\#\left\{d \in X^{\text{fav}}(H) \ : \ r_2(E_0^d) \ge (\log\log H)^{1/2-\epsilon}\right\}}{\#X^{\text{fav}}(H)} = 1. \tag{9.17}$$

Finally, given $k \ge 1$ and any sequence of integers

$$r_2 \ge r_4 \ge \cdots \ge r_{2^k} \ge 0,$$

we have

$$\begin{aligned}\lim_{H\to\infty} &\frac{\#\{d \in X^{\text{fav}}(H) \ : \ r_2(E^d) = r_2, \ \dots \ r_{2^k}(E^d) = r_{2^k}\}}{\#X^{\text{fav}}(H)} \\ &= P^{\text{Alt}}(r_{2^k} \,\big|\, r_{2^{k-1}}) \cdot P^{\text{Alt}}(r_{2^{k-1}} \,\big|\, r_{2^{k-2}}) \cdot \dots \cdot P^{\text{Alt}}(r_4 \,\big|\, r_2) \cdot P^{\text{Alt}}(r_2 \,\big|\, , \infty).\end{aligned}$$

Example 9.20. If $F(E[2])/F$ is an S_3 extension, we have that the automorphism T is non-equivariant, and E is vacuously uncofavored. From this, Theorem 9.14 always applies in this case, finishing the verification of the $k = 1$ portion of Theorem 1.10.

10. BASE-CASE SELMER CONDITIONS

10.1. **Dual modules.** In Section 8.2, given a twistable module N, we introduced $N^\vee$ and N', two reasonable definitions of a dual twistable module. We now give some of the basic properties of this definition.

Take a, c to be nonnegative integers. If the ideal (ℓ^c) of $\mathbb{Z}[\mathbb{F}]$ contains ω^a, we have an isomorphism

$$\begin{aligned} N^\vee[\omega^a] &\xrightarrow{\sim} \text{Hom}\left(N[\ell^c]/N[\ell^c/\omega^a],\ \mu_{\ell^c}\right) \\ \phi \otimes \tfrac{1}{\ell^c} &\longmapsto (t \mapsto \phi(t)) \end{aligned}$$

If b is at most a, this gives an isomorphism

$$N^\vee[\omega^a]/N^\vee[\omega^b] \xrightarrow{\sim} \text{Hom}\left(N[\ell^c/\omega^b]/N[\ell^c/\omega^a],\ \mu_{\ell^c}\right).$$

In particular, we have an isomorphism

$$\begin{aligned} N'[\omega] =& N^\vee[\ell]/N^\vee[\ell/\omega] \cong \text{Hom}\left(N[\omega],\ \mu_\ell\right) \\ \phi \otimes \tfrac{1}{\ell} \quad &\longmapsto \qquad\qquad (t \mapsto \phi(t)). \end{aligned}$$

That is to say, we have a natural nondegenerate G_F-equivariant pairing

$$N[\omega] \times N'[\omega] \longrightarrow \mu_\ell.$$

This defines (8.7).

Proposition 10.1. *Take χ to be an element of $H^1(G_F, \mathbb{F})$. Then, using the notation of Definition 8.13, the composition*

$$W^\chi \xrightarrow{\beta_{W,\chi}} W = \text{Hom}\left(N, \mu_{\ell^\infty}\right) \xrightarrow{\beta^\top_{N,\chi}} \text{Hom}\left(N^\chi, \mu_{\ell^\infty}\right)$$

is equivariant under the action of G_F. In particular, we have natural G_F-equivariant isomorphisms

$$(N^\vee)^\chi \cong (N^\chi)^\vee \quad \textit{and} \quad (N')^\chi = (N^\chi)'.$$

Proof. Take ϕ in W^χ, σ in G_F, and t in N^χ. Our goal is to prove

$$\sigma(\beta^\top_{N,\chi}(\beta_{W,\chi}(\phi)))(t) = \beta^\top_{N,\chi}(\beta_{W,\chi}(\sigma(\phi)))(t).$$

We note that, in $\mathbb{F}$, the condition that χ is a class of cocycles implies

$$\chi(\sigma)^{-1} = \sigma\chi(\sigma^{-1}).$$

In End$N$, this implies that $\sigma\chi(\sigma^{-1})\sigma^{-1}$ equals $\chi(\sigma)^{-1}$. We then have

$$\begin{aligned}
&\sigma(\beta^\top_{N,\chi}(\beta_{W,\chi}(\phi)))(t) && = \sigma\left[\beta^\top_{N,\chi}(\beta_{W,\chi}(\phi))(\sigma^{-1}t)\right] \\
&= \sigma\left[\beta_{W,\chi}(\phi)(\beta_{N,\chi}(\sigma^{-1}t))\right] && = \sigma\left[\beta_{W,\chi}(\phi)\left(\chi(\sigma^{-1})\sigma^{-1}\beta_{N,\chi}(t)\right)\right] \\
&= \sigma\left[\beta_{W,\chi}(\phi)\left(\sigma^{-1}\chi(\sigma)^{-1}\beta_{N,\chi}(t)\right)\right] && = \sigma\left(\beta_{W,\chi}(\phi)\right)\left(\chi(\sigma)^{-1}\beta_{N,\chi}(t)\right) \\
&= \chi(\sigma)(\sigma(\beta_{W,\chi}(\phi)))\left(\beta_{N,\chi}(t)\right) && = \beta_{W,\chi}(\sigma\phi)(\beta_{N,\chi}(t)) \\
&= \beta^\top_{N,\chi}(\beta_{W,\chi}(\sigma\phi))(t), &&
\end{aligned}$$

as claimed. □

Given a closed subgroup H of G_F, we can define connecting homomorphisms

$$\delta_H : H^0\left(H,\ N[\omega^2]/N[\omega]\right) \to H^1(H, N[\omega]), \tag{10.1}$$

$$\delta'_H : H^0\left(H,\ N'[\omega^2]/N'[\omega]\right) \to H^1(H, N'[\omega]) \tag{10.2}$$

associated to the exact sequences

$$0 \to N[\omega] \to N[\omega^2] \to N[\omega^2]/N[\omega] \to 0,$$

$$0 \to N'[\omega] \to N'[\omega^2] \to N'[\omega^2]/N'[\omega] \to 0.$$

We can alternatively take δ to be the class of the above extension in $\mathrm{Ext}^1_{G_F}(N[\omega^2]/N[\omega], N[\omega])$, so δ_H becomes the composition of restriction with a Yoneda product, with a similar definition for δ'.

The following proposition is essential in the proof of Proposition 8.15, though it will also have uses for H the absolute Galois group of a number field.

Proposition 10.2. *Take N and H as above. Under the cup product*

$$H^1(H, N[\omega]) \times H^1(H, N'[\omega]) \longrightarrow H^2(H, \mu_{\ell^2})$$

coming from the composition of (8.7) *with the inclusion $\mu_\ell \hookrightarrow \mu_{\ell^2}$, the image of δ_H is annihilated by the image of δ'_H.*

Proof. We first note that we have a natural pairing

$$\langle\ ,\ \rangle_1 : N[\ell\omega] \times N'[\ell\omega] \longrightarrow \mu_{\ell^2}$$

that satisfies

$$\ell\langle t, t'\rangle_1 = \langle \ell t, \ell t'\rangle \quad \text{for } t \in N[\ell\omega], t' \in N'[\ell\omega],$$

where the latter pairing is (8.7). Writing $\cup_1$ for the associated cup product, and using the notation

$$\iota : N[\omega] \hookrightarrow N[\ell\omega] \quad \text{and} \quad \ell : N[\omega\ell] \xrightarrow{\cdot\ell} N[\omega],$$

we have

$$\phi \cup_1 \iota_*\phi' = \ell_*\phi \cup \phi' \quad \text{for } \phi \in H^1(H, N[\omega\ell]),\ \phi' \in H^1(H, N'[\omega]).$$

Take $\delta_{1,H}$ to be the connecting homomorphism associated to

$$0 \to N[\ell\omega] \to N[\ell\omega^2] \xrightarrow{\cdot\ell} N[\omega^2]/N[\omega]$$

and the group H. Then $\delta_H = \ell_* \circ \delta_{1,H}$. From the above, it is then enough to prove that the images of $\delta_{1,H}$ and $\iota_* \circ \delta'_H$ annihilate each other. But $\iota_* \circ \delta'_H$ factors through the composition

$$H^0\left(H,\ N'[\omega^2]/N'[\omega]\right) \to H^1(H, N'[\omega]) \to H^1(H, N'[\omega^2]),$$

of maps from the long exact sequence, and is hence zero. This gives the proposition. $\square$

We have a pairing

$$\begin{aligned} P : N[\omega^2]/N[\omega] \times N'[\omega] \ &\longrightarrow \mathrm{Hom}(\mathbb{F}, \mu_\ell) \\ t \qquad\qquad \phi \otimes \tfrac{1}{\ell} &\longmapsto \ \left(\zeta \mapsto \phi\left((\zeta - 1)\tfrac{t}{\ell}\right)\right) \end{aligned}$$

and another pairing

$$\begin{aligned} P' : N[\omega] \ \times \ N'[\omega^2]/N'[\omega] \ &\longrightarrow \mathrm{Hom}(\mathbb{F}, \mu_\ell) \\ t \qquad\qquad \phi \otimes \tfrac{1}{\ell^2} \ &\longmapsto \ \left(\zeta \mapsto \phi\left((\zeta - 1)\tfrac{t}{\ell}\right)\right). \end{aligned}$$

We denote the associated cup products by $\cup_P$ and $\cup_{P'}$.

The rationale for our level of detail in these constructions is that it is necessary to prove the following somewhat obnoxious proposition. We note, however, that there is a method to circumvent the use of this proposition in our proof; see Remark 10.6.

Proposition 10.3. *Take N and H as above, with H a procyclic group with topological generator σ. Define a pairing*

$$\begin{aligned} P_{\mathbb{F}} : N[\omega^2]/N[\omega] \times \mathbb{F} \ &\longrightarrow N[\omega] \\ t \qquad\qquad \zeta \ &\longmapsto \ (\zeta - 1)t, \end{aligned}$$

and write $\cup_{\mathbb{F}}$ for the associated cup product. Given $\sigma \in G_F$, take

$$\chi_{-1}(\sigma) = \frac{\sigma\sqrt{-1}}{\sqrt{-1}}.$$

If $\ell = 2$, there is a unique submodule of order two of $\mathbb{F}$, and we will write χ_{-1} for the image in $H^1(H, \mathbb{F})$ of χ_{-1} under this embedding.

Then, for x in $H^0\left(H,\ N[\omega^2]/N[\omega]\right)$ and x' in $H^0\left(H,\ N'[\omega^2]/N'[\omega]\right)$, we have

$$x \cup_P \delta'_H x' \ = \ -\delta_H x \cup_{P'} x' \ + \ \begin{cases} (x \cup_{\mathbb{F}} \chi_{-1}) \cup_{P'} x' & \text{if } \ell = 2 \\ 0 & \text{otherwise} \end{cases}$$

in $H^1(H, \mathrm{Hom}(\mathbb{F}, \mu_\ell))$.

Proof. Take x and x' as in the proposition. Lift x to an element t of $N[\omega^2]$ and $\frac{1}{\ell}t$ of $N[\ell\omega^2]$, and lift x' to an element $f \otimes \frac{1}{\ell^2}$ in $N'[\omega^2]$. By replacing f with the alternative lift $\sigma^{-1}f$, we note that the class $x \cup_P \delta'_H x'$ is represented by a cocycle sending σ to

$$\zeta \longmapsto \quad f\left((\zeta - 1)\tfrac{1}{\ell}t\right) - \sigma^{-1}\left[f\left(\sigma(\zeta - 1)\tfrac{1}{\ell}t\right)\right].$$

The class $\delta_H x \cup_{P'} x'$ is represented by the cocycle sending σ to

$$\zeta \longmapsto \quad f\left((\zeta - 1)(\sigma - 1)\tfrac{1}{\ell}t\right) \ = \ f\left((\zeta - 1)\sigma\tfrac{1}{\ell}t\right) - f\left((\zeta - 1)\tfrac{1}{\ell}t\right),$$

and the sum of these is

$$\zeta \longmapsto \quad f\left((\zeta - 1)\sigma\tfrac{1}{\ell}t\right) - \sigma^{-1}\left[f\left(\sigma(\zeta - 1)\tfrac{1}{\ell}t\right)\right].$$

We suppose that $\mathbb{F}$ has order 2. This then simply equals

$$-1 \longmapsto \quad (\sigma^{-1} - 1)f(\sigma t) = f((\chi_{-1}(\sigma) - 1)t),$$

which agrees with the claim of the proposition.

Otherwise, take a in $(\mathbb{Z}/\ell^k\mathbb{Z})^\times$ so $\sigma\zeta = \zeta^a$ for $\zeta \in \mathbb{F}$. Since $\mathbb{F}$ has order greater than two, we find that $f\left(\sigma(\zeta - 1)\frac{1}{\ell}t\right)$ is valued in μ_ℓ, so the map

$$\zeta \longmapsto \quad \sigma^{-1}f\left(\sigma(\zeta - 1)\tfrac{1}{\ell}t\right) - \tfrac{1}{a}f\left(\sigma(\zeta - 1)\tfrac{1}{\ell}t\right)$$

is a coboundary of $\mathrm{Hom}(\mathbb{F}, \mu_\ell)$. We are then interested in the class of

$$\zeta \longmapsto \quad f\left(\left((\zeta-1)-\tfrac{1}{a}(\zeta^a-1)\right)\sigma\tfrac{1}{\ell}t\right).$$

Using the binomial theorem on $((\zeta-1)+1)^a$, we see

$$\left((\zeta-1)-\tfrac{1}{a}(\zeta^a-1)\right) = -\frac{1}{a}\left(\binom{a}{2}(\zeta-1)^2+\binom{a}{3}(\zeta-1)^3+\dots\right).$$

Mod ω^2, only the first term contributes.

Suppose $\ell = 2$. The above class is then

$$\zeta \longmapsto \quad f\left(\tfrac{a-1}{2}(\zeta-1)^2\tfrac{1}{2}t\right),$$

which from the definition of a can be shown to agree with $(x \cup_{\mathbb{F}} \chi_{-1}) \cup_{P'} x'$, as a is 1 mod 4 if and only if σ fixes $\sqrt{-1}$.

Now suppose $\ell > 2$. As before, the difference takes the form

$$\zeta \longmapsto \quad f\left(-\tfrac{a-1}{2}(\zeta-1)^2\sigma\tfrac{1}{\ell}t\right).$$

Writing q for this map, we see this satisfies

$$q(\zeta)^b = q(\zeta^b) = q(\zeta)^{b^2} \quad \text{for} \quad b \in (\mathbb{Z}/\ell^k\mathbb{Z})^\times,$$

the first equation coming from q being a homomorphism and the second coming from a direct calculation. In particular,

$$q(\zeta) = q(\zeta)^{-1}.$$

Since $\ell > 2$, this implies q is trivial, and we are done. □

10.2. **Selmer conditions.** Take N a twistable module over $(K/F, \mathscr{V}_0, \mathbb{F})$ as above. We will take the notation

$$M = N[\omega] \quad Q = N[\omega^2]/N[\omega] \quad R = N'[\omega^2]/N'[\omega].$$

Given a twist χ in $H^1(G_F, \mathbb{F})$, the map β_χ gives G_F equivariant isomorphisms

$$\beta_\chi : N^\chi[\omega] \xrightarrow{\sim} N[\omega] \quad \text{and} \quad \beta_\chi : N^\chi[\omega^2]/N^\chi[\omega] \xrightarrow{\sim} N[\omega^2]/N[\omega].$$

The connecting map (10.1) for N^χ can then be given as a map

$$\delta_{\chi,H} : H^0\left(H,\, N[\omega^2]/N[\omega]\right) \to H^1(H, N[\omega]).$$

For q in $H^0(H,\, N[\omega^2]/N[\omega])$, we calculate that this satisfies

$$\delta_{\chi,H}(q) = \delta_H(q) + q \cup_{\mathbb{F}} \chi, \tag{10.3}$$

with the cup product defined as in Proposition 10.3.

We can similarly define $\delta'_{\chi,H}$ for the twist $(N^\chi)'$, and it obeys an analogous relation to (10.3).

We will work in the situation of Notation 8.14, so S is a finite set, $(\overline{\mathfrak{p}}_s)_s$ are a set of primes indexed by S, and $(\sigma_s)_s$ is the accompanying set of Frobenius elements in

$$G_1 = \mathrm{Gal}\big(K(\mathscr{V}_0)/F(\mathbb{F}(-1))\big).$$

Recall that, for a given twist χ we defined a pairing between $H^1(G_F, M)$ and $\mathscr{R} = \bigoplus_s R^{\langle\sigma_s\rangle}$. We now prove that this pairing can be used to check local conditions at the primes indexed by S.

Proof of Proposition 8.15. For $s \in S$, we find that

$$\phi - \delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s) = \phi - q_s \cup \chi - \delta_{G_{F,\overline{\mathfrak{p}}_s}}(q_s)$$

is unramified at $\overline{\mathfrak{p}}_s$. The Selmer condition is satisfied at $\mathfrak{p}_s$ if and only if this is also zero. Via local Poitou-Tate duality, it is enough to check that

$$\Big(\phi - \delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s)\Big) \cup \psi = 0$$

is zero in $H^2(G_{F,\overline{\mathfrak{p}}_s}, \mu_\ell)$ for all ψ in $H^1(G_{F,\overline{\mathfrak{p}}_s}, M'[\omega])$. We also know that this pairing is zero if ψ is unramified.

We note that the composition

$$H^0(G_{F,\overline{\mathfrak{p}}_s}, N'[\omega^2]/N'[\omega]) \xrightarrow{\delta'_{\chi,G_{F,\overline{\mathfrak{p}}_s}}} H^1(G_{F,\overline{\mathfrak{p}}_s}, N'[\omega]) \xrightarrow{\text{res}} H^1(I_{F,\overline{\mathfrak{p}}_s}, N'[\omega])$$

is surjective; this follows as a consequence of (10.3) and from $G_{F,\overline{\mathfrak{p}}_s}$ having trivial action on $\mathbb{F}(-1)$. From Proposition 10.2, we then find that the local condition at $\mathfrak{p}_s$ is satisfied if and only if

$$\phi \cup \delta'_{\chi,G_{F,\overline{\mathfrak{p}}_s}}(r_s) = 0 \quad \text{for all } r_s \in H^0(G_{F,\overline{\mathfrak{p}}_s}, R).$$

From this, the proposition follows. □

We now will consider the pairing

$$\langle\ ,\ \rangle : \bigoplus_s Q^{\langle\sigma_s\rangle} \otimes \bigoplus_s R^{\langle\sigma_s\rangle} \to \tfrac{1}{\ell}\mathbb{Z}/\mathbb{Z}$$

in more detail. We have an isomorphism

$$\iota_R : R \xrightarrow{\sim} \text{Hom}(M \otimes \mathbb{F}, \mu_\ell)$$
$$\phi \otimes \tfrac{1}{\ell^2} \longmapsto \left(t \otimes \zeta \mapsto \phi\left((\zeta - 1)\tfrac{t}{\ell}\right)\right).$$

This is the map corresponds to the pairing P' defined before Proposition 10.3.

We will need the following notation:

Notation 10.4.

- $\sigma_0, \sigma_1, \sigma_2$ will denote elements of $G_1 = \text{Gal}(K(\mathscr{V}_0)/F(\mathbb{F}(-1)))$
- For each σ_0, fix a prime $\overline{\mathfrak{q}}_{\sigma_0}$ of $\overline{F}$ not over $\mathscr{V}_0$ so that $\text{Frob}_F\overline{\mathfrak{q}}_{\sigma_0}$ projects to σ_0.
- For each pair (σ_1, σ_2), take $B(\sigma_1, \sigma_2)$ to be a set of representatives in $\text{Gal}(K/F)$ of

$$\langle\sigma_1\rangle\backslash\text{Gal}(K/F)/\langle\sigma_2\rangle.$$

We assume that the class containing the identity is represented by 1.

- For any σ_0, take $B_{\text{inv}}(\sigma_0)$ to be the subset of $B(\sigma_0, \sigma_0)$ of elements τ for which τ^{-1} represents the same class. We assume the set $B(\sigma_0, \sigma_0)$ is chosen so any τ in $B_{\text{inv}}(\sigma_0)$ satisfies
$$\tau^2 \in \langle \sigma_0 \rangle.$$
- The map sending the class of τ to τ^{-1} acts freely on $B(\sigma_0, \sigma_0) - B_{\text{inv}}(\sigma_0)$. Take $B_{1/2}(\sigma_0)$ to be a subset of $B(\sigma_0, \sigma_0) - B_{\text{inv}}(\sigma_0)$ containing one representative from each orbit of this action. We choose the set $B(\sigma_0, \sigma_0)$ so we have
$$B(\sigma_0, \sigma_0) = B_{\text{inv}}(\sigma_0) \cup B_{1/2}(\sigma_0) \cup B_{1/2}(\sigma_0)^{-1}.$$

Proposition 10.5. *In the above context,*

$$\begin{aligned}
&\langle (q_s)_s,\, (r_s)_s \rangle_\chi \\
=&\sum_{s\in S} \text{inv}_{\mathfrak{p}_s} \left(\mathfrak{B}^{\text{nc}}_{M,F,\overline{\mathfrak{p}}_s}(q_s \cup_{\mathbb{F}} x_s) \cup \delta'_{\chi_0, G_{F,\overline{\mathfrak{p}}_s}}(r_s) \right) \\
&- \sum_{s\in S} \iota_R(r_s) \cup ((q_s \cup_{\mathbb{F}} x_s) \otimes x_s) \otimes a_1^{\text{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_s) \\
&+ \sum_{s,t\in S} \iota_R(r_s) \cup \sum_{\tau \in B(\sigma_s, \sigma_t)} ((\tau q_t - q_s) \cup_{\mathbb{F}} \tau x_t) \otimes x_s \otimes a_\tau^{\text{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_t) \\
=&-\sum_{s\in S} \text{inv}_{\mathfrak{p}_s} \left(\delta_{\chi_0, G_{F,\overline{\mathfrak{p}}_s}}(q_s) \cup \mathfrak{B}^{\text{nc}}_{N'[\omega],F,\overline{\mathfrak{p}}_s}(r_s \cup_{\mathbb{F}} x_s) \right) \\
&+ \sum_{s,t\in S} \iota_R(r_s) \cup \sum_{\tau \in B(\sigma_s, \sigma_t)} ((\tau q_t - q_s) \cup_{\mathbb{F}} \tau x_t) \otimes x_s \otimes a_\tau^{\text{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_t).
\end{aligned}$$

Proof. We first note that Proposition 10.2 allows us to rewrite $\langle (q_s)_s,\, (r_s)_s \rangle_\chi$ in the form

$$\begin{aligned}
&\sum_{s\in S} \text{inv}_{\mu_\ell, F, \overline{\mathfrak{p}}_s} \left(\left(\phi - \delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s) \right) \cup \delta'_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(r_s) \right) \\
=&\sum_{s\in S} \text{inv}_{\mu_\ell, F, \overline{\mathfrak{p}}_s} \left(\left(\phi - \delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s) \right) \cup \left(r_s \cup_{\mathbb{F}} \mathfrak{B}^{\text{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_s}(x_s) \right) \right).
\end{aligned}$$

This allows us to use the same strategy for the second claimed identity in the proposition that we use with the first identity.

We will need one basic properties of the symbols $\mathfrak{L}^{\text{nc}}$. Take M_1, M_2, M_3 to be three $\text{Gal}(K/F)$ modules of exponent ℓ, and take $\overline{\mathfrak{p}}$ and $\overline{\mathfrak{q}}$ to be primes of $\overline{F}$ not over $\mathscr{V}_0$. Choose

$$m_1 \in M_1(-1)^{G_{F,\overline{\mathfrak{p}}}}, \quad m_2 \in M_2(-1)^{G_{F,\overline{\mathfrak{q}}}}, \quad m_3 \in M_3^{G_{F,\overline{\mathfrak{p}}}},$$

and take

$$c_1 = \overline{\mathfrak{B}^{\text{nc}}_{M_1,F,\overline{\mathfrak{p}}}(m_1)}, \quad c_2 = \overline{\mathfrak{B}^{\text{nc}}_{M_1,F,\overline{\mathfrak{p}}}(m_2)}, \quad c_3 = m_3.$$

Given a permutation i_1, i_2, i_3 of $\{1,2,3\}$, take

$$\pi_{i_1,i_2,i_3} : (M_1 \otimes M_2)(-1)_{G_{F,\overline{\mathfrak{p}}}} \otimes M_3^{G_{F,\overline{\mathfrak{p}}}} \longrightarrow (M_{i_1} \otimes M_{i_2} \otimes M_{i_3})(-1)_{G_{F,\overline{\mathfrak{p}}_s}}$$

to be given by the correct permutation of coordinates. Then, for any such permutation,

$$\begin{aligned} &\text{inv}_{M_{i_1}\otimes M_{i_2}\otimes M_{i_3},F,\overline{\mathfrak{p}}}\left(c_{i_1} \cup c_{i_2} \cup c_{i_3}\right) \\ &\qquad = \begin{cases} \pi_{i_1,i_2,i_3}\left(\mathfrak{L}^{\text{nc}}_{M_1\otimes M_2/F}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})(m_1,m_2)\otimes c_3\right) & \text{if } i_1 < i_2 \\ -\pi_{i_1,i_2,i_3}\left(\mathfrak{L}^{\text{nc}}_{M_1\otimes M_2/F}(\overline{\mathfrak{p}},\overline{\mathfrak{q}})(m_1,m_2)\otimes c_3\right) & \text{if } i_1 > i_2. \end{cases} \end{aligned}$$

This is best verified at the level of cocycles. The appearance of a minus sign is a consequence of the skew commutativity of cup product.

We have a commutative diagram

$$\begin{array}{ccccc} N[\omega]\otimes R\otimes \mathbb{F} & \xrightarrow{(\text{Id},\, P_{\mathbb{F}})} & N[\omega]\otimes N'[\omega] & & \\ \downarrow & & & \searrow^{(8.7)} & \\ R\otimes N[\omega]\otimes \mathbb{F} & \xrightarrow{(-\iota_R,\,\text{Id})} & \text{Hom}\left(N[\omega]\otimes\mathbb{F},\,\mu_\ell\right)\otimes\left(N[\omega]\otimes\mathbb{F}\right) & \longrightarrow & \mu_\ell, \end{array}$$

where the vertical map is given by transposing the first two coordinates and the final horizontal map is the standard pairing. We note that the minus sign in the map $(\text{Id}, -\iota_R)$ is

essential for this diagram to commute, as we have

$$((\zeta - 1)\phi)\left(\tfrac{t}{\ell}\right) = \phi\left((\zeta^{-1} - 1)\left(\tfrac{t}{\ell}\right)\right).$$

Having noted this, the proposition is a consequence of Proposition 2.11. □

Remark 10.6. An attentive reader may note that the second identity of the proposition can alternatively be proved as a consequence of the first identity, Proposition 10.3, and the sixth part of Proposition 2.12. Because Proposition 10.3 is counterintuitive, we have decided this redundancy in our presentation is worth preserving.

The full form of Proposition 10.5 has a couple important uses, as we will see in the subsequent sections. However, the following consequence will tend to be far more important, as it lets us easily characterize ignorable pairs.

Proposition 10.7. *In the above situation, choose $s \in S$, and take X_s to be a set of primes of $\overline{F}$ not over $\mathscr{V}_0$ whose Frobenius elements project to σ_s. Fix ϕ_0, $(q_s)_s$, $(r_s)_s$, and $(x_s)_s$ as above, and take*

$$\langle \phi,\ (r_s)_s \rangle_\chi \left[\overline{\mathfrak{p}}_s = \overline{\mathfrak{p}}\right]$$

to be the result of the pairing after replacing each $\overline{\mathfrak{p}}_s$ in (8.9) *and* (8.8) *with $\overline{\mathfrak{p}}$. Define*

$$c(t,\tau) = \begin{cases} -1 & \text{if } s \neq t,\ \tau \in B(\sigma_s, \sigma_t) \ \text{ or } \ s = t,\ \tau \in B_{1/2}(\sigma_s) \\ -\frac{1}{2} & \text{if } s = t,\ \tau \in B_{\text{inv}}(\sigma_s), \ \text{ and } \ \ell \neq 2 \\ 0 & \text{otherwise.} \end{cases}$$

Then there is some $C_0 \in \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$ so

$$\begin{aligned} &\langle \phi,\ (r_s)_s \rangle_\chi \left[\overline{\mathfrak{p}}_s = \overline{\mathfrak{p}}\right] \\ &\quad = C_0 + \sum_{t,\tau} c(t,\tau) \cdot \iota_R(r_s - \tau r_t) \cup (q_s - \tau q_t) \cup_{\mathbb{F}} x_s \otimes \tau x_t \otimes a_\tau^{\text{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}_t) \end{aligned}$$

for all $\overline{\mathfrak{p}} \in X_s$.

Proof. This follows from the previous proposition and the reciprocity properties given in Proposition 2.12. □

10.3. **Some cancellable pairs.** In this section, we will give one basic recipe for constructing cancellable pairs $((q_s)_s, (r_s)_s)$ in the context of (8.12).

Notation 10.8. With N as above, take M_1 to be a G_F submodule of M, and take

$$\beta : M_1 \to N'[\omega]$$

to be a G_F-equivariant homomorphism. We assume this map is alternating, in the sense that

$$\beta(q) \cdot q = 0 \quad \text{in } \ \mu_\ell \ \text{ for all } q \in M_1.$$

Taking Q_1 to be the subset of $N[\omega^2]/N[\omega]$ corresponding to M_1 under tensoring with $\mathbb{F}$, we write $\overline{\beta}$ for the corresponding map $\overline{\beta} : Q_1 \to R$.

We call (M_1, β) *cancellable* if there is some $\sigma_0 \in G_1$ and some $q_A, q_B \in Q_1^{\langle \sigma_0 \rangle}$ so that

$$(\delta'_{\langle \sigma_0 \rangle} \circ \overline{\beta} - \beta_* \circ \delta_{\sigma_0})(q_A) \cup q_B \neq 0 \quad \text{in } \ H^1(\langle \sigma_0 \rangle, \mathbb{F}^\vee)$$

Given (M_1, β), we can define a quadratic form

$$f_\beta : \bigoplus_{s \in S} H^0(\langle \sigma_s \rangle, Q_1) \longrightarrow \tfrac{1}{\ell}\mathbb{Z}/\mathbb{Z}$$

by

$$f_\beta\big((q_s)_s\big) = \big\langle (q_s)_s, (\overline{\beta}(q_s))_s \big\rangle_\chi,$$

where χ is chosen from a fixed tuple set of twists X as in Section 8.3. Per Proposition 10.7, this form does not depend on χ, so the associated pairs $(q_s)_s, (\overline{\beta}(q_s))_s$ are not ignorable. But, if M_1, β is cancellable, the pairs tend to be cancellable; if $\mathscr{Q}_1$ is a vector space of

small codimension in the domain of f_β, we tend to find that the sum

$$\sum_{(q_s)_s \in \mathscr{Q}_1} f_\beta((q_s)_s)$$

is small.

To prove this, will prove that the associated bilinear form

$$B_\beta : \bigoplus_{s\in S} H^0(\langle\sigma_s\rangle,\, Q_1) \otimes \bigoplus_{s\in S} H^0(\langle\sigma_s\rangle,\, Q_1) \;\longrightarrow\; \tfrac{1}{\ell}\mathbb{Z}/\mathbb{Z}$$

given by

$$\begin{aligned} B_\beta\big((q_{1s})_s, (q_{2s})_s\big) &= f_\beta((q_{1s}+q_{2s})_s) - f_\beta((q_{1s})_s) - f_\beta((q_{2s})_s) \\ &= \big\langle (q_{1s})_s, (\overline{\beta}(q_{2s}))_s \big\rangle_\chi + \big\langle (q_{2s})_s, (\overline{\beta}(q_{1s}))_s \big\rangle_\chi \end{aligned}$$

has large rank.

Proposition 10.9. *In the context of Notation 10.8, suppose (M_1, β) is cancellable. Then the bilinear form B_β has rank at least*

$$\tfrac{1}{\ell}\left(\#\big\{s \in S \,:\, \sigma_s = \sigma_0\big\} - 1\right),$$

with σ_0 chosen among the tuples (σ_0, q_A, q_B) demonstrating that (M_1, β) is cancellable.

Remark 10.10. This lower bound on the rank of B_β could be improved without too much effort, but we have no need for such an improved estimate.

Proof. If no s_0 satisfies $\sigma_{s_0} = \sigma_0$, the statement is vacuous. So choose an s_0 so that the set

$$S_0 = \big\{s \in S - \{s_0\} \,:\, \sigma_s = \sigma_0 \text{ and } x_s \equiv x_{s_0} \bmod p \cdot \mathbb{F}(-1)\big\}$$

has maximal cardinality. In particular, this set has size at least the rank bound given in proposition statement.

For $s_1 \in S_0$, define elements

$$E^A(s_1) = (q'_s)_s \quad \text{with} \quad q'_s = \begin{cases} q_A & \text{if } s = s_1 \\ -q_A & \text{if } s = s_0 \\ 0 & \text{otherwise;} \end{cases}$$

$$E^B(s_1) = (q'_s)_s \quad \text{with} \quad q'_s = \begin{cases} q_B & \text{if } s = s_1 \\ 0 & \text{otherwise.} \end{cases}$$

We claim that

$$B_\beta\left(E^A(s_1), E^B(s_2)\right) \quad \text{is} \quad \begin{cases} \neq 0 & \text{if } s_1 = s_2 \\ = 0 & \text{otherwise.} \end{cases} \tag{10.4}$$

This will imply that B_Γ has rank at least $|S_0|$, giving the result.

The claim (10.4) is a consequence of Proposition 10.5 and Proposition 2.12. First, suppose that $s_1 \neq s_2$. Then, using the abuse of notation $\overline{\beta}E^B(s_2)$, we have

$$\begin{aligned} &\left\langle E_A(s_1), \overline{\beta}E_B(s_2)\right\rangle_\chi \\ &\quad = \iota_R(\overline{\beta}(q_B)) \cup \sum_{\tau \in B(\sigma_0,\sigma_0)} \tau q_A \cup \tau x_{s_0} \otimes x_{s_0} \otimes (a^{\mathrm{nc}}_\tau(\overline{\mathfrak{p}}_{s_2}, \overline{\mathfrak{p}}_{s_1}) - a^{\mathrm{nc}}_\tau(\overline{\mathfrak{p}}_{s_2}, \overline{\mathfrak{p}}_{s_0})) \end{aligned}$$

and

$$\begin{aligned} &\left\langle E_B(s_2), \overline{\beta}E_A(s_1)\right\rangle_\chi \\ &\quad = \iota_R(\overline{\beta}(q_A)) \cup \sum_{\tau \in B(\sigma_0,\sigma_0)} \tau q_B \cup \tau x_{s_0} \otimes x_{s_0} \otimes (a^{\mathrm{nc}}_\tau(\overline{\mathfrak{p}}_{s_1}, \overline{\mathfrak{p}}_{s_2}) - a^{\mathrm{nc}}_\tau(\overline{\mathfrak{p}}_{s_0}, \overline{\mathfrak{p}}_{s_1})). \end{aligned}$$

Per Proposition 2.12, these sum to zero.

Now, for the case $s_1 = s_2 = s$, we calculate

$$\begin{aligned}
&\left\langle E_A(s), \overline{\beta} E_B(s) \right\rangle_\chi \\
&\quad = \mathrm{inv}_{\mathfrak{p}_s} \left(\mathfrak{B}^{\mathrm{nc}}_{M,F,\overline{\mathfrak{p}}_s}(q_A \cup_{\mathbb{F}} x_s) \cup \delta'_{\chi_0, G_{F,\overline{\mathfrak{p}}_s}}(\overline{\beta}(q_B)) \right) \\
&\quad - \iota_R(\overline{\beta}(q_B)) \cup q_A \cup x_s \otimes x_s \otimes a_1^{\mathrm{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_s) \\
&\quad + \iota_R(\overline{\beta}(q_B)) \cup \sum_{\tau \in B(\sigma_0, \sigma_0)} \tau q_A \cup \tau x_{s_0} \otimes x_{s_0} \otimes (a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_s) - a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_{s_0}))
\end{aligned}$$

and

$$\begin{aligned}
&\left\langle E_B(s), \overline{\beta} E_A(s) \right\rangle_\chi \\
&\quad = -\mathrm{inv}_{\mathfrak{p}_s} \left(\delta_{\chi_0, G_{F,\overline{\mathfrak{p}}_s}}(q_A) \cup \mathfrak{B}^{\mathrm{nc}}_{N'[\omega],F,\overline{\mathfrak{p}}_s} \left(\overline{\beta}(q_B) \right) \right) \\
&\quad + \iota_R(\overline{\beta}(q_A)) \cup \sum_{\tau \in B(\sigma_0, \sigma_0)} \tau q_B \cup \tau x_{s_0} \otimes x_{s_0} \otimes (a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_s) - a_\tau^{\mathrm{nc}}(\overline{\mathfrak{p}}_{s_0}, \overline{\mathfrak{p}}_s)).
\end{aligned}$$

The second and third terms of the first expression canel with the second term of the second expression, with the extra appearance of $a_1^{\mathrm{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_s)$ merited by the unusual property given as the final statement of Proposition 2.12, part six. The first terms of each expression sum to something nonzero by the assumption of the proposition, giving the claim (10.4) and finishing the proof. □

The above proposition admits a converse, where B_β can be proved to be of small rank if $\overline{\beta}$ commutes with the connecting maps. In the examples we consider, this situation will only arise when β can be lifted to an alternating map from the divisible module N to N', where more specific propositions can be made.

10.4. **Main-term pairs.** Proposition 10.9 admits a converse, where B_β can be proved to be of small rank if $\overline{\beta}$ commutes with the connecting maps. Such a statement is insufficient for our purposes, as forms of small positive rank and the zero form will contribute differently to moments. Instead, in the special cases we can handle, we want to prove that

non-cancellable (M_1, β) give rise to main-term pairs. The two cases we are interested in are the alternating and non-alternating case of Section 9.1.

Proposition 10.11. *Suppose N is a twistable module in either the non-alternating case or the alternating case. Choose $\chi \in \mathbb{X}_F$, and recall the boundary maps $\delta_{G_F}, \delta'_{G_F}$ defined above. Then, for $\chi \in \mathbb{X}_F$, we have*

$$\delta_{\chi, G_F}\left(H^0(G_F, N[\omega^2]/N[\omega])\right) \subseteq \text{Sel}^{\omega}(N^{\chi}).$$

Furthermore, if r_0 is $H^0(G_F, N'[\omega^2]/N'[\omega])$, and if ϕ has the form given in (8.9) *and satisfies the local conditions at $\mathscr{V}_0$, we have*

$$\langle \phi, (r_0)_s \rangle_{\chi} = 0,$$

where $(r_0)_s$ denotes the tuple whose s coordinate is r for all $s \in S$.

Proof. The first part is immediate from the definitions. For the second part, we note that, for $v \in \mathscr{V}_0$,

$$\phi \cup \delta'_{\chi, G_v}(r_0) = 0,$$

as a consequence of the assumption that W_v is ℓ-divisible. The part then follows from Poitou-Tate duality, and in particular from the fact that (10.5) is the zero map. □

This deals with all the main terms that appear in the non-alternating case. In the alternating case, we have extra main-term pairs.

We first make the following observations. First, given a twistable module N with Selmer structure $(W_v)_v$, the module $N^{\oplus a}$ is also a twistable module with a standard choice of Selmer structure in $(W_v^{\oplus a})_v$. The natural analogue of the pairing $\langle\ ,\ \rangle_{\chi}$ for this direct sum is a pairing $\langle\ ,\ \rangle_{N^{\oplus a}, \chi}$ defined by

$$\langle (\phi_1, \ldots, \phi_a), (r_{1s}, r_{2s}, \ldots, r_{as})_s \rangle_{N^{\oplus a}, \chi} = \sum_{i \leq a} \langle \phi_i, (r_{is})_s \rangle.$$

Proposition 10.12. *Suppose N is in the alternating case, and take*

$$\beta : N \to N'$$

to be the equivariant alternating isomorphism given in Notation 9.8.

Given any nonnegative integer a, and given a symmetric $a \times a$ matrix T with coefficients in $\mathbb{Z}_\ell$, we can define an alternating map

$$\beta_T : N^{\oplus a} \cong N \otimes \mathbb{Z}_\ell^a \xrightarrow{\beta \otimes T} N' \otimes \mathbb{Z}_\ell^a \cong (N^{\oplus a})'.$$

Take χ as in the notation (8.8)*, and choose*

$$\phi = \phi_0 + \sum_{s \in S} \mathfrak{B}^{\mathrm{nc}}_{M^{\oplus a}, F, \overline{\mathfrak{p}}_s}(q_s \cup_{\mathbb{F}} x_s).$$

We assume this obeys the local conditions for $N^{\oplus a}$ at all places in $\mathscr{V}_0$. Then

$$\left\langle \phi,\ \left(\overline{\beta_T}(q_s)\right)_s \right\rangle_{N^{\oplus a}, \chi} = 0.$$

Proof. A symmetric matrix over any ring can be written as a sum of matrices $LL^\top$ with L another matrix defined over the ring. By decomposing the matrices in this way, we find that it suffices to prove the proposition in the case $a = 1$ with $\beta_T = \beta$.

Take q to be the form defined in (9.10). We now claim that

$$\mathrm{inv}_{\mu_\ell, F, \overline{\mathfrak{p}}_s}\left(\phi \cup \delta'_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(\overline{\beta}(q_s))\right) \ = \ -\mathrm{inv}\left(q_{G_{F,\overline{\mathfrak{p}}_s}}(\phi)\right).$$

To do this, we first note that

$$q_{G_{F,\overline{\mathfrak{p}}_s}}(\delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s)) = q_{G_{F,\overline{\mathfrak{p}}_s}}(\phi - \delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s)) = 0,$$

as a consequence of Proposition 3.3 and the fact that $\phi - \delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s)$ is unramified. From Proposition 3.2, we then get that

$$q_{G_{F,\overline{\mathfrak{p}}_s}}(\phi) = -\left(\phi - \delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s)\right) \cup \beta_* \delta_{\chi, G_{F,\overline{\mathfrak{p}}_s}}(q_s)$$

and this gives the claim. The proposition then follows from the definition (8.10) and Poitou-Tate duality, in the specific sense that the sum

$$\sum_{v \text{ of } F} \text{inv}_v : H^2\left(G_F, \overline{F}^{\times}\right) \longrightarrow \mathbb{Q}/\mathbb{Z} \tag{10.5}$$

is the zero map. □

10.5. **The space $\mathbf{Q}((q_s)_s)$.** Take N to be a twistable module as above, with notation as throughout this section. We do not assume that we are in either case of Section 9.1.

Definition 10.13. Given $(q_s)_s$ in $\mathscr{Q}$, we take $\mathbf{Q}((q_s)_s)$ to be the subspace of Q spanned by elements of the form

$$\tau_1 q_s - \tau_2 q_t \quad \text{for } s, t \in S,\ \tau_1, \tau_2 \in G_F.$$

If Q_1 is a G_F submodule of Q, we take $Q_1^{\perp}$ to be the orthogonal subspace of R with respect to the natural pairing

$$Q \times R \longrightarrow (\mathbb{F}/\ell\mathbb{F} \otimes \mathbb{F}/\ell\mathbb{F})^{\vee}.$$

We then take

$$\mathscr{R}(Q_1) = \bigoplus_{s \in S} H^0\left(\langle \sigma_s \rangle,\, Q_1^{\perp}\right).$$

Taking M_1 to be the natural image of $Q_1 \otimes \mathbb{F}$ in M, the exact sequence

$$0 \to M/M_1 \to (N/M_1)[\omega] \to Q_1 \to 0 \tag{10.6}$$

gives rise to a connecting map

$$\rho_H : H^0(H, Q_1) \to H^1(H, M/M_1)$$

for any closed subgroup H. We take

$$\mathscr{Q}_0(Q_1) = \bigoplus_{s\in S} \ker \rho_{\langle\sigma_s\rangle}.$$

The long exact sequence applied to (10.6) gives

$$\#\mathscr{Q}_0(Q_1) = \prod_{s\in S} \frac{\#H^0(\langle\sigma_s\rangle,\ N/M_1[\omega])}{\#H^0(\langle\sigma_s\rangle,\ M/M_1[\omega])}. \tag{10.7}$$

In addition, from the commutative diagram with exact rows

$$\begin{array}{ccccc} M & \longrightarrow & N[\omega^2] & \xrightarrow{\pi} & Q \\ \| & & \uparrow & & \uparrow \\ M & \longrightarrow & \pi^{-1}(Q_1) & \longrightarrow & Q_1 \\ \downarrow & & \downarrow & & \| \\ M/M_1 & \longrightarrow & (N/M_1)[\omega] & \longrightarrow & Q_1, \end{array}$$

we have a commutative square

$$\begin{array}{ccc} H^0(H, Q_1) & \xrightarrow{\rho_H} & H^1(H, M/M_1) \\ \downarrow & & \uparrow \\ H^0(H, Q) & \xrightarrow{\delta_H} & H^1(H, M) \end{array}$$

for any closed subgroup H, where the vertical maps come functorially from the standard inclusion and projections. For $s \in S$, we note that

$$\ker\left(H^1(G_{F,\overline{\mathfrak{p}}_s}/I_{F,\overline{\mathfrak{p}}_s}, M) \to H^1(G_{F,\overline{\mathfrak{p}}_s}/I_{F,\overline{\mathfrak{p}}_s}, M/M_1)\right) \quad \text{and} \quad H^1(I_{F,\overline{\mathfrak{p}}_s}, M_1^{\perp})^{G_{F,\overline{\mathfrak{p}}_s}}$$

anihilate each other with respect to the natural pairing

$$H^1(G_{F,\overline{\mathfrak{p}}_s}/I_{F,\overline{\mathfrak{p}}_s}, M) \otimes H^1(I_{F,\overline{\mathfrak{p}}_s}, N'[\omega]) \to H^2(G_{F,\overline{\mathfrak{p}}_s}, \overline{F}^{\times}).$$

We then have the following:

Proposition 10.14. *Suppose we are in the situation considered above, and take Q_1 a G_F-submodule of Q as above. Choose $(q_s)_s \in \mathscr{Q}$ so that $q_s \in Q_1$ for all $s \in S$. Then*

$$\langle (q_s)_s, (r_s)_s \rangle_\chi = 0 \quad \textit{for all } (r_s)_s \in \mathscr{R}(Q_1)$$

if and only if $(q_s)_s \in \mathscr{Q}_0(Q_1)$.

Proof. Given the above discussion, this follows from Proposition 10.5. □

11. IGNORABLE PAIRS

We have already seen two of the types of pairs $(q_s)_s, (r_s)_s$ that appear in the moment calculation (8.12). In this section, we consider ignorable pairs, where the sum

$$\sum_{\chi \in X} \langle (q_s)_s, (r_s)_s \rangle_\chi$$

can be forced to be small. Our techniques for forcing this sum to be small come from analytic number theory, and this somewhat limits what we can say. Ideally, given Proposition 10.7, we would be able to say that $(q_s)_s, (r_s)_s$ is ignorable whenever

$$(r_s - \tau_0 r_t) \cdot (q_s - \tau_0 q_t) \neq 0$$

for some choice of distinct $s, t \in S$ and some choice of $\tau_0 \in G_F$. For the tuple sets that come from decomposing $\mathbb{X}_F(H)$, this is too strong. Instead, we take the following notation.

Notation 11.1. Take a twistable module N, an indexing set S, and a set of G_1 elements $(\sigma_s)_s$ as above. Furthermore, fix a partition of S into three disjoint subsets S_{sm}, S_{med}, and S_{lg}.

Definition 11.2. Given $\big((q_s)_s, (r_s)_s\big)$ in $\mathscr{Q} \times \mathscr{R}$, we say that the pair is *ignorable by the large sieve* if there are distinct indices s, t in $S_{\text{med}} \cup S_{\text{lg}}$ and there is some τ_0 in G_F so that

$$(r_s - \tau_0 r_t) \cdot (q_s - \tau_0 q_t) \neq 0. \tag{11.1}$$

We say the pair is *ignorable by Chebotarev* if there is some $s \in S_{\text{lg}}$ satisfying

$$(r_s - \tau r_s) \cdot (q_s - \tau q_s) = 0 \quad \text{for all } \tau \in G_F \tag{11.2}$$

and there is some t in S_{sm} and τ_0 in G_F so (11.1) holds.

If either condition is satisfied, we call $\big((q_s)_s, (r_s)_s\big)$ *ignorable*.

Remark 11.3. The reasonability of this definition comes from Proposition 10.7. The condition (11.2) is needed because the Chebotarev density theorem is believed to be insufficient to prove equidistribution results for most kinds of spin, which are the terms of the form $a_\tau^{\text{nc}}(\overline{\mathfrak{p}}_s, \overline{\mathfrak{p}}_s)$.

The slight complication of the definition of an ignorable pair makes the resultant theory substantially more cumbersome. We turn to it now.

11.1. **Characterizing non-ignorable pairs.**

Definition 11.4. Given $(q_s)_s$ in $\mathscr{Q}$, we call $s_0 \in S_{\text{lg}}$ a *pariah index* for $(q_s)_s$ if there are not disjoint subsets S_1, S_2 of $S_{\text{lg}} - \{s_0\}$ and some choice of

$$(a_{1s})_{s \in S_1} \in \bigoplus_{s \in S_1} \mathbb{F}_\ell \quad \text{and} \quad (a_{2s})_{s \in S_2} \in \bigoplus_{s \in S_2} \mathbb{F}_\ell$$

satisfying

$$\sum_{s \in S_1} a_{1s} = \sum_{s \in S_2} a_{2s} = 1 \quad \text{and} \quad \sum_{s \in S_1} a_{1s} q_s = \sum_{s \in S_2} a_{2s} q_s = q_{s_0}.$$

We denote the set of pariahs by $S_{\text{par}}((q_s)_s)$.

We call s_0 an *m/l pariah index* if s_0 lies in $S_{\text{med}} \cup S_{\text{lg}}$ and the condition given above is satisfied with S_{lg} replaced by $S_{\text{med}} \cup S_{\text{lg}}$. We denote the set of m/l pariahs by $S_{\text{m, par}}$.

The possibility of pariah indices make bilinear sum computations more annoying than they might otherwise be. Fortunately, there cannot be too many of them, and their impact on the general moment (8.12) can typically be made negligible. We will return to this second claim later, but the first claim follows from the next proposition.

Proposition 11.5. *Taking g to be the corank of N, and given $(q_s)_s$ in $\mathscr{Q}$, we have*

$$\#S_{\text{par}}((q_s)_s) \leq 2g + 2$$

Proof. This statement is vacuous if S_{lg} has fewer than $g + 2$ elements. So we assume $\#S_{\text{lg}} \geq g + 2$.

Choose $s_0 \in S_{\text{lg}}$, and choose a sequence $s_1, \ldots, s_r \in S_{\text{lg}}$ so that

$$q_{s_1} - q_{s_0},\ \ldots,\ q_{s_r} - q_{s_0}$$

gives a basis for the $\mathbb{F}_\ell$-vector space spanned by all elements of the form $q_s - q_t$ with $s, t \in S_{\text{lg}}$.

Take $S'_{\text{lg}} = S_{\text{lg}} - \{s_0, \ldots, s_r\}$. Choose t_0 in S'_{lg}, and choose a sequence $t_1, \ldots, t_{r'} \in S_{\text{lg}}$ so that

$$q_{t_1} - q_{t_0},\ \ldots,\ q_{t_{r'}} - q_{t_0}$$

gives a basis for the space spanned by all elements of the form $q_s - q_t$ with $s, t \in S'_{\text{lg}}$.

We then have $r \leq g$ and $r' \leq g$, and we also have

$$S_{\text{par}}((q_s)_s) \subseteq \{s_0, \ldots, s_r\} \cup \{t_0, \ldots, t_{r'}\},$$

giving the proposition. □

The same proposition holds for $S_{\text{m, par}}$ using the same logic.

Definition 11.6. Given $S' \subseteq S$ and $(q_s)_s \in \mathscr{Q}$, take

$$\mathbf{Q}(S') = \mathbf{Q}(S',\, (q_s)_s)$$

to be the vector subspace of $\mathbf{Q}((q_s)_s)$ generated by the elements

$$\tau_1 q_s - \tau_2 q_t \quad \text{for } s,t \in S',\ \tau_1, \tau_2 \in G_F.$$

Given $(q_s)_s$, take

$$S_{\text{npar}} = S_{\text{lg}} - S_{\text{par}},\ \ S_{\text{m,npar}} = S_{\text{lg}} \cup S_{\text{med}} - S_{\text{m, par}}.$$

We call $(q_s)_s$ *unlawful* if $\mathbf{Q}(S_{\text{npar}}, (q_s)_s)$ is a proper submodule of $\mathbf{Q}(S, (q_s)_s)$.

Proposition 11.7. *In the above situation, suppose the pair $\big((q_s)_s, (r_s)_s\big)$ in $\mathscr{Q} \times \mathscr{R}$ is not ignorable by the large sieve. Then the equation*

$$\Gamma(\tau_1 q_s - \tau_2 q_t) \equiv \tau_1 r_s - \tau_2 r_t \quad \textit{for all } s,t \in S',\ \tau_1, \tau_2 \in G_F$$

defines G_F-equivariant homomorphisms

$$\begin{aligned} \Gamma_{\text{m,npar}} &: \mathbf{Q}(S') \to R/\mathbf{Q}(S_{\text{lg}} \cup S_{\text{med}})^{\perp} \quad \textit{with } S' = S_{\text{m,npar}} \\ \Gamma_{\text{m, l}} \quad &: \mathbf{Q}(S') \to R/\mathbf{Q}(S_{\text{m,npar}})^{\perp} \qquad \textit{with } S' = S_{\text{lg}} \cup S_{\text{med}}, \end{aligned}$$

with $\Gamma_{\text{m, npar}}$ alternating.

If the pair is also not ignorable by Chebotarev, the same equation defines G_F-equivariant homomorphisms

$$\begin{aligned} \Gamma_{\text{npar}} &: \mathbf{Q}(S') \to R/\mathbf{Q}(S)^{\perp} \qquad \textit{with } S' = S_{\text{npar}} \\ \Gamma \quad &: \mathbf{Q}(S') \to R/\mathbf{Q}(S_{\text{npar}})^{\perp} \quad \textit{with } S' = S, \end{aligned}$$

with Γ_{npar} alternating.

Remark 11.8. If $(q_s)_s$ is not unlawful, these four maps are all equal.

Proof. Assume to start that $\big((q_s)_s, (r_s)_s\big)$ is non-ignorable by the large sieve.

Given

$$a : S_{\text{med}} \cup S_{\text{lg}} \to \mathbb{F}_\ell \quad \text{satisfying} \quad \sum_{s \in S_{\text{med}} \cup S_{\text{lg}}} a_s = 0$$

and any function $\tau : S \to G_F$, we have

$$\left(\sum_{s \in S_{\text{med}} \cup S_{\text{lg}}} a_s \tau_s r_s \right) \cdot \left(\sum_{s \in S_{\text{med}} \cup S_{\text{lg}}} a_s \tau_s q_s \right) = 0, \tag{11.3}$$

as this sum can be rewritten in the form

$$- \sum_{\{s,t\} \subseteq S_{\text{med}} \cup S_{\text{lg}}} a_s a_t \left(\tau_s r_s - \tau_t r_t\right) \cdot \left(\tau_s q_s - \tau_t q_t\right).$$

If $s_0 \in S_{\text{lg}} \cup S_{\text{med}}$ is not an m/l pariah index, we can choose S_1, S_2, a_1, and a_2 as in Definition 11.4 so that we have

$$q_{s_0} = \sum_{s \in S_1} a_{1s} q_s = \sum_{s \in S_2} a_{2s} q_s.$$

Choosing $\tau \in G_F$, we can show

$$\left(r_{s_0} - \sum_{s \in S_1} a_{1s} \tau r_s \right) \cdot \left(q_{s_0} - \sum_{s \in S_1} a_{1s} \tau q_s \right) = 0,$$

$$\left(\sum_{s \in S_1} a_{1s} \tau r_s - \sum_{s \in S_2} a_{2s} r_s \right) \cdot \left(\sum_{s \in S_2} a_{2s} q_s - \sum_{s \in S_1} a_{1s} \tau q_s \right) = 0,$$

$$\left(-\tau r_{s_0} + \sum_{s \in S_2} a_{2s} r_s \right) \cdot \left(-\tau q_{s_0} + \sum_{s \in S_2} a_{2s} q_s \right) = 0$$

by applying (11.3) three times. But these sum to give

$$\left(r_{s_0} - \tau r_{s_0}\right) \cdot \left(q_{s_0} - \tau q_{s_0}\right) = 0 \quad \text{for } s_0 \in S_{\text{m,npar}},\ \tau \in G_F. \tag{11.4}$$

Take val : $\mathbb{F}_\ell[G_F] \to \mathbb{F}_\ell$ to be the homomorphism sending $[\sigma]$ to 1 for all σ in G_F. For S' a subset of S, define

$$I(S') = \left\{ (\alpha_s)_s \in \bigoplus_s \mathbb{F}_\ell[G_F] \ : \ \sum_s \mathrm{val}(\alpha_s) = 0 \right\}.$$

Repeating the argument used to prove (11.3) and applying (11.4) as necessary, we can show that, for all $(\alpha_s)_s \in I(S_{\text{m,npar}})$, all $s_1 \in S_{\text{med}} \cup S_{\text{lg}}$, all $s_0 \in S_{\text{m,npar}}$, and any $\tau \in G_F$, we have

$$\left(\tau r_{s_1} - r_{s_0} + \sum_{s \in S_{\text{m,npar}}} \alpha_s r_s \right) \cdot \left(\tau q_{s_1} - q_{s_0} + \sum_{s \in S_{\text{m,npar}}} \alpha_s q_s \right) = 0.$$

By taking the difference with the case given by $s_1 = s_0$, $\tau = 1$, we get

$$(\tau r_{s_1} - r_{s_0}) \cdot \left(\sum_{s \in S_{\text{m,npar}}} \alpha_s q_s \right) = - \left(\sum_{s \in S_{\text{m,npar}}} \alpha_s r_s \right) \cdot (\tau q_{s_1} - q_{s_0}).$$

Except in the case where $S_{\text{m,npar}}$ is empty, we can sum some number of identities of this form together to show

$$\left(\sum_{s \in S_{\text{med}} \cup S_{\text{lg}}} \alpha'_s r_s \right) \cdot \left(\sum_{s \in S_{\text{m,npar}}} \alpha_s q_s \right) = - \left(\sum_{s \in S_{\text{m,npar}}} \alpha_s r_s \right) \cdot \left(\sum_{s \in S_{\text{med}} \cup S_{\text{lg}}} \alpha'_s q_s \right) \tag{11.5}$$

for all $(\alpha_s)_s \in I(S_{\text{m,npar}})$ and $(\alpha'_s)_s \in I(S_{\text{med}} \cup S_{\text{lg}})$. If $S_{\text{m,npar}}$ is empty, (11.5) is vacuously true. The existence and equivariance of $\Gamma_{\text{m,npar}}$ and $\Gamma_{\text{m,l}}$ follow from this equation, as does the alternating property of the former map.

If $\big((q_s)_s, (r_s)_s\big)$ is also non-ignorable by Chebotarev, we can conclude from (11.4) that

$$(\tau r_{s_1} - r_{s_0}) \cdot (\tau q_{s_1} - q_{s_0}) = 0 \quad \text{for all } \ s_1 \in S, \ s_0 \in S_{\text{npar}}, \ \tau \in G_F.$$

Following the same argument as before, we find

$$\left(\sum_{s \in S} \alpha'_s r_s \right) \cdot \left(\sum_{s \in S_{\text{npar}}} \alpha_s q_s \right) = - \left(\sum_{s \in S_{\text{npar}}} \alpha_s r_s \right) \cdot \left(\sum_{s \in S} \alpha'_s q_s \right) \tag{11.6}$$

for all $(\alpha_s)_s \in I(S_{\text{npar}})$ and $(\alpha'_s)_s \in I(S)$. The existence and equivariance of Γ_{npar} and Γ follow from this equation, as does the alternating property of the former map. $\square$

11.2. **Counting non-ignorable pairs.** For our first result, we will fix $(q_s)_s \in \mathscr{Q}$ and give upper bounds on the number of non-ignorable pairs that contain it.

Proposition 11.9. *There is a $C > 0$ determined from just $(K/F, \mathscr{V}_0, \mathbb{F})$ so we have the following:*

Take N to be a twistable module of corank g, and take all other notation as above. Choose $(q_s)_s \in \mathscr{Q}$, and write $\mathbf{M}(S')$ for the image of

$$\mathbf{Q}(S', (q_s)_s) \otimes \mathbb{F}$$

in M for any subset S' of S. Then the number of $(r_s)_s \in \mathscr{R}$ so $\big((q_s)_s, (r_s)_s\big)$ is not ignorable by the large sieve has upper bound

$$\exp(Cg^2) \cdot \prod_{s \in S_{\text{med}} \cup S_{\text{lg}}} \#H^0\big(\langle \sigma_s \rangle,\, M/\mathbf{M}(S_{\text{med}} \cup S_{\text{lg}})\big) \cdot \prod_{s \in S_{\text{sm}}} \#H^0\big(\langle \sigma_s \rangle,\, M\big).$$

The number of $(r_s)_s \in \mathscr{R}$ so $\big((q_s)_s, (r_s)_s\big)$ is not ignorable (by either large sieve or Chebotarev) has upper bound

$$\exp(Cg^2) \cdot \prod_{s \in S_{\text{lg}}} \#H^0\big(\langle \sigma_s \rangle,\, M/\mathbf{M}(S)\big) \cdot \prod_{s \in S_{\text{med}}} \#H^0\big(\langle \sigma_s \rangle,\, M/\mathbf{M}(S_{\text{lg}} \cup S_{\text{med}})\big)$$
$$\cdot \prod_{s \in S_{\text{sm}}} \#H^0\big(\langle \sigma_s \rangle,\, M/\mathbf{M}(S_{\text{npar}})\big).$$

Proof. We first note that, for any G_F submodule $Q_1 \subseteq Q$ and any σ_0 in $G_{F(\mathbb{F}(-1))}$, we have

$$\#H^0\left(\langle \sigma_0 \rangle,\, Q_1^{\perp}\right) \,=\, \#H^0\left(\langle \sigma_0 \rangle,\, M/(Q_1 \otimes \mathbb{F})\right).$$

This follows from the existence of an equivariant perfect pairing

$$M \otimes R \to \text{Hom}(\mathbb{F}, \mu_\ell),$$

from the fact that σ_0 fixes $\mathbb{F}(-1)$, and from the standard equality

$$\#\left(Q_1^{\perp}\right)^{\langle\sigma_0\rangle} = \#\left(Q_1^{\perp}\right)_{\langle\sigma_0\rangle}.$$

To bound the number of $(r_s)_s$ that are not ignorable by the large sieve, we use the existence of the map $\Gamma_{\text{m,npar}}$. Having fixed this map and the value of r_{s_0} for some $s_0 \in S_{\text{m,npar}}$, there are

$$\#H^0\left(\langle\sigma_s\rangle,\, \mathbf{Q}(S_{\text{med}} \cup S_{\text{lg}})^{\perp}\right)$$

consistent choices of r_s for each s in $S_{\text{m,npar}} - \{s_0\}$. The choice of $\Gamma_{\text{m,npar}}$, the value of r_s at the m/l pariahs, and the value of r_{s_0} can then be absorbed by the $\exp(Cg^2)$ term. Accounting for the possible values of r_s for $s \in S_{\text{sm}}$ gives the first estimate.

For the second estimate, we need three of the homomorphisms from Proposition 11.7, using Γ, $\Gamma_{\text{m,npar}}$, and Γ_{npar} to constrict the possibilities of r_s for s in S_{sm}, S_{med}, and S_{lg} respectively. With this setup, the proof follows as before. □

Definition 11.10. We will write S_{jury} for the set of s in S_{lg} for which σ_s equals 1.

The jury indices are key to bounding the number of unlawful $(q_s)_s$ we need to consider, as we will see in the next proposition:

Proposition 11.11. *There is a $C > 0$ determined just from $(K/F, \mathscr{V}_0, \mathbb{F})$ so we have the following:*

Write g for the corank of N. Take $Q_{\min}$ and $Q_{\max}$ to be G_F-submodules of Q, with $Q_{\min}$ properly contained in $Q_{\max}$, and write $M_{\min}$ and $M_{\max}$ for the corresponding subspaces of M. Recall the notation $\mathscr{Q}_0(Q_1)$ from Definition 10.13.

Then the number of $(q_s)_s$ in $\mathscr{Q}_0(Q_{\max})$ that satisfy

$$\mathbf{Q}(S_{\text{npar}}) \subseteq Q_{\min}$$

has upper bound

$$(1+\#S_{\text{lg}})^{Cg}\cdot\exp(Cg^2)\cdot\ell^{(-\#S_{\text{jury}}+\#S_{\text{sm}}\cup S_{\text{med}})\cdot\dim Q_{\max}/Q_{\min}}$$
$$\cdot\prod_{s\in S}\min_{M_{\min}\subseteq M_1\subseteq M_{\max}}\frac{\#H^0\left(\langle\sigma_s\rangle,\,(N/M_1)[\omega]\right)}{\#H^0\left(\langle\sigma_s\rangle,\,(M/M_{\max})[\omega]\right)},$$

with M_1 varying over all G_F modules containing $M_{\min}$ and contained in $M_{\max}$.

Proof. Given a subspace M_1 of M, take $\frac{1}{\omega}M_1$ to be the maximal subspace of $N[\omega^2]$ satisfying

$$\omega\left(\tfrac{1}{\omega}M_1\right)=M_1.$$

Applying the definition of ρ_H from Definition 10.13 with $Q_1=Q_{\max}$, we find that the intersection

$$\ker\rho_{\langle\sigma_s\rangle}\cap H^0(\langle\sigma_s\rangle,\,Q_{\min})$$

is identified as the kernel of the connecting map

$$H^0(\langle\sigma_s\rangle,\,Q_{\min})\to H^1(\langle\sigma_s\rangle,\,M/Q_{\max})$$

corresponding to the standard exact sequence

$$0\to M/M_{\max}\to\tfrac{1}{\omega}M_{\min}/M_{\max}\to Q_{\min}\to 0.$$

In particular, this intersection has size

$$\frac{\#H^0\left(\langle\sigma_s\rangle,\,\frac{1}{\omega}M_{\min}/M_{\max}\right)}{\#H^0\left(\langle\sigma_s\rangle,\,M/M_{\max}\right)}.$$

After absorbing the choice of pariah indices into the $(1+|S_{\text{lg}}|)^{Cg}$ term using Proposition 11.5 and absorbing the choice of q_s at the pariahs and some basepoint into the $\exp(Cg^2)$

term, we find that the count of $(q_s)_s \in \mathscr{Q}_0(Q_{\max})$ satisfying $\mathbf{Q}(S_{\text{npar}}) \subseteq Q_{\min}$ is at most

$$(1+\#S_{\text{lg}})^{Cg} \cdot \exp(Cg^2) \cdot \prod_{s \in S_{\text{sm}} \cup S_{\text{med}}} \frac{\#H^0\left(\langle\sigma_s\rangle,\, \frac{1}{\omega}M_{\max}/M_{\max}\right)}{\#H^0\left(\langle\sigma_s\rangle,\, M/M_{\max}\right)} \cdot \prod_{s \in S_{\text{lg}}} \frac{\#H^0\left(\langle\sigma_s\rangle,\, \frac{1}{\omega}M_{\min}/M_{\max}\right)}{\#H^0\left(\langle\sigma_s\rangle,\, M/M_{\max}\right)}.$$

We now claim that, for all G_F-modules M_1 satisfying $M_{\min} \subseteq M_1 \subseteq M_{\max}$ and all s, we have

$$\#H^0\left(\langle\sigma_s\rangle,\, \tfrac{1}{\omega}M_{\min}/M_{\max}\right) \leq \#H^0\left(\langle\sigma_s\rangle,\, \tfrac{1}{\omega}M_1/M_1\right). \tag{11.7}$$

We first note that the standard inclusion gives us an inequality

$$\#H^0\left(\langle\sigma_s\rangle,\, \tfrac{1}{\omega}M_{\min}/M_{\max}\right) \leq \#H^0\left(\langle\sigma_s\rangle,\, \tfrac{1}{\omega}M_1/M_{\max}\right).$$

Next, from the long exact sequence associated to the exact sequence

$$0 \to M_{\max}/M_1 \to \tfrac{1}{\omega}M_1/M_1 \to \tfrac{1}{\omega}M_1/M_{\max} \to 0$$

and the equality

$$\#H^0(\langle\sigma_s\rangle, M_{\max}/M_1) = \#H^1(\langle\sigma_s\rangle, M_{\max}/M_1),$$

we get the inequality

$$\#H^0\left(\langle\sigma_s\rangle,\, \tfrac{1}{\omega}M_1/M_{\max}\right) \leq \#H^0\left(\langle\sigma_s\rangle,\, \tfrac{1}{\omega}M_1/M_1\right).$$

Combining this with the previous inequality gives (11.7).

To finish the proof of the proposition, we note that we also have

$$\#H^0\left(\langle\sigma_s\rangle,\, \tfrac{1}{\omega}M_{\min}/M_{\max}\right) \geq \frac{1}{\#Q_{\max}/Q_{\min}} \cdot \#H^0\left(\langle\sigma_s\rangle,\, \tfrac{1}{\omega}M_1/M_{\max}\right)$$

for all M_1 as before, with equality when $\sigma_s = 1$. □

11.3. **Bounding moments using non-ignorable pairs.** We now turn to finding bounds for the expression (8.12).

Notation 11.12. Fix a twistable module N, and take X to be a tuple set of twists defined with respect to an indexing set $S = S_{\text{sm}} \cup S_{\text{med}} \cup S_{\text{lg}}$ and G_1-tuple $(\sigma_s)_s$, as in Section 8.3.

Take c_{LS} to be the maximum value taken by the expression

$$\frac{1}{|X|} \cdot \left| \sum_{\chi \in X} \exp\left(2\pi i \cdot \left\langle (q_s)_s,\, (r_s)_s \right\rangle_\chi\right) \right| \tag{11.8}$$

as $(q_s)_s, (r_s)_s$ varies over pairs that are ignorable by the large sieve. If there is no pair ignorable by the large sieve, take $c_{\text{LS}} = 0$.

Similarly, take c_{Cheb} to be the maximum value this expression takes over pairs ignorable by Chebotarev, again taking $c_{\text{Cheb}} = 0$ if there is no such pair.

These maxima are always at most one.

Fix ϕ_0 in $\mathscr{S}_{M/F}(\mathscr{V}_0)$. Our goal is to find upper bounds for

$$\frac{1}{\#\mathscr{R}} \sum_{\chi \in X} \sum_{(q_s)_s \in \mathscr{Q}_1} \sum_{(r_s)_s \in \mathscr{R}} \exp\left(2\pi i \cdot \left(\left\langle \phi_0,\, (r_s)_s \right\rangle_\chi + \left\langle (q_s)_s,\, (r_s)_s \right\rangle_\chi\right)\right) \tag{11.9}$$

for various subsets $\mathscr{Q}_1$ of $\mathscr{Q}$. We note that, if $\mathscr{Q}_2$ is a subset of $\mathscr{Q}_1$ so that

$$q + \mathscr{Q}_1 = \mathscr{Q}_1 \quad \text{for all } q \in \mathscr{Q}_2,$$

and if $\mathscr{Q}_3$ is a set of representatives of the quotient $\mathscr{Q}_1/\mathscr{Q}_2$, we can bound (11.9) by

$$\frac{\#\mathscr{Q}_2}{\#\mathscr{R}} \sum_{\chi \in X} \sum_{(q_s)_s \in \mathscr{Q}_3} \sum_{(r_s)_s \in \mathscr{R}} \exp\left(2\pi i \cdot \left(\left\langle \phi_0,\, (r_s)_s \right\rangle_\chi + \left\langle (q_s)_s,\, (r_s)_s \right\rangle_\chi\right)\right). \tag{11.10}$$

Proposition 11.13. *There is a $C > 0$ determined just from $(K/F, \mathscr{V}_0, \mathbb{F})$ so we have the following:*

Take N and X as above, and choose a G_F-submodule $Q_{\text{m,l}}$ of Q. Taking

$$\mathscr{Q}_1 = \left\{ (q_s)_s \in \mathscr{Q} \,:\, \mathbf{Q}\big(S_{\text{med}} \cup S_{\text{lg}},\, (q_s)_s\big) = Q_{\text{m,l}} \right\},$$

the sum (11.9) *has upper bound*

$$\mathcal{T}_{N,M_{\mathrm{m,l}}}(X) \cdot \exp\left(Cg^2 \ + \ Cg \cdot \#S_{\mathrm{sm}}\right) \cdot |X| \ \ + \ \ \exp(Cg \cdot \#S) \cdot c_{\mathrm{LS}} \cdot |X|,$$

where $M_{\mathrm{m,l}}$ *denotes the subspace of* M *associated to* $Q_{\mathrm{m,l}}$ *and* $\mathcal{T}_{N,M_{\mathrm{m,l}}}(X)$ *equals the Tamagawa ratio* $\mathcal{T}_{N,M_{\mathrm{m,l}}}(\chi)$ *for any* χ *chosen from* X.

Proof. We start by applying (11.10) with $\mathscr{Q}_2$ taken as the subset of $\mathscr{Q}$ of elements that are zero outside S_{sm} and with $\mathscr{Q}_3$ taken as the subset of $\mathscr{Q}_1$ of elements that are zero outside $S_{\mathrm{med}} \cup S_{\mathrm{lg}}$. Taking $\mathscr{Q}_3'$ to be the subset of $\mathscr{Q}_3$ for which there is no element $(r_s)_s$ in $\mathscr{R}(Q_{\mathrm{m,l}})$ supported over $S_{\mathrm{med}} \cup S_{\mathrm{lg}}$ for which

$$\left\langle \phi_0,\, (r_s)_s \right\rangle_\chi + \left\langle (q_s)_s,\, (r_s)_s \right\rangle_\chi \neq 0$$

for any (or all) $\chi \in X$, we find that the sum (11.10) remains unchanged if we replace $\mathscr{Q}_3$ with $\mathscr{Q}_3'$. From Proposition 10.14 and (10.7), we can bound the size of $\mathscr{Q}_3'$ by

$$\exp(Cg) \cdot \prod_{s \in S_{\mathrm{med}} \cup S_{\mathrm{lg}}} \frac{\#H^0(\langle \sigma_s \rangle,\, (N/M_{\mathrm{m,l}})[\omega])}{\#H^0(\langle \sigma_s \rangle,\, M/M_{\mathrm{m,l}}[\omega])}.$$

But, fixing $(q_s)_s$ in $\mathscr{Q}_3'$, we can bound

$$\frac{1}{\#\mathscr{R}} \sum_{\chi \in X} \sum_{(r_s)_s \in \mathscr{R}} \exp\left(2\pi i \cdot \left(\left\langle \phi_0,\, (r_s)_s \right\rangle_\chi + \left\langle (q_s)_s,\, (r_s)_s \right\rangle_\chi\right)\right) \tag{11.11}$$

by

$$c_{\mathrm{LS}} \cdot |X| \ + \ \exp(Cg^2) \cdot \prod_{s \in S_{\mathrm{med}} \cup S_{\mathrm{lg}}} \frac{\#H^0\left(\langle \sigma_s \rangle,\, M/M_{\mathrm{m,l}}\right)}{\#H^0\left(\langle \sigma_s \rangle,\, M\right)}$$

using the first part of Proposition 11.9 and the definition of c_{LS}. Taking products gives the proposition. □

We next show that, in cases where there are many jury indices, the contribution of unlawful $(q_s)_s$ to (11.9) is fairly small.

Proposition 11.14. *There is a $C > 0$ determined just from $(K/F, \mathscr{V}_0, \mathbb{F})$ so we have the following:*

Take N and X as above, and choose G_F-submodules $Q_{\min}$, $Q_{\max}$ of Q so $Q_{\max}$ properly contains $Q_{\min}$, with $M_{\min}, M_{\max}$ the associated submodules of M. Take

$$\mathscr{Q}_1 = \left\{(q_s)_s \in \mathscr{Q} \,:\, \mathbf{Q}\big(S,\,(q_s)_s\big) = Q_{\max},\ \mathbf{Q}\big(S_{\text{npar}}((q_s)_s),\,(q_s)_s\big) = Q_{\min}\right\}.$$

Then, for any G_F-module M_1 containing $M_{\min}$ and contained in $M_{\max}$, the expression (11.9) *is at most*

$$(1+\#S)^{Cg} \,\cdot\, \exp(Cg^2) \,\cdot\, \ell^{(-\#S_{\text{jury}} + 2\cdot\#S_{\text{sm}}\cup S_{\text{med}})\,\cdot\,\dim Q_{\max}/Q_{\min}} \cdot \mathcal{T}_{N,M_1}(X)\cdot|X|$$
$$+\ \exp(Cg\cdot\#S)\cdot(c_{\text{LS}} + c_{\text{Cheb}})\cdot|X|.$$

Proof. Given $(q_s)_s \in \mathscr{Q}_1$, there is a subset S_0 of S_{lg} of size at most $O(g)$ so that $\mathbf{Q}(S_{\text{npar}})$ equals $\mathbf{Q}(S_0 \cap S_{\text{npar}})$ and so, for every s_0 in $S_0 \cap S_{\text{npar}}$, there are disjoint subsets S_1, S_2 of $S_0 - \{s_0\}$ and functions

$$a_i : S_i \to \mathbb{F}_\ell \qquad \text{satisfying } \sum_{s\in S_i} a_i = 1 \text{ for } i = 1,2$$

so that

$$q_{s_0} = \sum_{s\in S_1} a_{1s} q_s = \sum_{s\in S_2} a_{2s} q_s.$$

This can be proved by the same greedy algorithm argument used for Proposition 11.5. By adjoining another $O(g)$ indices from S to S_0, we can additionally force

$$\mathbf{Q}\big(S,\,(q_s)_s\big) = \mathbf{Q}\big(S_0,\,(q_s)_s\big).$$

For any such S_0, define $\mathscr{Q}_2(S_0)$ to be

$$\{(q_s)_s \in \mathscr{Q} \,:\, q_s = 0 \text{ for } s\in S_0,\ q_s \in Q_{\min} \text{ for } s\in S_{\text{lg}},\ q_s \in Q_{\max} \text{ for } s \in S\}.$$

Taking $\overline{\mathscr{Q}_1}$ to be the set of tuples $\big((q_s)_s, S_0\big)$ so that $(q_s)_s$ is in $\mathscr{Q}_1$ and S_0 is a subset of at most $O(g)$ indices satisfying the requirements given above, we see that

$$\big((q_{1s} + q_{2s})_s,\ S_0\big) \in \overline{\mathscr{Q}_1} \quad \text{if } \big((q_{1s})_s,\ S_0\big) \in \overline{\mathscr{Q}_1} \text{ and } (q_2)_s \in \mathscr{Q}_2(S_0).$$

We can then consider the set of equivalence classes of $\overline{\mathscr{Q}_1}$ mod the union of the $\mathscr{Q}_2(S_0)$. Take $\mathscr{Q}_3$ to be a set of representatives for this set of equivalence classes. We then have

$$\#\mathscr{Q}_3 \leq (1 + \#S)^{Cg} \cdot \exp(Cg^2)$$

for some C as in the proposition statement, since this bounds the number of ways to choose S_0 and the values of q_s at S_0.

So, fixing $((q_{1s})_s, S_0)$ in $\mathscr{Q}_3$, we can reduce to bounding

$$\frac{1}{\#\mathscr{R}} \sum_{\chi \in X} \sum_{(q_s)_s \in \mathscr{Q}_2(S_0)} \sum_{(r_s)_s \in \mathscr{R}} \exp\left(2\pi i \cdot \left(\left\langle \phi_0,\ (r_s)_s \right\rangle_\chi + \left\langle (q_s + q_{1s})_s,\ (r_s)_s \right\rangle_\chi\right)\right).$$

Since $\mathscr{Q}_2(S_0)$ is a vector space, this is bounded by

$$\frac{1}{\#\mathscr{R}} \sum_{\chi \in X} \sum_{(q_s)_s \in \mathscr{Q}_2(S_0)} \sum_{(r_s)_s \in \mathscr{R}} \exp\left(2\pi i \cdot \left(\left\langle (q_s)_s,\ (r_s)_s \right\rangle_\chi\right)\right). \tag{11.12}$$

Take $\mathscr{Q}_2'$ to be the subspace of $(q_s)_s$ in $\mathscr{Q}_2$ so that

$$\left\langle (q_s)_s,\ (r_s)_s \right\rangle_\chi = 0$$

for all $(r_s)_s$ in $\mathscr{R}(Q_{\max})$. The above sum is then unchanged if we replace $\mathscr{Q}_2(S_0)$ with $\mathscr{Q}_2'$, and we have

$$\#\mathscr{Q}_2' \leq (1 + \#S)^{Cg} \cdot \exp(Cg^2) \cdot \ell^{(-\#S_{\text{jury}} + \#S_{\text{med}} \cup S_{\text{lg}}) \cdot \dim Q_{\max}/Q_{\min}} \cdot \prod_{s \in S} \frac{\#H^0\left(\langle \sigma_s \rangle,\ (N/M_1)[\omega]\right)}{\#H^0\left(\langle \sigma_s \rangle,\ M/M_{\max}\right)}.$$

from Proposition 10.14 and Proposition 11.11.

Now take $(q_s)_s \in \mathscr{Q}_2'$. Then (11.12) can be bounded by

$$(c_{\text{LS}} + c_{\text{Cheb}}) \cdot |X| \; + \; \frac{|X|}{\#\mathscr{R}} \cdot \exp(Cg^2) \cdot \ell^{\#S_{\text{sm}} \cup S_{\text{med}} \cdot \dim Q_{\max}/Q_{\min}} \prod_{s \in S} \#H^0(\langle \sigma_s \rangle, M/M_{\max})$$

via Proposition 11.9. The proposition is proved by combining this with the estimate on the size of $\mathscr{Q}_3$ and the size of $\mathscr{Q}_2'$. □

Having dealt with the case that we do not have access to the Chebotarev density theorem, and having dealt with unlawful $(q_s)_s$, the remaining case we need to deal with is the full case.

Proposition 11.15. *There is a $C > 0$ determined just from $(K/F, \mathscr{V}_0, \mathbb{F})$ so we have the following:*

Take N and X as above, and choose a G_F-submodule Q_1 of Q, with M_1 the associated submodule of M. Taking

$$\mathscr{Q}_1 = \left\{ (q_s)_s \; : \; \mathbf{Q}\big(S, \, (q_s)_s\big) = \mathbf{Q}\big(S_{\text{npar}}((q_s)_s), \, (q_s)_s\big) = Q_1 \right\},$$

we can bound (11.9) *by*

$$\begin{aligned} &\exp(Cg^2) \cdot \mathcal{T}_{N,M_1}(X) \cdot |X| \\ &\qquad + \; \exp(Cg \cdot \#S) \cdot (c_{\text{LS}} + c_{\text{Cheb}}) \cdot |X|. \end{aligned}$$

Proof. Take $\mathscr{Q}_1'$ to be the subset of $(q_s)_s$ in $\mathscr{Q}_1$ so that

$$\big\langle \phi_0, \, (r_s)_s \big\rangle_\chi + \big\langle (q_s)_s, \, (r_s)_s \big\rangle_\chi = 0 \quad \text{ for all } (r_s)_s \in \mathscr{R}(Q_1).$$

We can restrict (11.9) from $\mathscr{Q}_1$ to $\mathscr{Q}_1'$ without changing its value.

We can bound the size of $\mathscr{Q}_1'$ using Proposition 10.14 and (10.7) and can use the second part of Proposition 11.9 to estimate (11.11). This is enough to prove the proposition. □

For Proposition 11.14 to be useful, we need S_{jury} to be large and for $S_{\text{sm}} \cup S_{\text{med}}$ to be small. If we pull this out as an assumption, the previous two propositions can be combined to the following useful form.

Assumption 11.16. With notation as above, we say Assumption 11.16 is satisfied if

$$\#\{s \in S \,:\, \sigma_s = \sigma_0\} \geq \frac{|S|}{2|G_1|} \quad \text{for all } \sigma_0 \in G_0 \tag{11.13}$$

and

$$\#S_{\text{sm}} \cup S_{\text{med}} \;\leq \tfrac{|S|}{8|G_1|}.$$

Proposition 11.17. *There is a $C > 0$ determined just from $(K/F, \mathscr{V}_0, \mathbb{F})$ so we have the following:*

Take $S = S_{\text{sm}} \cup S_{\text{med}} \cup S_{\text{lg}}$ and $(\sigma_s)_s$ obeying Assumption 11.16. Take N to be a twistable module defined with respect to $(K/F, \mathscr{V}_0, \mathbb{F})$, and define c_{LS} and c_{Cheb} as in Notation 11.12. Take Q_0 to be a G_F submodule of Q, with M_0 the associated submodule of M. Defining

$$\mathscr{Q}(Q_0) = \{(q_s)_s \in \mathscr{Q} \,:\, \mathbf{Q}((q_s)_s) = Q_0\},$$

take $\mathscr{Q}_1$ to be a subset of $\mathscr{Q}(Q_0)$. Take ϕ in $\mathscr{S}_{M/F}(\mathscr{V}_0)$, and take X as above.

Then, if $\mathscr{Q}(Q_0)$ is nonempty, the sum (11.9) *has upper bound*

$$\exp(Cg^2) \cdot \mathcal{T}_{N,M_0} \cdot \frac{\#\mathscr{Q}_1}{\#\mathscr{Q}_0} \cdot |X| \;+\; \exp\left(Cg^2 - \tfrac{\#S}{C}\right) \cdot \mathcal{T}_{N,M_0}(X) \cdot |X| \;+\; \exp(Cg \cdot \#S) \cdot (c_{\text{LS}} + c_{\text{Cheb}}) \cdot |X|.$$

11.4. **Estimating moments using non-ignorable pairs.** If the twistable module N is in either the alternating or non-alternating case of Notation 9.8, we have additional control on the general moment (8.12) coming from our work on main-term pairs in Section 10.4.

Proposition 11.18. *Given $(K/F, \mathscr{V}_0, \mathbb{F})$, with $\mathbb{F}$ trivial as a* $\text{Gal}(K/F)$ *module, there is some $C > 0$ so we have the following:*

Take N to be a twistable module of corank g with local conditions $(W_v)_v$ that is either in the alternating case or non-alternating case. Take n_1, n_2 to be nonnegative integers, and take

$$N_1 = N^{\oplus n_1}, \quad N_2 = N^{\oplus n_2}, \quad N_0 = N_1 \oplus N_2.$$

These all carry standard Selmer structures induced from N. We use the notation M_0, Q_0, etc.

Choose a nonempty index set $S = S_{\text{sm}} \cup S_{\text{med}} \cup S_{\text{lg}}$, sequences $(\sigma_s)_s$ and $(x_s)_s$, and a tuple set of twists X so Assumption 11.16 holds.

Taking the notation

$$\mathscr{R} = \bigoplus_{s \in S} H^0(\langle \sigma_s \rangle, R_0), \quad \mathscr{Q} = \bigoplus_{s \in S} H^0(\langle \sigma_s \rangle, N_0)$$

$$\mathscr{Q}_{N_0,+}(Q_1) = \{(q_s)_s \in \mathscr{Q} : \mathbf{Q}((q_s)_s) \subseteq Q_1\}),$$

$$\mathscr{Q}_{N_0}(Q_1) = \{(q_s)_s \in \mathscr{Q} : \mathbf{Q}((q_s)_s) = Q_1\},$$

we take $\mathscr{Q}_1$ to be a subset of $\mathscr{Q}_{N_0}(Q_1)$. We assume either that

- *There is no $\beta : M_1 \to N_0'[\omega]$ so (M_1, β) is cancellable, in the sense of Notation 10.8; or*
- *The space $\mathscr{Q}_1$ is the intersection of $\mathscr{Q}_{N_0}(Q_1)$ with a coset of $\mathscr{Q}_{N_0,+}(Q_1)$ of some subspace of codimension at most $|S|/8|G_1|$.*

Choose $\phi_0 \in \mathscr{S}_{M_0/F}(\mathscr{V}_0)$. We assume that, for $(q_s)_s$ in $\mathscr{Q}_1$, the element

$$\phi = \phi_0 + \sum_{s \in S} \mathfrak{B}^{\text{nc}}_{N[\omega],F,\overline{\mathfrak{p}}_s}(q_s \cup_{\mathbb{F}} x_s)$$

satisfies the local conditions at all v in $\mathscr{V}_0$.

For any $(q_s)_s$ in $\mathscr{Q}_1$, the projection of q_s to Q_2 does not depend on the choice of s. We also presume it does not depend on the choice of $(q_s)_s$ from $\mathscr{Q}_1$. Call this element $\pi_2(\mathscr{Q}_1)$.

For each $\sigma_0 \in G_1$, we can consider the composition

$$\mathscr{S}_{M_0/F}(\mathscr{V}_0) \to \mathscr{S}_{M_2/F}(\mathscr{V}_0) \xrightarrow{\text{res}} H^1(\langle \sigma_0 \rangle,\, M_2).$$

If $\phi_0 - \delta_{G_F}(\pi_2(\mathscr{Q}_1))$ is nonzero under this composition for some σ_0, then

$$\frac{1}{\#\mathscr{R}} \sum_{\chi \in X} \sum_{(q_s)_s \in \mathscr{Q}_1} \sum_{(r_s)_s \in \mathscr{R}} \exp\left(2\pi i \cdot \left(\left\langle \phi_0,\, (r_s)_s \right\rangle_\chi + \left\langle (q_s)_s,\, (r_s)_s \right\rangle_\chi\right)\right) \tag{11.14}$$

is zero. Otherwise, taking

$$b = \begin{cases} \frac{1}{2} n_1(n_1+1) & \textit{in the alt. case} \\ 0 & \textit{in the n-alt. case,} \end{cases}$$

the difference between (11.14) *and*

$$\left(\#H^0(G_F, M)\right)^{n_2} \cdot \left(\#H^0(G_F, R)\right)^{n_1} \cdot \ell^b \cdot \frac{\#\mathscr{Q}_1}{\#\mathscr{Q}_{N_0}(Q_1)} \cdot |X|$$

has magnitude at most

$$\exp\left(Cg_0^2 - \tfrac{\#S}{C}\right) \cdot |X| \;+\; \exp(Cg_0 \cdot \#S) \cdot (c_{\text{LS}} + c_{\text{Cheb}}) \cdot |X|,$$

where $g_0 = g \cdot (n_1 + n_2)$.

Proof. Via Proposition 10.11, we see we can adjust the set of ϕ under consideration by $\delta_{G_F}(\pi_2(\mathscr{Q}_1))$ without changing any pairings. So we may as well assume that $\pi_2(\mathscr{Q}_1)$ is zero.

Under this assumption, if ϕ_0 does not vanish on M_2 when restricted to some $\langle \sigma_0 \rangle$, we choose s_0 so σ_{s_0} equals σ_0 using Assumption 11.16, and we note there is some choice of $r_{s_0} \in R_2$ so, if $(r_s)_s$ equals r_{s_0} at s_0 and otherwise equals 0, we have

$$\langle \phi_0, (r_s)_s \rangle_\chi \neq 0.$$

From this, we find (11.14) is zero in this case. So suppose ϕ_0 does vanish on M_2 when restricted to any $\langle\sigma_0\rangle$.

For any positive constant C determined from $(K/F, \mathscr{V}_0, \mathbb{F})$, the statement is vacuous if $|S|$ is smaller than Cg_0. So we assume that $|S|$ is at least this large.

Take $\mathscr{Q}_1'$ to be the subset of $(q_s)_s$ in $\mathscr{Q}_1$ where

$$\mathbf{Q}\big(S_{\text{npar}}((q_s)_s),\ (q_s)_s\big) = Q'.$$

Via Proposition 11.14, replacing $\mathscr{Q}_1$ with $\mathscr{Q}_1'$ changes (11.14) by at most

$$\big(Cg_0^2 - \tfrac{\#S}{C}\big) \cdot \mathcal{T}_{N,M'}(X) \cdot |X|.$$

For $(q_s)_s$ in $\mathscr{Q}_1'$ and a non-ignorable pair $\big((q_s)_s, (r_s)_s\big)$, we have a map

$$\Gamma : Q_1 \longrightarrow R_1.$$

defined as in Proposition 11.7. We then find that the value of $r_s - \Gamma(q_s)$ projected to R_1 does not depend on $s \in S$. Calling this value r_0, we find from Proposition 10.11 that $(r_s)_s$ and $(r_s - r_0)_s$ give equal pairing values.

We next note that, if $(r_s)_s$ is in $\bigoplus_s H^0(\langle\sigma_s\rangle,\ R_2)$, we have

$$\langle\phi, (r_s)_s\rangle_\chi = 0$$

for all ϕ from $\mathscr{Q}_1$ and all χ in X.

We then find (11.14) is within the error stated for the proposition of

$$\prod_{s\in S} \big(\#H^0(\langle\sigma_s\rangle,\ R)\big)^{-n_1} \cdot H^0(G_F, R)^{n_1}$$
$$\cdot \sum_{\Gamma} \sum_{\chi\in X} \sum_{(q_s)_s \in \mathscr{Q}_1'} \exp\Big(2\pi i \cdot \Big(\big\langle\phi_0,\ (\Gamma(r_s))_s\big\rangle_\chi + \big\langle(q_s)_s,\ (r_s)_s\big\rangle_\chi\Big)\Big),$$

where Γ ranges over alternating equivariant maps from Q_1 to R_1.

We next claim that we can restrict that sum over Γ to homomorphisms that commute with the connecting maps, in the sense of Section 9. Outside, (M_1, Γ) is cancellable, so we can assume that $\mathscr{Q}_1$ comes from a coset $\mathscr{Q}_2$ of small codimension in $\mathscr{Q}_{N_0,+}(Q_1)$. From Proposition 10.9, we have a bound

$$\left| \sum_{\chi \in X} \sum_{(q_s)_s \in \mathscr{Q}_2} \exp\left(2\pi i \cdot \left(\left\langle \phi_0,\, (\Gamma(r_s))_s \right\rangle_\chi + \left\langle (q_s)_s,\, (r_s)_s \right\rangle_\chi \right)\right) \right| \leq \exp\left(C g_0^2 - \tfrac{|S|}{C} \right) \cdot |X| \cdot |\mathscr{Q}_2|.$$

From Proposition 11.11, this statement still holds when we replace $\mathscr{Q}_2$ by $\mathscr{Q}_1'$.

But, by applying Proposition 9.7 to the graph of a map from $M^{\oplus n_1}$ to $R^{\oplus n_1}$, we find that, in the non-alternating case, the only Γ that commutes with the connecting maps is the zero map; and, in the alternating case, the Γ are the ℓ^b different β_T considered in Proposition 10.12. Applying this proposition then finishes our proof. □

Part 4. The Base Case II: Gridding

12. Grids of twists

12.1. Grids of ideals.

Notation 12.1. Fix $(K/F, \mathscr{V}_0, \mathbb{F})$ as in Notation 8.1. We take $\mathscr{P}$ to be the set of primes of F outside $\mathscr{V}_0$ that split completely in the extension $F(\mathbb{F}(-1))/F$. We write $K(\mathscr{V}_0)$ as before, for the maximal exponent ℓ abelian extension of K ramified only over $\mathscr{V}_0$, and we write

$$G_1 = \mathrm{Gal}(K(\mathscr{V}_0)/F(\mathbb{F}(-1))).$$

We will take $G_1/\!\sim$ to be the set of equivalence classes of G_1 under conjugation by $\mathrm{Gal}(K(\mathscr{V}_0)/F)$.

Take H to be a positive real number satisfying $\log^{(3)} H > 1$. We define

$$\alpha(H) = \exp\left(\exp^{(3)}\left(\tfrac{1}{4} \log^{(3)} H \right)^{-1} \right) \quad \text{and} \quad a_0(H) = \exp^{(3)}\left(\tfrac{1}{3} \log^{(3)} H \right).$$

For i a nonnegative integer, we then define

$$\mathscr{P}_i(H) = \left\{\mathfrak{p} \in \mathscr{P} \,:\, a_0(H) \cdot \alpha(H)^i \leq N_{F/\mathbb{Q}}(\mathfrak{p}) < a_0(H) \cdot \alpha(H)^{i+1}\right\}.$$

If C is a class of $G_1/\sim$, we will also define

$$\mathscr{P}_i(H, C) = \{\mathfrak{p} \in \mathscr{P}_i(H) \,:\, \text{Frob}\,\mathfrak{p} = C\}.$$

We also take the notation

$$i_{\text{med}}(H) = \left\lceil \exp^{(3)}\left(\tfrac{1}{2}\log^{(3)} H\right)\right\rceil.$$

Definition 12.2. With $(K/F, \mathscr{V}_0, \mathbb{F})$ and H as above, take S to be a finite set partitioned as $S_{\text{sm}} \cup S_{\text{med}} \cup S_{\text{lg}}$. For $s \in S_{\text{sm}}$, take $\mathfrak{p}_s$ be a prime in $\mathscr{P}$ satisfying $N_{F/\mathbb{Q}}(\mathfrak{p}_s) \leq a_0(H)$. For $s \in S_{\text{med}} \cup S_{\text{lg}}$, take i_s to be a nonnegative integer. We make the following assumptions:

- For $s_1 \neq s_2$ in S_{sm}, $\mathfrak{p}_{s_1}$ and $\mathfrak{p}_{s_2}$ are distinct.
- For $s_1 \neq s_2$ in $S_{\text{med}} \cup S_{\text{lg}}$, i_{s_1} and i_{s_2} are distinct.
- For $s \in S_{\text{med}} \cup S_{\text{lg}}$, s is in S_{med} if and only if $i_s < i_{\text{med}}(H)$.

Taking the notation

$$X_s = \begin{cases} \{\mathfrak{p}_s\} & \text{if } s \in S_{\text{sm}} \\ \mathscr{P}_{i_s}(H) & \text{if } s \in S_{\text{med}} \cup S_{\text{lg}}, \end{cases}$$

we define a set of ideals X of F by

$$X = \left\{\prod_{s \in S} \mathfrak{p}_s \,:\, \mathfrak{p}_s \in X_s \text{ for } s \in S\right\}. \tag{12.1}$$

If X contains no ideal of norm greater than H, we will say that X is an *unfiltered grid of ideals of height* H.

Now, suppose that the tuple

$$\left(H, S, (\mathfrak{p}_s)_{s \in S_{\text{sm}}}, (i_s)_{s \in S_{\text{med}} \cup S_{\text{lg}}}\right)$$

defines an unfiltered grid of ideals of height H. For $s \in S$, take C_s to be an class of $G_1/\sim$. For $s \in S_{\text{sm}}$, we assume that $\mathfrak{p}_s$ has Frobenius class C_s. Then, defining

$$X_s = \begin{cases} \{\mathfrak{p}_s\} & \text{if } s \in S_{\text{sm}} \\ \mathscr{P}_{i_s}(H,\, C_s) & \text{if } s \in S_{\text{med}} \cup S_{\text{lg}}, \end{cases}$$

the set X defined by (12.1) will be called a *grid (or filtered grid) of ideals of height H*.

Notation 12.3. Fix $(K/F, \mathscr{V}_0, \mathbb{F})$ and H, and take all notation as above. Write $\mathscr{H}$ for the set of squarefree products of primes in $\mathscr{P}$. Given $\mathfrak{h} \in \mathscr{H}$ that satisfies $N_{F/\mathbb{Q}}(\mathfrak{h}) \leq H$, we will write $\omega(\mathfrak{h})$ for the number of distinct prime divisors of $\mathfrak{h}$, and $\omega_{\text{sm}}(\mathfrak{h})$ for the number of prime divisors of norm at most $a_0(H)$.

In addition, we will call $\mathfrak{h}$ *good* if the following assumptions hold:

(1) *(Not too many primes)* We have

$$\omega(\mathfrak{h}) \leq (\log\log H)^2.$$

(2) *(Inside a grid)* There is a grid of ideals of height H described by the information

$$\big(S,\, (\mathfrak{p}_s)_{s\in S_{\text{sm}}},\, (i_s)_{s\in S_{\text{med}}\cup S_{\text{lg}}},\, (C_s)_s\big)$$

that contains $\mathfrak{h}$.

(3) *(Not too many small primes)* We have

$$|S_{\text{sm}}| \,\leq\, (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}} \quad \text{and} \quad |S_{\text{med}}| \leq (\log^{(2)} H)^{\frac{1}{2}+\frac{1}{100}}.$$

(4) *(Enough primes)* We also have

$$|S| = \omega(\mathfrak{h}) \,\geq\, \frac{\log^{(2)} H}{\log^{(3)} H}.$$

(5) *($(C_s)_s$ is balanced)* For any C in $G_1/\sim$, we have

$$\left| \#\left\{ s \in S_{\text{lg}} \,:\, C_s = C \right\} \;-\; \frac{\#C}{\#G_1} \cdot \#S \right| \leq \#S^{3/4}.$$

(6) *(No Siegel zeros)* Given $x \geq 2$, there is at most one positive squarefree integer $d_{x,\text{sie}} \leq x$ so the Dedekind zeta function associated to $\mathbb{Q}(\sqrt{d_{x,\text{sie}}})$ has a real zero particularly close to $s = 1$; we give a more precise specification for this potentially-defined integer in Proposition 12.11. Taking

$$x = \exp^{(3)}\left(\tfrac{2}{5} \log^{(3)} H\right),$$

we assume that either $\ell \neq 2$, that $d_{x,\text{sie}}$ does not exist, or that $N_{F/\mathbb{Q}}(a_{\mathscr{V}_0} \cdot \mathfrak{h}_{\text{sm}})$ is indivisible by $d_{x,\text{sie}}$, where $\mathfrak{h}_{\text{sm}}$ is the product of the primes of $\mathfrak{h}$ indexed by S_{sm} and $a_{\mathscr{V}_0}$ is the product of all rational primes over the finite places of $\mathscr{V}_0$.

(7) *(Prepared for higher Selmer work)* Among the primes indexed by

$$\{s \in S_{\text{lg}} \,:\, C_s = \{1\}\},$$

there are at least $(\log \log H)^{2/3 - 1/100}$ primes of norm at most

$$\exp^{(3)}\left(\tfrac{2}{3} \log^{(3)} H\right)$$

and at least $(\log \log H)^{1 - 1/100}$ primes of norm at least

$$\exp^{(3)}\left(\tfrac{3}{4} \log^{(3)} H\right).$$

(8) *($(C_s)_s$ is not overbalanced)* Given a nonzero function $f : G_1/\sim \to \mathbb{Z}$ whose magnitude does not exceed $\exp^{(2)}\left(\tfrac{1}{2} \log^{(4)} H\right)$, we have

$$\left| \sum_{s \in S} f(C_s) \right| \geq \#S^{1/4}.$$

Given an integer j satisfying $1 \leq j \leq 8$, we will write $\mathscr{H}_{\text{bad},j}(H)$ for the set of $\mathfrak{h}$ as above that have the first $j-1$ properties enumerated above but which do not have the j^{th} property.

We will need the following estimate on the number of ideals in $\mathscr{H}$.

Proposition 12.4. *Take $(K/F, \mathscr{V}_0, \mathbb{F})$ as above, and write $d_{\mathbb{F}}$ for the degree of $F(\mathbb{F}(-1))$ over F. Fix some $A > 0$. Then there is some $C > 0$ determined from this information so that we have the following:*

For $x > C$ and r a positive integer no larger than $A \cdot \log\log x$, we have

$$\begin{aligned}\frac{x}{C \cdot \log x} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot \log\log x)^{r-1}}{(r-1)!} &\leq \#\left\{\mathfrak{h} \in \mathscr{H} \,:\, \omega(\mathfrak{h}) = r \text{ and } N_{F/\mathbb{Q}}(\mathfrak{h}) < x\right\} \\ &\leq \frac{Cx}{\log x} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot \log\log x)^{r-1}}{(r-1)!}.\end{aligned}$$

The upper bound here is a special case of Proposition 13.1, which is given in the next section. The lower bound is substantially more annoying, and I do not know of a good way to prove it without invoking the methods of Section 5 of [48], and specifically without using Lemma 5.1 of that paper.

This lower bound is important for our work because of the form of the following proposition. To render the contribution of $\mathscr{H}_{\text{bad},j}(H)$ negligible, we need to be able to compare it with the main term provided by Proposition 12.4.

Proposition 12.5. *Fix a real number δ, and take*

$$\kappa = 1 - \exp(\delta) \cdot d_{\mathbb{F}}^{-1}.$$

In addition, fix some sufficiently small $\epsilon > 0$. Then there is a real number $C > 0$ determined just from $(K/F, \mathscr{V}_0, \mathbb{F})$, δ, and ϵ so that, for all $H > C$ and j in $\{1, \ldots, 7\}$, we have

$$\sum_{\mathfrak{h} \in \mathscr{H}_{\text{bad},j}(H)} \exp\left(\delta \cdot \omega(\mathfrak{h}) \,+\, a_j(\mathfrak{h}, H)\right) \;\leq\; \frac{H}{(\log H)^{\kappa}} \cdot E_j(H), \tag{12.2}$$

where we have taken

$$
\begin{aligned}
a_1(\mathfrak{h}, H) &= \omega(\mathfrak{h}) \cdot (1-\epsilon) \log^{(3)} H & E_1(H) &= \exp\left(-\left(\log^{(2)} H\right)^2\right) \\
a_2(\mathfrak{h}, H) &= \omega(\mathfrak{h}) \cdot \exp^{(2)}\left(\tfrac{1}{4} \log^{(3)} H\right)^{1-\epsilon} & E_2(H) &= \exp^{(3)}\left(\tfrac{1}{4} \log^{(3)} H\right)^{-1+\epsilon} \\
a_3(\mathfrak{h}, H) &= \omega_{\text{sm}}(\mathfrak{h}) \cdot \left(\tfrac{1}{100} - \epsilon\right) \log^{(3)} H & E_3(H) &= \exp^{(2)}\left(\tfrac{1}{3} \log^{(3)} H\right)^{-1} \\
a_4(\mathfrak{h}, H) &= \omega_{\text{sm}}(\mathfrak{h}) \cdot \left(\log^{(2)} H\right)^{\frac{2}{3} - \frac{1}{100} - \epsilon} & E_4(H) &= \frac{(\log H)^{\kappa}}{(\log H)^{1-\epsilon}} \\
a_5(\mathfrak{h}, H) &= \omega_{\text{sm}}(\mathfrak{h}) \cdot \left(\log^{(2)} H\right)^{\frac{1}{6} - \frac{1}{100} - \epsilon} & E_5(H) &= \exp^{(2)}\left(\left(\tfrac{1}{2} - \epsilon\right) \cdot \log^{(3)} H\right)^{-1} \\
a_6(\mathfrak{h}, H) &= \omega_{\text{sm}}(\mathfrak{h}) \cdot \left(\log^{(2)} H\right)^{\frac{1}{15} - \frac{1}{100} - \epsilon} & E_6(H) &= \exp^{(2)}\left(\tfrac{2}{5} \log^{(3)} H\right)^{-1+\epsilon} \\
a_7(\mathfrak{h}, H) &= 0 & E_7(H) &= \exp^{(2)}\left(\left(\tfrac{2}{3} - \epsilon\right) \cdot \log^{(3)} H\right)^{-1} \\
a_8(\mathfrak{h}, H) &= 0 & E_8(H) &= \left(\log^{(2)} H\right)^{-\frac{1}{4}+\epsilon}.
\end{aligned}
$$

We will prove this in Section 13.

12.2. **Grids of twists.** Take X to be a grid of height H with associated index set S. Given

$$\mathfrak{h} = \prod_{s \in S} \mathfrak{p}_s$$

in this set, there are

$$\#\mathscr{S}_{\mathbb{F}/F}(\mathscr{V}_0) \cdot \left(\frac{(\ell-1) \cdot \#\mathbb{F}}{\ell}\right)^{|S|}$$

twists defined mod $Ш_1(F, \mathbb{F})$ that satisfy $\mathfrak{h}_F(\chi) = \mathfrak{h}$.

It would be best to consider this set of twists simultaneously, but these twists can vary in their behvaior when restricted to the places in $\mathscr{V}_0$, which is nonideal. The following setup helps us remedy this situation.

Notation 12.6. Take $(K/F, \mathscr{V}_0, \mathbb{F})$ as before. For every conjugacy class C of $\text{Gal}(K(\mathscr{V}_0)/F)$ that acts trivially on $\mathbb{F}(-1)$, fix an element $\sigma_{\text{bp}}(C)$ of $\text{Gal}(K(\mathscr{V}_0)/F)$ in this conjugacy class.

Suppose X is a filtered grid of height H associated to the tuple $(X_s)_{s\in S}$ of sets of primes and the tuple $(C_s)_{s\in S}$ of conjugacy classes of $\mathrm{Gal}(K(\mathscr{V}_0)/F)$. For $s \in S$, we take $X_{\mathrm{bp},s}$ to be the set of primes $\overline{\mathfrak{p}}$ of $\overline{F}$ such that $\overline{\mathfrak{p}}$ divides some prime in X_s and

$$\mathrm{Frob}_F\, \overline{\mathfrak{p}} = \sigma_{\mathrm{bp}}(C_s) \quad \text{in} \ \ \mathrm{Gal}(K(\mathscr{V}_0)/F).$$

Choose $x \in \mathbb{F}(-1)$. For $s \in S$, we define a subset $X_{\mathrm{tw},s}(x)$ of the module of twists

$$H^1(G_F, \mathbb{F})/Ш_1(F, \mathbb{F})$$

by

$$X_{\mathrm{tw},s}(x) = \left\{ \mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_s}(x) \ : \ \overline{\mathfrak{p}}_s \in X_{\mathrm{bp},s} \right\}.$$

Given $(\chi_0, (x_s)_s)$ in

$$\mathscr{S}_{\mathbb{F}/F}(\mathscr{V}_0) \ \times \prod_{s\in S} \mathbb{F}(-1)^\times, \tag{12.3}$$

we then take $X_{\mathrm{tw}}(\chi_0, (x_s)_s)$ to be the set of twists of the form

$$\chi_0 + \sum_{s\in S} \chi_s \quad \text{for some } \ (\chi_s)_s \in \prod_{s\in S} X_{\mathrm{tw},s}(x_s).$$

The sets $X_{\mathrm{bp},s}$ are infinite, but can easily be collapsed down to finite sets via the following claim:

Proposition 12.7. *In the above situation, given $s \in S$ and $\overline{\mathfrak{p}}_{1s}, \overline{\mathfrak{p}}_{2s}$ in $X_{\mathrm{bp},s}$, and given $x \in \mathbb{F}(-1)^\times$, we have*

$$\mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_{1s}}(x) - \mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_{2s}}(x) \ \neq \ 0$$

if and only if

$$\overline{\mathfrak{p}}_{1s} \cap F(\mathbb{F}(-1)) \ \neq \ \overline{\mathfrak{p}}_{2s} \cap F(\mathbb{F}(-1)).$$

Furthermore, if this difference is nonzero, it is ramified at $\overline{\mathfrak{p}}_{1s} \cap F$.

Proof. This follows from the form of the construction of the sections $\mathfrak{B}^{\mathrm{nc}}$ and from (5.17). □

From this, for $x \in \mathbb{F}(-1)$ the map $\overline{\mathfrak{p}} \mapsto \mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}}(x)$ descends to a bijection

$$\left\{\overline{\mathfrak{p}} \cap F(\mathbb{F}(-1)) \,:\, \overline{\mathfrak{p}} \in X_{\mathrm{bp},s}\right\} \xrightarrow{\sim} X_{\mathrm{tw},s}.$$

At this point, we have split the set of twists χ for which $\mathfrak{h}_F(\chi)$ lies in X into several pieces $X_{\mathrm{tw}}(\chi_0, (x_s)_s)$. Our next claim is that these pieces do not overlap.

Proposition 12.8. *Still in the context of Notation 12.6, suppose* $(\chi_{10}, (x_{1s})_s)$ *and* $(\chi_{20}, (x_{2s})_s)$ *both lie in* (12.3)*. Then the sets*

$$X_{\mathrm{tw}}(\chi_{10}, (x_{1s})_s) \quad \textit{and} \quad X_{\mathrm{tw}}(\chi_{20}, (x_{2s})_s)$$

are either disjoint or identical.

Proof. Suppose these sets overlap. We can then find $(\overline{\mathfrak{p}}_{1s})_s$, $(\overline{\mathfrak{p}}_{2s})_s$ in the product of the $X_{\mathrm{bp},s}$ so that

$$\chi_{10} + \sum_{s\in S} \mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_{1s}}(x_{1s}) \;=\; \chi_{20} + \sum_{s\in S} \mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_{2s}}(x_{2s}).$$

There is then some tuple $(\tau_s)_{s\in S}$ of elements from G_F so that $\overline{\mathfrak{p}}_{2s} = \tau_s \overline{\mathfrak{p}}_{1s}$ for all s. Then, for $(\overline{\mathfrak{p}}_s)_s$ in the product of the $X_{\mathrm{bp},s}$, the construction of $\mathfrak{B}^{\mathrm{nc}}$ forces

$$\chi_{10} + \sum_{s\in S} \mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_s}(x_{1s}) \;=\; \chi_{20} + \sum_{s\in S} \mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\tau_s\overline{\mathfrak{p}}_s}(x_{2s}),$$

and the proposition follows. □

Proposition 12.9. *There are positive real numbers* $C, c > 0$ *determined just from* $(K/F, \mathscr{V}_0, \mathbb{F})$ *so we have the following:*

Take N *to be any twistable module defined from* $(K/F, \mathscr{V}_0, \mathbb{F})$*. Fix* $(\chi_0, (x_s)_s)$ *in* (12.3)*, and take* X *to be a filtered grid of ideals of height* $H > C$*. Then, defining* c_{LS} *as in Notation*

11.12 for $X_{\text{tw}}(\chi_0, (x_s)_s)$, we have

$$c_{\text{LS}} \leq \exp^{(3)}\left(\tfrac{1}{3}\log^{(3)} H\right)^{-c}.$$

In addition, if X contains no ideals in $\mathscr{H}_{\text{bad},j}(H)$ for $j = 1, 3, 6$, we have

$$c_{\text{Cheb}} \leq \exp^{(3)}\left(\tfrac{1}{3}\log^{(3)} H\right)^{-c}.$$

Proof. Suppose $((q_s)_s,\ (r_s)_s)$ is ignorable by the large sieve. Then there are distinct indices s_1, s_2 in $S_{\text{med}} \cup S_{\text{lg}}$ and an element τ_0 in G_F so that

$$(r_{s_1} - \tau_0 r_{s_2}) \cdot (q_{s_1} - \tau_0 q_{s_2}) \neq 0.$$

Fix $\chi_s \in X_{\text{tw},s}(x_s)$ for $s \in S - \{s_1, s_2\}$. For

$$(\overline{\mathfrak{p}}_1, \overline{\mathfrak{p}}_2) \in X_{\text{bp},s_1} \times X_{\text{bp},s_2},$$

define a twist $\chi[\overline{\mathfrak{p}}_1, \overline{\mathfrak{p}}_2]$ by

$$\chi[\overline{\mathfrak{p}}_1, \overline{\mathfrak{p}}_2] = \chi_0 + \mathfrak{B}^{\text{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_1}(x_{s_1}) + \mathfrak{B}^{\text{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_2}(x_{s_2}) + \sum_{s \neq s_1,s_2} \chi_s.$$

The set of twists of this form give a subset of X_{tw} that is in bijection with $X_{\text{tw},s_1} \times X_{\text{tw},s_2}$. We denote this subset by Z_{tw} Our goal is to show that

$$\left|\sum_{\chi \in Z_{\text{tw}}} \exp\left(2\pi i \cdot \left\langle (q_s)_s,\ (r_s)_s \right\rangle_\chi\right)\right| \leq C \cdot \exp^{(3)}\left(\tfrac{1}{3}\log^{(3)} H\right)^{-c} \cdot \#X_{\text{tw},s_1} \cdot \#X_{\text{tw},s_2}.$$

From Proposition 10.7, we find there are a sequence of elements $a(\overline{\mathfrak{p}}_1), b(\overline{\mathfrak{p}}_2)$ of $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$ indexed by primes from X_{bp,s_1} and X_{bp,s_2} respectively and a sequence of elements $c_\tau \in \mathbb{F}_\ell(-1)$ indexed by

$$B\left(\sigma_{\text{bp}}(C_{s_1}),\ \sigma_{\text{bp}}(C_{s_1})\right)$$

so that

$$\left\langle (q_s)_s,\, (r_s)_s \right\rangle_{\chi[\overline{\mathfrak{p}}_1,\overline{\mathfrak{p}}_2]} \;=\; a(\overline{\mathfrak{p}}_1) \;+\; b(\overline{\mathfrak{p}}_2) \;+\; \sum_{\tau} c_\tau a_\tau^{\text{nc}}(\overline{\mathfrak{p}}_1, \overline{\mathfrak{p}}_2)$$

for all $(\overline{\mathfrak{p}}_1, \overline{\mathfrak{p}}_2)$ in $X_{\text{bp},s_1} \times X_{\text{bp},s_2}$. By the ignorability hypothesis, we know the c_τ are not all zero. From Proposition 2.13, for fixed $\overline{\mathfrak{p}}_2$, we can define a function

$$f_{\overline{\mathfrak{p}}_2} : \text{Gal}\big(K\big(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}}_2 \cap F\}\big)/F\big) \to \mathbb{C}$$

so that

$$f_{\overline{\mathfrak{p}}_2}(\text{Frob}_F\, \overline{\mathfrak{p}}) = \exp\left(2\pi i \cdot \left(\sum_{\tau} c_\tau \cdot a_\tau^{\text{nc}}(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}_2)\right)\right)$$

for primes $\overline{\mathfrak{p}}$ not dividing $\mathscr{V}_0$ or $\overline{\mathfrak{p}}_2 \cap F$ for which $\text{Frob}_F\, \overline{\mathfrak{p}}$ projects to $\sigma_{\text{bp}}(C_{s_1})$ in $\text{Gal}(K(\mathscr{V}_0)/F)$, and so that

$$f(\sigma) = 0 \quad \text{if} \;\; \sigma \neq \sigma_{\text{bp}}(C_{s_1}) \quad \text{in} \;\; \text{Gal}(K(\mathscr{V}_0)/F).$$

This function is furthermore of zero average on cosets of

$$\text{Gal}\left(K\big(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}}_2 \cap F\}\big)/K(\mathscr{V}_0)\right),$$

so we can apply Theorem 6.3 to get the claim of the proposition.

Now suppose $((q_s)_s,\, (r_s)_s)$ is ignorable by Chebotarev. If the pair is also ignorable by the large sieve, the above argument works. So we can assume it is not ignorable by the large sieve. In particular, there must be some $s_1 \in S_{\text{lg}}$, $s_2 \in S_{\text{sm}}$, and $\tau_0 \in G_F$ so

$$(r_{s_1} - \tau_0 r_{s_2}) \cdot (q_{s_1} - \tau_0 q_{s_2}) \neq 0.$$

while we have

$$(r_{s_1} - \tau r_s) \cdot (q_{s_1} - \tau q_s) = 0 \quad \text{for all} \;\; s \in S_{\text{sm}} \cup S_{\text{med}},\; \tau \in G_F.$$

Fix a choice of $\overline{\mathfrak{p}}_s \in X_{\text{bp},s}$ for $s \neq s_1$. For $\overline{\mathfrak{p}}_1$ in X_{bp,s_1}, take

$$\chi[\overline{\mathfrak{p}}_1] = \chi_0 + \mathfrak{B}^{\text{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_1}(x_{s_1}) + \sum_{s \neq s_1} \mathfrak{B}^{\text{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}}(x_s).$$

Then we can use Proposition 10.7 to write

$$\left\langle (q_s)_s,\, (r_s)_s \right\rangle_{\chi[\overline{\mathfrak{p}}_1]} = C + \sum_{s \in S_{\text{sm}}} \sum_{\tau \in B_s} c_\tau(s) \cdot a^{\text{nc}}_\tau(\overline{\mathfrak{p}}_1, \overline{\mathfrak{p}}_s)$$

for all $\overline{\mathfrak{p}}_1$ in $X_{\text{bp},s}$. Here, the B_s are subsets of G_F representing double cosets, the $c_\tau(s)$ are coefficients, and C is some element of $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$ not depending on $\overline{\mathfrak{p}}_1$. If we take

$$K_{\text{sm}} = K(\mathscr{V}_0 \cup \{\overline{\mathfrak{p}}_s \cap F \,:\, s \in S_{\text{sm}}\}),$$

we find that there is a function

$$f : \text{Gal}(K_{\text{sm}}/F) \to \mathbb{C}$$

with zero average on the coset of $\text{Gal}(K_{\text{sm}}/K(\mathscr{V}_0))$ containing $\sigma_{\text{bp}}(C_{s_1})$ so that

$$f(\text{Frob}\,\overline{\mathfrak{p}}) = \exp\left(2\pi i \cdot \left(\sum_{s \in S_{\text{sm}}} \sum_{\tau} c_\tau(s) \cdot a^{\text{nc}}_\tau(\overline{\mathfrak{p}}, \overline{\mathfrak{p}}_2)\right)\right)$$

for $\overline{\mathfrak{p}} \in X_{\text{bp},s_1}$.

We now wish to apply Theorem 12.10. We can bound the degree $n_{K_{\text{sm}}}$ of $K_{\text{sm}}/\mathbb{Q}$ by $C \cdot \exp(C \cdot |S_{\text{sm}}|)$, and we can bound its discriminant by

$$\left(C \cdot \exp^{(3)}\left(\tfrac{1}{3}\log^{(3)} H\right)\right)^{\exp(C \cdot |S_{\text{sm}}|)} \;\leq\; \exp^{(3)}\left(\left(\tfrac{1}{3} + \tfrac{1}{100} + \epsilon\right)\log^{(3)} H\right),$$

with the last inequality true for sufficiently large H relative to the choice of $\epsilon > 0$, and where we are using

$$\#S_{\text{sm}} \leq (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}}.$$

From the assumption that X does not meet $\mathscr{H}_{\text{bad},6}(H)$, we get that the Dedekind zeta function for K_{sm} has no real zero in the range

$$\left(1 - \frac{c}{n_{K_{\text{sm}}}! \cdot \log x},\, 1\right),$$

with x defined as in Notation 12.3.

We have bounds

$$n_{K_{\text{sm}}}! \cdot \log x \;\leq\; \exp^{(2)}\left(\tfrac{2}{5}\log^{(3)} H\right)^2$$

for all sufficient H. Then Theorem 12.10 applies, and the proposition follows.

□

12.3. **The Chebotarev Density Theorem.** We start by quoting the effective form of the Chebotarev density theorem that we will use.

Theorem 12.10 ([32])**.** *There are absolute effective constants C, c so we have the following:*

Take L/K to be a Galois extension of number fields, take n_L to be the degree of L over $\mathbb{Q}$, and take Δ_L to be the absolute value of the discriminant of L. Take ϕ to be a real valued class function on $G = Gal(L/K)$ of magnitude at most one.

- *The Dedekind zeta function for L has at most one real zero in the interval*

$$[1-\alpha,\, 1] \quad \textit{with } \alpha = \begin{cases} 1/2 & \textit{if } L = \mathbb{Q} \\ 1/(4\log \Delta_L) & \textit{otherwise.} \end{cases}$$

  If this zero exists, it is simple. Take β_0 to be this zero if it exists, and take $\beta_0 = 1/2$ otherwise.

- *Under the assumption*

$$\log N \geq 10 n_L (\log \Delta_L)^2,$$

we have

$$\left| \sum_{\substack{\mathfrak{p} \text{ prime in } K \\ N_{K/\mathbb{Q}}(\mathfrak{p}) \leq N}} \phi(\text{Frob } \mathfrak{p}) \; - \; \frac{1}{|G|} \left(\sum_{\sigma \in G} \phi(\sigma) \right) \text{Li } (N) \right| \leq \text{Li } (N^{\beta_0}) + C n_L N e^{-c\sqrt{\frac{\log N}{n_L}}}.$$

Stronger forms of this theorem are now known (see [52]), but this statement suffices for our purposes. To use this theorem, we need some control on the Siegel zero β_L. Our source on this is [49].

Proposition 12.11. *There exists an absolute effective constant $c > 0$ so we have the following:*

For any $x \geq 2$, there is at most one rational squarefree integer $d_{x,\text{sie}}$ of magnitude at most x such that the zeta function associated to $\mathbb{Q}(\sqrt{d_{x,\text{sie}}})$ has a real zero in the interval

$$\left(1 - \frac{c}{\log x}, \; 1\right).$$

Furthermore, the integer $d_{x,\text{sie}}$ satisfies

$$d_{x,\text{sie}} \; \geq \; c \cdot \log x.$$

Finally, suppose K is a number field of degree n_K and discriminant of magnitude at most x. We assume K does not contain $\mathbb{Q}(\sqrt{d_{x,\text{sie}}})$ if $d_{x,\text{sie}}$ exists. Then the Dedekind zeta function for K contains no zero in the interval

$$\left(1 - \frac{c}{n_K! \cdot \log x}, \, 1\right).$$

Proof. For the first part, suppose $d_1, d_2 < x$ are distinct squarefree rational integers other than 1, and take $L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. $L/\mathbb{Q}$ is then a degree 4 extension of discriminant dividing $2^8(d_1 d_2)^2$. Its Dedekind zeta function is a product of the Riemann zeta function with three Artin L-functions corresponding to the quadratic characters for $\mathbb{Q}(\sqrt{d_1})$, $\mathbb{Q}(\sqrt{d_2})$ and $\mathbb{Q}(\sqrt{d_1 d_2})$. These Artin L-functions are entire. Per the first part of the above theorem, the

Dedekind zeta function for L has at most one zero in the range

$$(1 - (16 \log(4x))^{-1},\ 1).$$

In particular, only one of the three mentioned L-functions can have a zero in this range. The uniqueness of $d_{x,\text{sie}}$ follows by adjusting c. Its effective lower bound follows from [49, Theorem 1], though this result was known earlier; this theorem actually gives the stronger, still-effective statement

$$d_{x,\text{sie}} \geq c(\log x)^2.$$

Finally, the result for $K/\mathbb{Q}$ is a direct consequence of [49, Lemma 8]. □

We note that the discriminant bound in the above argument comes from the following three standard facts given e.g. in [40, Chapter 3.2]:

- Given an extension of number fields L/K, the different $\mathfrak{d}_{L/K}$ is the ideal in $\mathcal{O}_L$ generated by all elements of the form

  $$f'_\alpha(\alpha)$$

  where α ranges over those elements of L for which $L = K(\alpha)$ and f_α is the minimal monic polynomial with coefficients in $\mathcal{O}_K$ having α as a root.
- Given a tower of extensions $M/L/K$ of number fields, we have

  $$\mathfrak{d}_{M/K} = \mathfrak{d}_{M/L} \cdot \mathfrak{d}_{L/K}.$$

- The discriminant $\Delta_{L/K}$ equals $N_{L/K}(\mathfrak{d}_{L/K})$.

For a rational integer d, consideration of the polynomial $x^2 - d$ gives that, for a number field K not containing $\sqrt{d}$, $K(\sqrt{d})/K$ has different dividing $(2\sqrt{d})$. Then $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})/\mathbb{Q}$ has different dividing $(4\sqrt{d_1 d_2})$, and the discriminant bound follows.

13. Bad grids and the proof of Proposition 12.5

13.1. **Preliminary results.** We start with a couple of the propositions we need. We take $(K/F, \mathscr{V}_0, \mathbb{F})$ as above.

Given this information, there are positive constants C, c so that, for C_0 a class of $G_1/\sim$, we have

$$\left| \sum_{\substack{\mathfrak{p} \text{ of } F \\ N_{F/\mathbb{Q}}(\mathfrak{p})<x \\ \text{Frob } \mathfrak{p}=C_0}} 1 \; - \; \frac{|C_0|}{|\text{Gal}(K(\mathscr{V}_0)/F)|} \cdot \text{Li}(x) \right| \leq Cx \exp(-c\sqrt{\log x}) \tag{13.1}$$

for $x \geq 1$. Applying partial summation, we find that there is a function

$$c_{\text{Mert}} : G_1/\sim \; \to \mathbb{R}$$

and a new pair of constants $C, c > 0$ so that, for $x \geq 3$, we have

$$\left| \sum_{\substack{\mathfrak{p} \text{ of } F \\ N_{F/\mathbb{Q}}(\mathfrak{p})<x \\ \text{Frob } \mathfrak{p}\sim C_0}} \frac{1}{N_{F/\mathbb{Q}}(\mathfrak{p})} \; - \; \frac{|C_0|}{|\text{Gal}(K(\mathscr{V}_0)/F)|} \cdot \log\log x \; - \; c_{\text{Mert}}(C_0) \right| \leq C \exp(-c\sqrt{\log x}), \tag{13.2}$$

This is a generalization of one of the Mertens' theorems. We will need a generalization of one of the others as well, though we leave it as the following weak statement: there is some $C > 0$ so, for $x \geq 1$, we have

$$\sum_{\substack{\mathfrak{p} \text{ of } F \\ N_{F/\mathbb{Q}}(\mathfrak{p})<x}} \frac{\log N_{F/\mathbb{Q}}(\mathfrak{p})}{N_{F/\mathbb{Q}}(\mathfrak{p})} \leq C \cdot \log x. \tag{13.3}$$

This can again be proved via partial summation. As a consequence of these statements, we can use an argument due to Hardy and Ramanujan [16] to prove the following upper bound

Proposition 13.1. *Take $(K/F, \mathscr{V}_0, \mathbb{F})$ as above.Then there is some constant $C > 0$ depending just on this information so we have the following:*

Take the notation $\mathscr{H}$ and $d_{\mathbb{F}}$ as before. Suppose we have integers $r > k \geq 0$ and real numbers $x, y > 2$ satisfying

$$y^{k+1} \geq x,$$

and take $\pi_{r,k}(x, y)$ to be the number of ideals $\mathfrak{h}$ in $\mathscr{H}$ of norm at most x that satisfy $\omega(\mathfrak{h}) = r$ and for which $\mathfrak{h}$ is divisible by at least k prime ideals of norm at most y. Then

$$\pi_{r,k}(x, y) \leq \frac{Cx}{\log x} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot \log\log y + C)^k}{k!} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot \log\log x + C)^{r-k-1}}{(r-k-1)!}.$$

Proof. From (13.2) and (13.3), we can follow [16] to show that there is some $C > 0$ so that

$$\sum_{\substack{\mathfrak{p} \in \mathscr{P} \\ N_{F/\mathbb{Q}}(\mathfrak{p}) \leq y}} \frac{\log x}{N_{F/\mathbb{Q}}(\mathfrak{p}) \cdot \log(x/N_{F/\mathbb{Q}}(\mathfrak{p}))} \leq d_{\mathbb{F}}^{-1} \cdot \log\log y + C \tag{13.4}$$

for positive reals x, y satisfying $\sqrt{x} \geq y \geq 2$. The argument from [16] also gives the inequality

$$\pi_{r,0}(x, y) \leq \frac{1}{r-1} \sum_{\substack{\mathfrak{p} \in \mathscr{P} \\ N_{F/\mathbb{Q}}(\mathfrak{p}) \leq \sqrt{x}}} \pi_{r-1,0}\left(\frac{x}{N_{F/\mathbb{Q}}(\mathfrak{p})}, y\right),$$

and we can then use this inequality and (13.4) to inducitvely prove

$$\pi_{r,0}(x, y) \leq \frac{Cx}{\log x} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot \log\log x + C)^{r-1}}{(r-1)!},$$

with (13.1) giving the case $r = 1$.

We also have the relation

$$\pi_{r,k}(x, y) \leq \frac{1}{k} \sum_{\substack{\mathfrak{p} \in \mathscr{P} \\ N_{F/\mathbb{Q}}(\mathfrak{p}) \leq y}} \pi_{r-1,k-1}\left(\frac{x}{N_{F/\mathbb{Q}}(\mathfrak{p})}, y\right),$$

which holds for $k > 0$. Using the above estimate on $\pi_{r,0}$ as a base case, the full proposition can be proved inductively from this relation and (13.4). □

We also need a basic estimate for the binomial distribution.

Proposition 13.2. *Choose p in the interval $(0,1)$, take n a positive integer, and take $X_1, \ldots, X_n$ to be i. i. d. random variables with*

$$X_i = \begin{cases} 1 & \text{with probability } p \\ 0 & \text{with probability } 1-p \end{cases}$$

Then there is a positive real number C depending on p but not on n so that, for any integer a,

$$\Pr\left(\sum_{i\leq n} X_i = a\right) \leq \frac{C}{\sqrt{n}}.$$

In addition, for $\delta \geq 0$, we have

$$\Pr\left(\left|\sum_{i\leq n} X_i \; - \; pn\right| \geq \delta n^{1/2}\right) \leq 2\exp(-2\delta^2).$$

Proof. The second part of this proposition is the form of Hoeffding's inequality given as [42, Theorem 1]. For the first part, assuming a and $n-a$ are both positive, we use Stirling's approximation to say there is an absolute constant $C_0 > 0$ so that

$$\binom{n}{a} p^a (1-p)^{n-a} \leq C_0 \cdot \frac{n^{n+1/2}}{a^{a+1/2}\cdot(n-a)^{n-a+1/2}} p^a (1-p)^{n-a}$$
$$\leq C_0 \cdot \left(\frac{pn}{a}\right)^a \cdot \left(\frac{(1-p)n}{n-a}\right)^{n-a} \cdot \frac{n^{1/2}}{a^{1/2}\cdot(n-a)^{1/2}} \leq C_0 \cdot \frac{n^{1/2}}{a^{1/2}\cdot(n-a)^{1/2}},$$

with the last inequality a consequence of the AM-GM inequality. If

$$|a - pn| \leq \tfrac{1}{2} pn,$$

we can prove the claim of the first part of the proposition with $C = 2C_0(1-p)^{-1}p^{-1}$. Otherwise, we can apply Hoeffding's inequality, getting a different C that still only depends on p. This gives the proposition. □

13.2. **The proof of Proposition 12.5.**

13.2.1. *The case $j = 1$ of Proposition 12.5.* Take $r > (\log^{(2)} H)^2$. The contribution of the portion of $\mathscr{H}_{\text{bad},1}$ with r prime divisors to (12.2) can be bounded by Proposition 13.1. This contribution is at most

$$\frac{H}{\log H} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot \log\log H + C)^{r-1}}{(r-1)!} \cdot \exp\left((1-\epsilon) \cdot r \cdot \log\log\log H\right),$$

where we have absorbed the $\exp(\delta \cdot \omega(\mathfrak{h}))$ term into the a_1 term by potentially shrinking ϵ. Via Stirling's approximation, we can find some new C so this is bounded by

$$\begin{aligned} &\tfrac{H}{\log H} \exp\left(r \cdot C_0 + (2-\epsilon) r \log^{(3)} H - r \log r\right) \\ \leq &\tfrac{H}{\log H} \exp\left(r \cdot C_0 - \epsilon r \log r\right) \leq \tfrac{H}{\log H} \exp(-r), \end{aligned}$$

with the last inequality holding for all r large enough (with respect to ϵ and C_0). This gives the $j = 1$ case of the proposition.

13.2.2. *The case $j = 2$ of Proposition 12.5.* For $j = 2$, we note that there are two reasons an ideal $\mathfrak{h}$ in $\mathscr{H}$ of norm at most H can fail to appear in a grid of ideals of height H:

(1) It can have more than one prime factor from some interval $\mathscr{P}_i(H)$, or

(2) It can share a space X as in (12.1) with an ideal of norm greater than H.

Our starting point is to note that there are constants $C_0, C_1, c > 0$ depending just on F so that, for $N > C_1$, the number of integral ideals of F of norm at most N is within $C_1 N^{1-c}$ of $C_0 N$ (see [39] for a streamlined approach to this old result). From (13.2), we have

$$\sum_{\mathfrak{p} \in \mathscr{P}_i(H)} \frac{1}{N_{F/\mathbb{Q}}(\mathfrak{p})} \leq C \cdot \left(\log\log(a_0 \alpha^{i+1}) - \log\log(a_0 \alpha^i)\right) + C \exp\left(-c\sqrt{\log(a_0 \alpha^i)}\right).$$

for some constants $C, c > 0$ depending on F. Replacing C as necessary, this expression has upper bound

$$\frac{C}{(\log \alpha)^{-1} + i}.$$

As such, the number of ideals of norm at most H with at least two prime divisors from $\mathscr{P}_i(H)$ is bounded by

$$\frac{CH}{((\log \alpha)^{-1} + i)^2}$$

for some C depending just on F. Summing over all i, we see the number of ideals in $\mathscr{H}_{\text{bad},2}(H)$ that are bad for the first reason listed above is bounded by

$$\frac{CN}{\exp^{(3)}\left(\frac{1}{4}\log^{(3)} H\right)}$$

for some C depending on F. If the ideal $\mathfrak{h}$ is in $\mathscr{H}_{\text{bad},2}$ for the second reason, we have

$$H \geq N_{F/\mathbb{Q}}(\mathfrak{h}) \geq H \cdot \alpha^{-\omega(\mathfrak{h})}.$$

Having already restricted $\omega(\mathfrak{h})$ to have upper bound $(\log^{(2)} H)^2$, the number of ideals satisfying can be bounded by

$$\frac{CN}{\left(\exp^{(3)}\left(\frac{1}{4}\log^{(3)} H\right)\right)^{1-\epsilon}},$$

where C depends on F and the positive constant $\epsilon > 0$. From this and the bound $\omega(\mathfrak{h}) \leq (\log^{(2)} H)^2$, we get the claim of the proposition for $j = 2$.

13.2.3. *The case $j = 3$ of Proposition 12.5.* We note that the prime divisors of $\mathfrak{h}$ in a grid that are indexed by S_{sm} are those that are of norm at most y, where y is a positive real satisfying

$$\log\log y = (\log^{(2)} H)^{1/3}.$$

Those indexed by S_{med} have norm at most y, where

$$\log\log y \leq (\log^{(2)} H)^{1/2}$$

for sufficiently large H. We now claim that, for β either $1/2$ or $1/3$ and for ϵ in the interval $(0,1)$, there is some $C>0$ so, for $H>C$,

$$\sum_{j\geq(\log^{(2)} H)^{\beta+\frac{1}{100}}} \exp\left(\tfrac{(1-\epsilon)j}{100}\cdot\log^{(3)} H\right)\cdot\frac{(d_{\mathbb{F}}^{-1}\cdot(\log^{(2)} H)^{\beta}+C_0)^j}{j!}\leq C\cdot\exp^{(2)}\left(\beta\cdot\log^{(3)} H\right)^{-1}$$

and

$$\sum_{r\geq 0}\frac{H}{\log H}\exp(\delta r)\cdot\frac{(d_{\mathbb{F}}^{-1}\cdot\log^{(2)} H+C_0)^r}{r!}\leq\frac{CH}{(\log H)^{\kappa}}$$

The proposition for $j=3$ then follows by multiplying these together and applying Proposition 13.1. The latter claim follows simply from

$$e^x=\sum_{j\geq 0}\frac{x^j}{j!},$$

and the former claim comes from applying Stirling's formula again, so that the summand at j is bounded by

$$\exp\left(j\cdot C_1+\left(\beta+\tfrac{1-\epsilon}{100}\right)\cdot j\cdot\log^{(3)} H-j\log j\right)$$

for some C_1 not depending on H. The estimate follows for sufficient j since

$$j\geq(\log^{(2)} H)^{\beta+1/100}\quad\text{and so}\quad\log j\geq(\beta+1/100)\cdot\log^{(3)} H.$$

13.2.4. *The case $j=4$ of Proposition 12.5.* The contribution to (12.2) from ideals in $\mathscr{H}_{\text{bad},4}(H)$ with r prime divisors is bounded by

$$\frac{H}{\log H}\cdot\frac{(e^{\delta}d_{\mathbb{F}}^{-1}\cdot\log^{(2)} H+C_0)^{r-1}}{(r-1)!}\left(\left(\log^{(2)} H\right)^{\frac{1}{3}+\frac{1}{100}}\cdot\left(\log^{(2)} H\right)^{\frac{2}{3}-\frac{1}{100}-\epsilon}\right),$$

where we are using the fact that these ideals do not have too many small prime divisors. Assume that $r\geq 1$. Using Stirling's approximation, there is C_0 so this is bounded by

$$\frac{H}{\log H}\cdot\exp\left(rC_0+r\log^{(3)} H-r\log r+(\log^{(2)} H)^{1-\epsilon}\right)$$

With $r \leq \log^{(2)} H / \log^{(3)} H$, we calculate

$$r \log^{(3)} H - r \log r \ \leq \ \frac{\log^{(2)} H \cdot \log^{(4)} H}{\log^{(3)} H}$$

for H sufficiently large; this can be proved by noting that

$$-r \log \left(\frac{r}{\log^{(2)} H} \right)$$

increases for r in the range from 1 to

$$\log^{(2)} H \cdot \exp \left(-\frac{1}{\log^{(2)} H} \right)$$

and decreases thereafter. The case $j = 4$ can then be demonstrated directly, with the contribution from $r = 1$ handled separately.

13.2.5. *The case $j = 5$ of Proposition 12.5.* Given a grid X with associated indexing set S, we can apply Hoeffding's inequality and the Chebotarev density theorem, or specifically Proposition 13.2 and (13.1), to say that the number of ideals in X with too few jury primes is bounded by

$$|X| \cdot \left(C \cdot \exp\left(-c|S|^{1/2} \right) \ + \ |S| \cdot \exp^{(3)} \left(\left(\frac{1}{3} - \epsilon \right) \log^{(3)} H \right)^{-1} \right)$$

for ϵ positive and at most $\frac{1}{3}$, for H sufficiently large relative to $(K/F, \mathscr{Y}_0, \mathbb{F})$ and ϵ, and for c and C also determined from this information. The rest follows from

$$|S| \geq \frac{\log^{(2)} H}{\log^{(3)} H} \quad \text{and} \quad |S_{\text{sm}}| \leq \left(\log^{(2)} H \right)^{\frac{1}{3} + \frac{1}{100}}.$$

13.2.6. *The case $j = 6$ of Proposition 12.5.* Suppose $d_{x,\text{sie}}$ exists for

$$x = \exp^{(3)} \left(\tfrac{2}{5} \log^3 H \right).$$

There is then an absolute $c > 0$ so that

$$d_{x,\text{sie}} > c \cdot \exp^{(2)}\left(\tfrac{2}{5}\log^{(3)} H\right).$$

Take d_0 to be the product of all primes dividing $d_{x,\text{sie}}$ that are not divisible by some prime in $\mathscr{V}_0$. Then there is a c determined from $\mathscr{V}_0$ so

$$d_0 > c \cdot \exp^{(2)}\left(\tfrac{2}{5}\log^{(3)} H\right).$$

The ideals $\mathfrak{h}$ in $\mathscr{H}_{\text{bad},6}(H)$ satisfy $\omega_{\text{sm}}(\mathfrak{h}) \leq (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}}$. Taking k to be the number of prime divisors of d_0, we can assume k is then at most this large. We can then bound the number of squarefree ideals of F whose norm divides some power of d_0 by

$$([F:\mathbb{Q}]+1)^k \leq \exp\left(C \cdot (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}}\right),$$

where C depends on F.

The number of ideals in $\mathscr{H}_{\text{bad},6}(H)$ with $r+k$ prime divisors is then bounded by

$$\frac{CH}{d_0 \cdot \log H} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot \log^{(2)} H + C)^r}{r!} \cdot \exp\left(C \cdot (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}}\right).$$

We can then bound (12.2) for $j = 6$ by

$$\frac{CH}{d_0 \cdot \log H} \cdot \exp\left(\left(C + (\log^{(2)} H)^{\frac{1}{15}-\frac{1}{100}-\epsilon}\right) \cdot (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}}\right) \cdot \sum_{r\geq 0} \frac{(e^{\delta} d_{\mathbb{F}}^{-1} \cdot \log^{(2)} H + C)^r}{r!},$$

and the part follows.

If this integer has k prime factors, there are at most

$$([F:\mathbb{Q}]+1)^k$$

If $\mathscr{H}_{\text{bad},5}(H)$ is nonempty, we must have

$$k \leq (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}} + C_0$$

for some C_0 determined from F and $\mathscr{V}_0$. We can then bound the number of ideals in this class by

$$\frac{CH}{\exp^{(2)}\left(\frac{2}{5}\log^{(3)} H\right)} \cdot \exp\left(C \cdot (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}}\right)$$

for $H > C$, where C is some constant determined from $K, F, \mathscr{V}_0$. This is bounded by

$$\frac{CH}{\exp^{(2)}\left(\frac{2}{5}\log^{(3)} H\right)^{1-\epsilon}},$$

where C depends now also on the positive constant ϵ. The case $j = 5$ then follows from

$$\omega_{\text{sm}}(\mathfrak{h}) \leq (\log^{(2)} H)^{\frac{1}{3}+\frac{1}{100}}.$$

13.2.7. *The case $j = 7$ of Proposition 12.5.* We will some variations of Proposition 13.1. If $\sqrt{x} \geq y_2 \geq y_1 \geq 0$, we can follow the same argument as in [16] to show

$$\sum_{\substack{\mathfrak{p}\in\mathscr{P} \\ N_{F/\mathbb{Q}}(\mathfrak{p})\leq y}} \frac{\log x}{N_{F/\mathbb{Q}}(\mathfrak{p}) \cdot \log(x/N_{F/\mathbb{Q}}(\mathfrak{p}))} \leq d_{\mathbb{F}}^{-1} \cdot (\log\log y_2 - \log\log y_1) + C. \tag{13.5}$$

By starting with this and applying the same argument as Proposition 13.1, under the same circumstances as the proposition, we find the number of ideals counted by $\pi_{r,k}(x, y)$ that have exactly k prime factors less than y is bounded by

$$\frac{Cx}{\log x} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot \log\log y + C)^k}{k!} \cdot \frac{(d_{\mathbb{F}}^{-1} \cdot (\log\log x - \log\log y) + C)^{r-k-1}}{(r-k-1)!}. \tag{13.6}$$

We can also restrict the count to products of primes $\mathfrak{p}$ satisfying $\text{Frob}_F \mathfrak{p} = 1$ in $\text{Gal}(K(\mathscr{V}_0)/F)$. Writing d for the degree of this extension, the resulting number of ideals is

$$\frac{Cx}{\log x} \cdot \frac{(d^{-1} \cdot \log\log y + C)^k}{k!} \cdot \frac{(d^{-1} \cdot (\log\log x - \log\log y) + C)^{r-k-1}}{(r-k-1)!}.$$

Following a similar induction argument to Proposition 13.1, we find that the number of ideals in $\mathscr{H}$ with exactly $r_1 > 0$ prime factors satisfying $\mathrm{Frob}_F \mathfrak{p} = 1$, of which exactly k have norm less than y, in addition to $r_2 > 0$ prime factors satisfying $\mathrm{Frob}_F \mathfrak{p} \neq 1$, is bounded by

$$\frac{Cx}{\log x} \cdot \frac{\left((d_{\mathbb{F}}^{-1} - d^{-1}) \log^{(2)} x + C\right)^{r_2}}{(r_2 - 1)!} \cdot \frac{\left(d^{-1} \cdot \log\left(\frac{\log x}{\log y}\right) + C\right)^{r_1 - k}}{(r_1 - k - 1)!} \cdot \frac{\left(d^{-1} \cdot \log^{(2)} y + C\right)^{k}}{k!}.$$

The sum (12.2) over ideals with at most k prime divisors of norm at most y satisfying $\mathrm{Frob}_F \mathfrak{p} = 1$ is then bounded by

$$\frac{Cx}{\log x} \cdot \exp\left(e^{\delta} \cdot \left((d_{\mathbb{F}}^{-1} - d^{-1}) \log^{(2)} x \, + \, d^{-1} \cdot \log\left(\frac{\log x}{\log y}\right) \, + \, C\right)\right) \cdot \sum_{j \leq k} \frac{\left(e^{\delta} \cdot d^{-1} \cdot \log^{(2)} y + C\right)^{j}}{j!}$$

The first part follows from this estimate, and the second part follows similarly.

13.2.8. *The final case of Proposition 12.5.* The case $j = 8$ will follow from basic properties of a multinomial distribution. Choose $k \geq 2$, and take $X_1, X_2, \ldots$ to be a sequence of i.i.d. random variables valued in the set $\{1, \ldots, k\}$, writing p_i for the probability than X_1 equals i for $i \leq k$. We assume all these k probabilities are positive. There is then C determined from k and the p_i so that, for $n > 0$ and $n_1, \ldots, n_k$ summing to n, the probability that

$$\#\{j \leq k \, : \, X_j = 1\} = n_1, \, \ldots, \, \#\{j \leq k \, : \, X_j = k\} = n_k$$

has upper bound $C \cdot n^{-\frac{1}{2}(k-1)}$; this can be seen by applying Proposition 13.2 $k - 1$ times. If $b_1, \ldots, b_k$ are integers not all equal to zero, and if b is also an integer, we can apply this result and Hoeffding's inequality to say that, for $\epsilon > 0$, there is a $C > 0$ so that the probability of

$$\sum_{i \leq k} b_i \cdot \#\{j \leq k \, : \, X_j = i\} = b$$

has upper bound $C \cdot n^{-\frac{1}{2}+\epsilon}$.

Now, take X to be an unfiltered grid of height H. The number of class functions f as in part 7 of Proposition 12.5 is bounded by

$$\exp\left(C \cdot \exp\left(\tfrac{1}{2}\log^{(4)} H\right)\right)$$

for some C depending on the starting data. The number of ideals in $\mathscr{H}_{\text{bad},7}(H)$ in X can then be bounded by

$$|X| \cdot (\log^{(2)} H)^{-\frac{1}{4}+\epsilon},$$

and from this we can finish the proof for $j = 8$, and hence can finish the proof of the proposition. □

14. Proofs of the base-case theorems

14.1. **The parity of Selmer ranks in grids.** Take N to be a twistable module defined with respect to $(K/F, \mathscr{V}_0, \mathbb{F})$, and take $(W_v)_v$ to be a set of local conditions in the sense of Definition 8.5. We will assume that $(N, (W_v)_v)$ is in the alternating case of Notation 9.8, though for the theory below there is no need to assume that $\mathbb{F}$ is a trivial G_F module or that N is potentially favored and uncofavored.

Take

$$\varepsilon : \text{Gal}(K/F(\mathbb{F}(-1))) \longrightarrow \mathbb{F}_2$$

to be the map defined by

$$\varepsilon(\sigma) = \dim H^0(\langle\sigma\rangle, N[\omega]) \mod 2. \tag{14.1}$$

Fix a set of local twists $(\chi_v)_{v\in\mathscr{V}_0}$. From [37, Theorem 6.6] and the subsequent discussion, we know that there is $k_0 \in \mathbb{F}_2$ so that, for $\chi \in \mathbb{X}_F(\infty, (\chi_v)_v)$, we have

$$\dim \text{Sel}^{\omega}(N^{\chi}) = k_0 + \sum_{\mathfrak{p}\mid \mathfrak{h}_F(\chi)} \varepsilon(\text{Frob}\,\mathfrak{p}). \tag{14.2}$$

Definition 14.1. We say that N is in the parity-invariant case if

$$\sum_{\mathfrak{p} | \mathfrak{h}_F(\chi)} \varepsilon(\mathrm{Frob}\,\mathfrak{p}) = 0 \quad \text{for all } \chi \in \mathbb{X}_F\left(\infty,\, (1)_{v \in \mathscr{V}_0}\right).$$

Following the argument of [37], the following always hold:

- If $\ell > 2$, N is in the parity-invariant case if and only if ε is zero.
- If $\ell = 2$ and ε is not a homomorphism, N is not in the parity-invariant case.
- If $\ell = 2$ and there is some homomorphism from $\mathrm{Gal}(K/F)$ to $\mathbb{F}_2$ that restricts to ε, then N is in the parity-invariant case.

The only remaining cases have $\ell = 2$ and $F(\mathbb{F}(-1))/F$ a nontrivial extension, which forces $|\,\mathbb{F}\,|$ to be divisible by four. We opt not to comment further on these cases.

Outside the parity invariant-case, we can show that about half the twists in $\mathbb{X}_F(H, (\chi_v)_v)$ have even Selmer rank, and about half have odd Selmer rank. This is easiest to show in the transition from unfiltered boxes of twists, and relies on the following simple statistical result.

Proposition 14.2. *Given a finite abelian group A and $\epsilon > 0$, there is $c > 0$ so we have the following:*

Take A_0 to be a generating subset of A that contains 0. Choose a positive integer $r \geq 0$, and take $X_1, \ldots, X_r$ to be independent random variables valued in A_0 so, for $a_0 \in A_0$ and $i \leq r$, the probability that X_i takes value a_0 is at least ϵ. Then, for all $a \in A$, we have

$$\left| \Pr\left(\sum_{i \leq r} X_i = a \right) - |A|^{-1} \right| \leq \exp(-cr).$$

Proof. For a random variable X valued in A, take

$$\widehat{X} : \mathrm{Hom}\left(A, \mathbb{C}^\times\right) \longrightarrow \mathbb{C}$$

to be the associated characteristic function

$$\phi \mapsto \sum_{a \in A} \phi(a) \cdot \Pr(X = a).$$

We then find

$$\Pr(X = a) = |A|^{-1} \cdot \sum_{\phi \in \mathrm{Hom}(A, \mathbb{C}^\times)} \phi(-a) \cdot \widehat{X}(\phi)$$

for all $a \in A$. For X, X' independent variables valued in A, we also have $\widehat{X + X'} = \widehat{X} \cdot \widehat{X'}$, and we find

$$\Pr\left(\sum_{i \leq r} X_i = a\right) = |A|^{-1} \cdot \sum_{\phi \in \mathrm{Hom}(A, \mathbb{C}^\times)} \phi(-a) \cdot \left(\prod_{i \leq r} \widehat{X_i}(\phi)\right)$$

From the assumptions on A_0 and $X_1, \ldots, X_r$, we know that there is some $c_0 > 0$ determined from ϵ so that

$$\left|\widehat{X_i}(\phi)\right| \leq 1 - c_0$$

for all nontrivial ϕ and all $i \leq r$. From this estimate and the previous equality, the proposition follows. □

Proposition 14.3. *Take N to be a twistable module in the alternating case but outside the parity-invariant case. There are then real numbers $c, C > 0$ so we have the following:*

Take $H > C$, and suppose that X is an unfiltered grid of ideals of F of height H with associated indexing set $S = S_{\mathrm{sm}} \cup S_{\mathrm{med}} \cup S_{\mathrm{lg}}$. We assume this grid does not meet $\mathscr{H}_{\mathrm{bad},j}(H)$ for $j = 1, 3, 4$. Take $(\chi_v)_{v \in \mathscr{V}_0}$ to be a set of local twists chosen so $\mathbb{X}_F(\infty, (\chi_v)_v)$ is nonzero. Define ε from N as in (14.1)*. Then*

$$\left| \frac{\#\left\{\chi \in \mathbb{X}_F(H, (\chi_v)_v) \,:\, \mathfrak{h}_F(\chi) \in X \text{ and } \sum_{\mathfrak{p} | \mathfrak{h}_F(\chi)} \varepsilon(\mathfrak{p}) \equiv 0\right\}}{\#\left\{\chi \in \mathbb{X}_F(H, (\chi_v)_v) \,:\, \mathfrak{h}_F(\chi) \in X\right\}} - \frac{1}{2} \right| \leq \exp(-c|S|).$$

Proof. Take A to be the abelian group

$$\mathbb{F}_2 \oplus \left(\prod_{v \in \mathscr{V}_0} H^1(G_v, \mathbb{F})\right) \Big/ \mathscr{S}_{\mathbb{F}/F}(\mathscr{V}_0).$$

Take A_0 to be the subset of this group of elements of the form

$$\left(\varepsilon(\mathrm{Frob}_F\overline{\mathfrak{p}}),\ \left(\mathrm{res}_{G_v}\mathfrak{B}^{\mathrm{nc}}_{\mathbb{F},F,\overline{\mathfrak{p}}_s}(x)\right)_v\right),$$

where $\overline{\mathfrak{p}}$ varies through all primes of $\overline{F}$ not over $\mathscr{V}_0$ for which $\mathrm{Frob}_F\overline{\mathfrak{p}}$ acts trivially on $\mathbb{F}(-1)$, and where x varies through all generators of $\mathbb{F}(-1)$.

Because there is an alternating automorphism of $N[\omega]$, we know that $N[\omega]$ has even dimension as an $\mathbb{F}_\ell$ vector space, so

$$\varepsilon(1) = 0.$$

Because of this, we find that A_0 contains 0. In addition, we find that the span of A_0 contains $\mathbb{F}_2 \oplus 0$; this is an equivalent condition to N being outside the parity-invariant case. From our assumptions on the bad ideals allowed in X, we can choose C so that, for $H > C$,

$$|S_{\mathrm{med}} \cup S_{\mathrm{lg}}| \geq \tfrac{1}{2}|S|.$$

For $s \in S_{\mathrm{med}} \cup S_{\mathrm{lg}}$, we have a natural map from

$$\{\chi \in \mathbb{X}_F \ :\ \mathfrak{h}_F(\chi) \in X_s\}$$

to A_0. By the Chebotarev density theorem, if we choose a twist uniformly at random from this set, the probability that it maps to a given $a \in A_0$ has lower bound $\frac{1}{2}|A_0|^{-1}$ so long as H is sufficiently large. The result then follows from Proposition 14.2. □

14.2. **Moment estimates on good grids of twists.** We start by proving Theorem 8.11, a coarse moment estimate on the size of $\mathrm{Sel}^\omega N^\chi$.

Proof of Theorem 8.11. From Proposition 12.4, there is some $c, C > 0$ determined from K/F so that, for $H > C$,

$$\#\mathbb{X}_F(H) \geq \frac{c \cdot H}{(\log H)^\kappa},$$

where we have taken

$$\kappa = 1 - (\ell - 1)\ell^{k-1} \cdot d_{\mathbb{F}}^{-1}.$$

We have the trivial bound

$$\dim \text{Sel}^{\omega}(N^{\chi}) \leq Cg(1 + |S|)$$

for C determined from $(K/F, \mathscr{V}_0, \mathbb{F})$. From this bound and Proposition 12.5, we find that the contribution to the moment from twists in $\mathscr{H}_{\text{bad},j}(H)$ is within the right hand side of (8.5) for $j = 1, 2$ (twists with too many prime factors of their height and twists outside any grid).

We deal with $j = 3, 4, 5, 6$ next. In these cases, it is useful to split the sets of bad twists into grids X_{tw}. We can bound the sum of $\#\text{Sel}^{\omega}N^{\chi}$ over X_{tw} using Proposition 11.13, using Proposition 12.9 to bound the term c_{LS}. Using these estimates, and using the fact that there are at most $\exp(Cg^2)$ choices of $Q_{\text{m},1}$ in Proposition 11.13, the case then follows from Proposition 12.5. We note that the case $j = 3$, in addition to the case $j = 1$ handled above, forced us to assume that g is bounded by $c \cdot \log^{(3)} H$.

Finally, if X_{tw} either a good grid or a grid from $\mathscr{H}_{\text{bad},j}(H)$ with $j = 7, 8$, we can bound the sum of $\#\text{Sel}^{\omega}N^{\chi}$ over X_{tw} by $\exp(Cg^2) \cdot \#X_{\text{tw}}$ using Proposition 11.17 for the unlawful portion and Proposition 11.15, with our bound on c_{Cheb} coming from the second part of Proposition 12.9. From this, we get the proposition. □

We now will focus on twistable modules N in the alternating case and the non-alternating case. The following notation is convenient.

Notation 14.4. Given integers $n \geq j \geq 0$ and a prime ℓ, take $\text{gr}_{\ell}(j, n)$ to equal the number of j-dimensional subspaces of $\mathbb{F}_{\ell}^n$. We can calculate

$$\text{gr}_{\ell}(j, n) = \frac{(\ell^n - 1)(\ell^{n-1} - 1) \dots (\ell^{n-k+1} - 1)}{(\ell^k - 1)(\ell^{k-1} - 1) \dots (\ell - 1)}.$$

Given a twistable module N, we define

$$P_{\text{fav}}(N) = \lim_{H\to\infty} \frac{\#\mathbb{X}^{\text{fav}}_{F,N}(H)}{\#\mathbb{X}_F(H)}.$$

We will later prove that this limit exists.

Proposition 14.5. *Take N to be a twistable module with local conditions $(W_v)_v$ defined with respect to $(K/F, \mathscr{V}_0, \mathbb{F})$. We assume that N is either in the alternating or non-alternating case. Given $\epsilon > 0$, there is then $c, C > 0$ so we have the following:*

Take $H > C$, and take X_{tw} to be a grid of twists of height H. If $P_{\text{fav}}(N) = 1$, we assume that the associated grid of ideals does not meet $\mathscr{H}_{\text{bad},j}(H)$ for $j = 1, \dots, 7$. If $P_{\text{fav}}(N) < 1$, we instead assume that the associated grid of ideals is good. We also assume that X_{tw} is a subset of $\mathbb{X}^{\text{fav}}_{F,N}$. Write $(\chi_v)_{v\in\mathscr{V}_0}$ for the local twists found from restricting any element of X_{tw}.

Take m to be a nonnegative integer that satisfies

$$m \leq (\log^{(2)} H)^{1/8-\epsilon}.$$

Then, defining

$$b(j) = \begin{cases} \frac{j(j+1)}{2} & \text{if } N \text{ is in the alternating case} \\ j \cdot u_{\text{r/c}}(N, (\chi_v)_v) & \text{otherwise,} \end{cases}$$

and taking

$$\text{S}^\chi = \frac{\text{Sel}^\omega N^\chi}{\mathscr{S}^\cap(N, (\chi_v)_v) + \delta_{\chi, G_F}(H^0(G_F, Q))},$$

we find that

$$\sum_{\chi\in X_{\text{tw}}} (\#\text{S}^\chi)^m - |X_{\text{tw}}| \cdot \sum_{j=0}^{m} \text{gr}_\ell(j, m) \cdot \ell^{b(j)}$$

has magnitude less than

$$\exp\left(-(\log\log H)^{1/4-\epsilon}\right) \cdot |X_{\text{tw}}|.$$

Proof. We will consider the Selmer group on $N^{\oplus m}$ whose local conditions are given by $(W_v^{\oplus m})_v$. We will first use

$$\sum_{\chi \in X_{\text{tw}}} (\#\text{Sel}^\omega N^\chi)^m = \sum_{Q_0 \subseteq Q^{\oplus m}} \sum_{\chi \in X_{\text{tw}}} \#\left\{\phi \in \text{Sel}^\omega(N^{\oplus m})^\chi \,:\, \mathbf{Q}(\phi) = Q_0\right\}, \tag{14.3}$$

with the sum being over G_F submodules of $Q^{\oplus m}$, where $Q = N[\omega^2]/N[\omega]$.

From Proposition 9.7, the cofavored submodules of $N^{\oplus m}$ are those of the form

$$A \otimes_{\mathbb{F}_\ell} N[\omega],$$

where A is a subspace of $\mathbb{F}_\ell^m$. If T is a G_F-submodule of $N^{\oplus m}[\omega]$ that is not of this form, Remark 9.4 gives

$$\mathcal{T}_{N^{\oplus m},T}(X_{\text{tw}}) \leq \exp(-(\log\log H)^{1/4-\epsilon}).$$

From this, Proposition 11.17, and Proposition 12.9, we find that the contribution of non-cofavored Q_0 to the right hand side of (14.3) fits in the error of the proposition.

So fix $A \subseteq \mathbb{F}_\ell^m$, and consider the sum

$$\sum_{\chi \in X_{\text{tw}}} \#\left\{\phi \in \text{Sel}^\omega(N^{\oplus m})^\chi \,:\, \mathbf{Q}(\phi) = A \otimes Q\right\}. \tag{14.4}$$

Taking j to be the rank of A, we may change bases so $A = (\mathbb{F}_\ell)^j \oplus 0$, which corresponds to the splitting $N_0 = N_1 \oplus N_2$ with

$$N_0 = N^{\oplus m}, \quad N_1 = N^{\oplus j}, \quad N_2 = N^{\oplus m-j}.$$

Recalling the notation of Proposition 11.18, we take U to be the subset of $(\phi_0, (q_s)_s)$ in

$$\mathscr{S}_{N_0[\omega]/F}(\mathscr{V}_0) \,\oplus\, \mathscr{Q}_{N_0}(Q_1)$$

for which the element defined by

$$\Phi(\phi_0, (q_s)_s) = \phi_0 + \sum_{s \in S} \mathfrak{B}^{\text{nc}}_{N[\omega],F,\bar{\mathfrak{p}}_s}(q_s \cup_{\mathbb{F}} x_s)$$

satisfies the local conditions at $\mathscr{V}_0$, and so that

$$\phi_0 - \delta_{G_F}(\pi_2((q_s)_s))$$

projects to $\mathscr{S}^{\cap}(N_2,\,(\chi_v)_v)$. Take V to be the subspace defined by the same condition in

$$W = \mathscr{S}_{N_0[\omega]/F}(\mathscr{V}_0) \,\oplus\, \mathscr{Q}_{N_0,+}(Q_1).$$

From Proposition 11.18, the difference between (14.4) and

$$\frac{\#\mathscr{S}_{N_0[\omega]/F}(\mathscr{V}_0)\cdot\#V}{\#W}\cdot\big(\#H^0(G_F,N[\omega])\big)^{m-j}\cdot\big(\#H^0(G_F,N[\omega])\big)^{j}\cdot\ell^{b_0}\cdot|X_{\text{tw}}| \tag{14.5}$$

is bounded by

$$\exp\Big(-(\log^{(2)}H)^{1-\epsilon}\Big)\cdot|X_{\text{tw}}|$$

for H sufficiently large, where b_0 is $j(j+1)/2$ in the alternating case and is otherwise zero.

Take

$$W' = \mathscr{S}_{N_0[\omega]/F}(\mathscr{V}_0) \,\oplus\, \bigoplus_{s\in S} H^0(\langle\sigma_s\rangle,\,Q_1).$$
$$W'' = \mathscr{S}_{N_1[\omega]/F}(\mathscr{V}_0) \,\oplus\, \bigoplus_{s\in S} H^0(\langle\sigma_s\rangle,\,Q_1).$$

Then

$$W/V \,\cong\, W'/(V\cap W') \,\cong\, \mathscr{S}_{N_2[\omega]/F}(\mathscr{V}_0)/\mathscr{S}^{\cap}(N_2,\,(\chi_v)_v) \,\oplus\, W''/(V\cap W'').$$

Choose any χ in X_{tw}, and take $\mathscr{V}$ to be the set of places where χ ramifies outside $\mathscr{V}_0$. Then W'' is identified with $\mathscr{S}_{N_1[\omega]/F}(\mathscr{V}\cup\mathscr{V}_0)$, and $V\cap W''$ is identified with the kernel of the map

$$\mathscr{S}_{N_1[\omega]/F}(\mathscr{V}\cup\mathscr{V}_0)\to\prod_{v\in\mathscr{V}_0}H^1(G_v,N_1[\omega])\Big/W_v(\chi_v)^{\oplus j}.$$

Then $W''/(V \cap W'')$ has order equal to the image of this map. This image is identified with

$$\left(\frac{\#\mathscr{S}_{M/F}(\mathscr{V}_0) \cdot \#Ш_1(F,M) \cdot \prod_{v \in \mathscr{V}} \#H^1(I_v,M)^{G_v/I_v}}{\#\ker\Big(H^1(G_F,M) \to \prod_{v\in\mathscr{V}_0} H^1(G_v,M)/W_v(\chi) \times \prod_{v\notin\mathscr{V}\cap\mathscr{V}_0} H^1(I_v,M)\Big)} \right)^{\oplus j}.$$

The proposition then follows as a consequence of (9.11). □

14.3. **The proofs of the base-case Selmer rank theorems.** We now finally justify the double definition we gave of potentially favored twistable module.

Proposition 14.6. *Suppose N is a twistable module defined from the data $(K/F, \mathscr{V}_0, \mathbb{F})$. Take*

$$(Y_\sigma)_{\sigma\in G_1}$$

to be a multivariate normal distribution with covariance matrix Σ satisfying

$$\Sigma_{\sigma_1,\sigma_2} = \begin{cases} d^{-1}(1-d^{-1}) & \text{if } \sigma_1 = \sigma_2 \\ -d^{-2} & \text{if } \sigma_1 \neq \sigma_2, \end{cases}$$

with d equal to the degree of the extension G_1. Take $P_{0,\text{fav}}(N)$ to be the probability that

$$\sum_{\sigma\in G_1} (1+\epsilon\cdot Y_\sigma)\cdot \dim H^0(\langle\sigma\rangle,\, N[\omega]) \geq \sum_{\sigma\in G_1} (1+\epsilon\cdot Y_\sigma)\cdot \dim H^0(\langle\sigma\rangle,\, (N/T)[\omega]).$$

holds for all G_F-submodules T of $N[\omega]$ and all $\epsilon \geq 0$.

Then

$$P_{\text{fav}}(N) = P_{0,\text{fav}}(N).$$

Proof. Take X to be an unfiltered grid of ideals of height H that does not meet $\mathscr{H}_{\text{bad},j}(H)$ for $j = 1, 3, 4$. It suffices to prove that, among the twists χ in $\mathbb{X}_F\big(H,\,(\chi_v)_v\big)$ satisfying

$\mathfrak{h}(\chi)$, the proportion which favor N is $P_{\text{fav}}(N)$ with error going to zero as H goes to infinity, as we can use Proposition 12.5 to see that the set of remaining twists is negligible.

Take $S = S_{\text{sm}} \cup S_{\text{med}} \cup S_{\text{lg}}$ to be the indexing set of S, and take

$$S_1 = S_{\text{med}} \cup S_{\text{lg}}.$$

As a consequence of the Chebotarev density theorem, we can remove $o(H) \cdot |S|^{-1} \cdot |X_s|$ primes from X_s for each $s \in S_1$ to force

$$\#\{\mathfrak{p} \in X_s \ : \ \text{Frob}\,\mathfrak{p} = C_0\} = |X_s| \cdot \frac{|C_0|}{|G_1|}$$

for all $s \in S$ and any class C_0 of $G_1/\sim$. Take X' to be the product of these sets; we see that X has at most $o(H) \cdot |X|$ ideals not contained in X'.

Define a random function

$$Y : G_1/\sim \ \to \mathbb{Z}$$

by

$$Y(\mathfrak{h})(C) = \#\left\{\mathfrak{p}|\mathfrak{h}(\chi) \ : \ \mathfrak{p} \in \bigcup_{s \in S_1} X_s, \ \text{Frob}\,\mathfrak{p} = C\right\},$$

where $\mathfrak{h}$ is chosen uniformly at random from X'. Equivalently, this is a multinomial distribution where the probability of C is $|C|/|G_1|$, and we consider the adjustment

$$Y'(C) = Y(C) - \tfrac{|C| \cdot |S_1|}{|G_1|}$$

Per the multivariate central limt theorem (see [46, 2.7]), we find that the random function

$$C \mapsto |S_1|^{-1/2} \cdot Y'(C)$$

converges to the random function

$$C \mapsto \sum_{\sigma \in C} Y_\sigma(C)$$

as $|S_1|$ heads to infinity. The probability that a twist from X' is favorable with respect only to the primes indexed by S_1 is thus given by $P_{\text{fav}}(N)$. Since

$$\#S_{\text{sm}} = o\left(\#S_1^{1/2}\right),$$

the same is true when we adjoin the primes in S_{sm}. □

Remark 14.7. With some additional work, this last proposition can be made to apply to twists in sets $\mathbb{X}_F(H,\ (\chi_v)_v)$ with local constrictions. The same probabilities are recovered.

To move from moments to ranks, we will follow the trend of the literature and use a brief argument in the theory of holomorphic functions. In particular, the argument given below is quite similar to the proof of Lemma 18 in [18].

Proposition 14.8. *There is $C > 0$ so we have the following:*

Take $a_0, a_1, \dots$ and $b_0, b_1, \dots$ to be sequences of nonnegative real numbers, and take

$$F(z) = \sum_{i \geq 0} a_i z^i \quad \textit{and} \quad G(z) = \sum_{i \geq 0} b_i z^i.$$

Choose $\epsilon > 0$, $C_0 > 0$, a positive integer m, and a prime ℓ.

- *Suppose that we have*

$$F(\ell^{m+1}),\ G(\ell^{m+1}) \leq \ell^{C_0 m + \frac{1}{4}m^2}$$

and

$$|F(z) - G(z)| \leq \epsilon \quad \textit{for } z \in \{1, \ell, \dots, \ell^m\}.$$

Then

$$|a_i - b_i| \leq \ell^{Cm}\left(\epsilon + \ell^{C_0 m - \frac{1}{4}m^2}\right) \quad \textit{for } i \geq 0.$$

- *Suppose that we have*

$$F(\ell^{m+1}),\ G(\ell^{m+1}) \leq \ell^{C_0 m + \frac{1}{2}m^2}$$

and

$$|F(z) - G(z)| \leq \epsilon \quad \textit{for } z \in \{\pm 1, \pm \ell, \ldots, \pm \ell^m\}.$$

Then

$$|a_i - b_i| \leq \ell^{Cm} \left(\epsilon + \ell^{C_0 m - \frac{1}{2}m^2}\right) \quad \textit{for } i \geq 0.$$

Proof. By replacing m with the nonnegative integer $m-1$ if necessary, we can assume that F and G are holomorphic on an open disk containing the circle of radius ℓ^{m+1}.

For the first case, we will make use of the definitions

$$\begin{aligned}
R(z) &= \prod_{i=0}^{m} \left(1 - \frac{z}{\ell^i}\right), \\
R_j(z) &= \left(1 - \frac{z}{\ell^j}\right)^{-1} \cdot R(z) \text{ for } j \leq k, \\
H(z) &= F(z) - G(z) - \sum_{j \leq m} \frac{F(\ell^j) - G(\ell^j)}{R_j(\ell^j)} R_j(z).
\end{aligned}$$

$H(z)$ has zeros at $1, \ell, \ldots, \ell^k$, and hence can be written in the form $H_1(z)R(z)$, where H_1 is holomorphic on any open set where F and G are holomorphic.

Since $(1 - \ell^{j-i})$ is an integer for $j > i$, we have the bound

$$\left|R_j(\ell^j)\right| \geq \prod_{i=j+1}^{m} \left(1 - \frac{\ell^j}{\ell^i}\right) \geq \prod_{i=1}^{\infty} \left(1 - 2^{-i}\right) > 0$$

for all $j \leq m$. This gives an absolute lower bound for the magnitude of $R_j(\ell^j)$.

For $i \geq 1$, we have $\ell^i - 1 \geq \ell^{i-1}$. We consequently have

$$|R(z)| \geq \prod_{i=0}^{m} \ell^{m-i} = \ell^{\frac{m(m-1)}{2}}$$

for all z satisfying $|z| = \ell^{m+1}$. For z on the same circle, we have

$$|R_j(z)| \leq \ell^{\frac{(m+2)(m+1)}{2}}$$

for $j \leq m$, as follows from the estimate $\ell^i + 1 \leq \ell^{i+1}$.

From these estimates and the assumptions on F and G, we find there is some absolute $C_1 > 0$ so that, for all z satisfying $|z| = \ell^{m+1}$, we have

$$|H_1(z)| \leq \ell^{C_1(m+1)} \cdot \left(\epsilon + \ell^{-\frac{1}{4}m^2 + C_0 m}\right).$$

Writing $H_1(z)$ in the form

$$\sum_{i \geq 0} c_i z^i,$$

we have

$$c_i \leq \ell^{(-i+C_1)(m+1)} \cdot \left(\epsilon + \ell^{-\frac{1}{4}m^2 + C_0 m}\right)$$

from Cauchy's integral formula.

Writing

$$\prod_{i=0}^{\infty} \left(1 - \frac{z}{\ell^i}\right) = \sum_{i \geq 0} d_i z^i,$$

we see that

$$\sum_{i \geq 0} |d_i| \leq \prod_{i=0}^{\infty} \left(1 + 2^{-i}\right) < \infty.$$

From this absolute bound, we can bound the i^{th} coefficient of the power series expansion of H using the above bounds on c_i. After noting that the coefficients of

$$\sum_{j \leq m} \frac{F(\ell^j) - G(\ell^j)}{R_j(\ell^j)} R_j(z).$$

are bounded by some constant times $(m+1)\epsilon$, we can derive the bound for the coefficients of the power series expansion of $F - G$ that is claimed in the proposition.

The second part follows the same argument starting from the alternative function

$$R(z) = \prod_{i=0}^{m} \left(1 - \frac{z}{\ell^i}\right) \left(1 + \frac{z}{\ell^i}\right).$$

□

Proof of Theorem 9.10 and Theorem 9.14. We will give the main argument in the non-alternating case. Take

$$u = u_{\text{r/c}}\left(N,\ (\chi_v)_v\right).$$

We start by noting that, if we take

$$G(z) = \sum_{r \geq 0} \lim_{n \to \infty} P^{\text{Mat}}_{\ell,\,u}(r|n) \cdot z^r,$$

then, for $m \geq 0$, we have

$$G(\ell^m) = \cdot \sum_{j=0}^{m} \text{gr}_\ell(j, m) \cdot \ell^{u \cdot j}.$$

There is some C_0 determined from u but not m so this has upper bound $\ell^{\frac{1}{4}m^2 + C_0 m}$ for $m \geq 1$.

Then, given a grid of twists X_{tw} of height H as in Proposition 14.5, we can apply Proposition 14.8 with

$$m = (\log^{(2)} H)^{1/8-\epsilon}$$

to say that

$$\#\{\chi \in X_{\text{tw}} \ :\ \text{Sel}^\omega N^\chi = r + r_0\} - \lim_{n \to \infty} P^{\text{Mat}}_{\ell,\,u} \cdot \#X_{\text{tw}} \leq \#X_{\text{tw}} \exp\left(-(\log^{(2)} H)^{1/4-\epsilon}\right),$$

for $H \geq C$, where C depends on N and ϵ.

Combining this with Proposition 12.5 then gives the theorem.

The alternating case is much the same, and only requires the observation that the Selmer rank parity is constant for twists from X_{tw}, which allows us to apply Proposition 14.8. $\square$

REFERENCES

[1] M. Bhargava, D. M. Kane, H. W. Lenstra, Jr., B. Poonen, and E. Rains. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. *Cambridge Journal of Mathematics.*, 3(3):275–321, 2015.

[2] M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver, and A. Shnidman. Three-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field. *arXiv preprint arXiv:1709.09790*, 2017.

[3] V. Blomer, L. Goldmakher, and B. Louvel. l-functions with n-th-order twists. *International Mathematics Research Notices*, 2014(7):1925–1955, 2014.

[4] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[5] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, pages 405–420, 1971.

[6] L. E. Dickson. *History of the Theory of Numbers*, volume 2. Carnegie Institution Washington, DC, 1920.

[7] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*. Springer Science & Business Media, 1995.

[8] M. Flach. A generalisation of the Cassels-Tate pairing. *Journal für die reine und angewandte Mathematik*, 412:113–127, 1990.

[9] É. Fouvry and J. Klüners. On the 4-rank of class groups of quadratic number fields. *Inventiones mathematicae*, 167(3):455–513, 2007.

[10] J. Friedlander, H. Iwaniec, B. Mazur, and K. Rubin. The spin of prime ideals. *Inventiones mathematicae*, 193(3):697–749, 2013.

[11] E. Friedman. Analytic formulas for the regulator of a number field. *Inventiones mathematicae*, 98(3):599–622, 1989.

[12] F. Gerth. The 4-class ranks of quadratic fields. *Inventiones mathematicae*, 77(3):489–515, 1984.

[13] D. Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number Theory Carbondale 1979*, pages 108–118. Springer, 1979.

[14] L. Goldmakher and B. Louvel. A quadratic large sieve inequality over number fields. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 154, pages 193–212. Cambridge University Press, 2013.

[15] B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Inventiones mathematicae*, 84(2):225–320, 1986.

[16] G. H. Hardy and S. Ramanujan. The normal number of prime factors of a number n. *The Quarterly Journal of Mathematics*, 48:76–92, 1917.

[17] D. Heath-Brown. A mean value estimate for real character sums. *Acta Arithmetica*, 72(3):235–275, 1995.

[18] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem, II. *Inventiones mathematicae*, 118(1):331–370, 1994.

[19] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[20] B. W. Jordan, Z. Klagsbrun, B. Poonen, C. Skinner, and Y. Zaytman. Statistics of K-groups modulo p for the ring of integers of a varying quadratic number field. *arXiv preprint arXiv:1703.00108*, 2017.

[21] M. Jutila. On mean values of Dirichlet polynomials with real characters. *Acta Arithmetica*, 27(1):191–198, 1975.

[22] D. Kane. On the ranks of the 2-Selmer groups of twists of a given elliptic curve. *Algebra & Number Theory*, 7(5):1253–1279, 2013.

[23] D. Kane and Z. Klagsbrun. On the joint distribution of $\mathrm{Sel}_\phi(E/\mathbb{Q})$ and $\mathrm{Sel}_{\phi'}(E'/\mathbb{Q})$ in quadratic twist families. *arXiv preprint arXiv:1702.02687*, 2017.

[24] Z. Klagsbrun and R. J. Lemke Oliver. The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point. *Research in the Mathematical Sciences*, 1(1):15, 2014.

[25] Z. Klagsbrun, B. Mazur, and K. Rubin. A markov model for Selmer ranks in families of twists. *Compositio Mathematica*, 150(7):1077–1106, 2014.

[26] J. Klys. The distribution of p-torsion in degree p cyclic fields. *arXiv preprint arXiv:1610.00226*, 2016.

[27] V. Kolyvagin. Euler systems. In *The Grothendieck Festschrift*, pages 435–483. Springer, 2007.

[28] V. A. Kolyvagin and D. Y. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[29] P. Koymans and D. Milovic. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \bmod 4$. *International Mathematics Research Notices*, 2018. Advanced access.

[30] P. Koymans and C. Pagano. On the distribution of $\mathrm{Cl}(K)[\ell^\infty]$ for degree ℓ cyclic fields. *arXiv preprint arXiv:1812.06884*, 2018.

[31] D. Kriz. Supersingular main conjectures, Sylvester's conjecture and Goldfeld's conjecture. *arXiv preprint arXiv:2002.04767*, 2020.

[32] J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Fröhlich, editor, *Algebraic Number Fields: L-functions and Galois properties*, London, 1977. Academic Press.

[33] S. Louboutin. Explicit bounds for residues of Dedekind zeta functions, values of L-functions at $s = 1$, and relative class numbers. *Journal of Number Theory*, 85(2):263–282, 2000.

[34] B. Mazur, K. Rubin, and A. Silverberg. Twisting commutative algebraic groups. *Journal of Algebra*, 314(1):419–438, 2007.

[35] J. S. Milne. On the arithmetic of abelian varieties. *Inventiones Mathematicae*, 17:177–190, 1972.

[36] J. S. Milne. *Arithmetic duality theorems*, volume 1 of *Perspectives in Mathematics*. Academic Press, Inc., Boston, MA, 1986.

[37] A. Morgan. Quadratic twists of abelian varieties and disparity in Selmer ranks. *arXiv preprint arXiv:1706.06063*, 2017.

[38] D. Mumford. On the equations defining abelian varieties. I. *Inventiones mathematicae*, 1(4):287–354, 1966.

[39] M. R. Murty and J. Van Order. Counting integral ideals in a number field. *Expositiones Mathematicae*, 25(1):53–66, 2007.

[40] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften*. Springer, 1999.

[41] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2008.

[42] M. Okamoto. Some inequalities relating to the partial sum of binomial probabilities. *Annals of the Institute of Statistical Mathematics*, 10(1):29–35, 1959.

[43] B. Poonen and E. Rains. Self cup products and the theta characteristic torsor. *Mathematical Research Letters*, 18(6):1305–1318, 2011.

[44] B. Poonen and E. Rains. Random maximal isotropic subspaces and Selmer groups. *Journal of the American Mathematical Society*, 25(1):245–269, 2012.

[45] B. Poonen and M. Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Annals of Mathematics*, 150(3):1109–1149, 1999.

[46] R. J. Serfling. *Approximation theorems of mathematical statistics*, volume 162. John Wiley & Sons, 1980.

[47] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[48] A. Smith. 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. *arXiv preprint arXiv:1702.02325*, 2017.

[49] H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Inventiones mathematicae*, 23(2):135–152, 1974.

[50] P. Swinnerton-Dyer. The effect of twisting on the 2-Selmer group. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 145, pages 513–526. Cambridge Univ Press, 2008.

[51] J. Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, Djursholm, 1963.

[52] J. Thorner and A. Zaman. A unified and improved Chebotarev density theorem. *arXiv preprint arXiv:1803.02823*, 2018.

[53] C. Weibel. Algebraic K-theory of rings of integers in local and global fields. *Handbook of K-theory*, pages 139–190, 2005.

[54] A. Weiss. The least prime ideal. *Journal für die reine und angewandte Mathematik.*, 338:56–94, 1983.

[55] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.

[56] A. Wiles. The Birch and Swinnerton-Dyer conjecture. *The Millennium Prize Problems*, page 29, 2006.

[57] W. Zhang. Selmer groups and the indivisibility of Heegner points. *Cambridge Journal of Mathematics*, 2(2):191–253, 2014.