Anticyclotomic Iwasawa Theory for Modular Forms

by

Trevor S Arnold

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Mathematics) in the University of Michigan 2006

Doctoral Committee:

Professor Christopher M Skinner, chair
Professor Brian D Conrad
Associate Professor Stephen M DeBacker
Assistant Professor Nicholas A Ramsey
Assistant Professor Martin J Strauss
INFORMATION TO USERS

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleed-through, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

UMI Microform 3224810
Copyright 2006 by ProQuest Information and Learning Company.
All rights reserved. This microform edition is protected against unauthorized copying under Title 17, United States Code.

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
to the memory of Margaret Hubbard Jones
Acknowledgements

I am grateful to Chris Skinner for his guidance and insight and to Brian Conrad for his devotion to my education. Both are mathematicians of extraordinary vision and serve as examples towards which I direct my aspirations; their influence on my mathematical development cannot be overstated. I would also like to thank my committee members Stephen DeBacker, Nick Ramsey, and Martin Strauss.

I have benefitted greatly from interaction with the algebraic number theorists at Michigan, especially Mahesh Agarwal, Eiji Aoki, Tobias Berger, Bryden Cais, Ellen Eischen, Wansu Kim, Kris Kloosin, Tong Liu, Mihran Papikian, James Parson, Sreekar Shastry, and Xin-yun Sun; their comraderie and perspective have proved invaluable. The students in algebraic geometry and commutative algebra at Michigan have been very supportive of my interest in their field; among them I am particularly fortunate to count as friends Hai Long Dao, Afsaneh Mehran, and Cornelia Yuen.

My extra-mathematical life has provided a great deal of variety to my graduate school experience, so thanks to Andreea Boboc, Chih-long Hu, Cyan James, and Amy Kiefer. Throughout my education, my family has somehow managed to stand behind me without looking over my shoulder; for this they deserve a great deal of credit. Finally, Sarah Iveson has done a great deal for me, perhaps more than she is aware. I reward her thus: <3.
Contents

Dedication ii

Acknowledgements iii

CHAPTER 1. Introduction 1
1.1. Motivation: the conjecture of Birch and Swinnerton-Dyer 1
1.2. Iwasawa theory 4
1.3. The method 6
1.4. Iwasawa theory of CM forms 8
1.5. Iwasawa theory for Hida families 9

CHAPTER 2. CM forms 11
2.1. Notation and definitions 11
2.2. Divisibility from Euler systems 21
2.3. Divisibility from descent 35
2.4. $p$-adic heights and the linear term 46

CHAPTER 3. Hida families 66
3.1. Background 66
3.2. The Euler system argument 75
3.3. Descent from the nearly ordinary Hecke algebra 78

Bibliography 80
CHAPTER 1

Introduction

Let $M$ be an arithmetic object, by which we mean an object which arises from a collection of polynomials with coefficients in $\mathbb{Q}$. For example, $M$ could be a number field, which arises from an irreducible polynomial in 1 variable, or an elliptic curve, which arises from a polynomial of the form $y^2 = x^3 + Ax + B$. Several invariants have been introduced in order to study the structure of such objects. It has been a major theme in algebraic number theory in recent years to study how the $L$-function $L(M, s)$ of $M$ (an analytic invariant) is related to the Selmer group $\text{Sel}(M)$ of $M$ (an algebraic invariant).

This thesis is concerned with the arithmetic of modular forms, i.e., we take $M$ to be an elliptic cuspidal newform. The purpose of this introductory chapter is twofold. First, we explain how Iwasawa theory, and in particular anticyclotomic Iwasawa theory, allows one to relate the $L$-functions and Selmer groups attached to $M$. Second, we describe the results and conjectures that will be presented in Chapters 2 and 3. We give few precise definitions and statements here, relegating technicalities to the later chapters.

1.1. Motivation: the conjecture of Birch and Swinnerton-Dyer

Let $E$ be an elliptic curve over $\mathbb{Q}$. The classical Mordell-Weil theorem states that $E(\mathbb{Q})$ is a finitely generated abelian group, the torsion subgroup of which can be calculated without serious difficulty. Thus, in order to determine the structure of $E(\mathbb{Q})$ explicitly, it remains to calculate the rank $r_E = \dim_{\mathbb{Q}} E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$. The
conjecture of Birch and Swinnerton-Dyer predicts that this rank can be calculated in terms of the \( L \)-function \( L(E, s) \) associated to \( E \).

**Conjecture 1.1.1** (Birch and Swinnerton-Dyer). For any elliptic curve \( E \) defined over \( \mathbb{Q} \),

\[ r_E = \text{ord}_s L(E, s). \]

Perhaps the most successful known approach to Conjecture 1.1.1 is via the Galois cohomology of \( E \). Let \( p \) be a rational prime and consider the Kummer sequence

\[ 0 \longrightarrow E[p^n] \longrightarrow E \overset{\times p^n}{\longrightarrow} E \longrightarrow 0. \]

The associated long exact sequence in Galois cohomology gives rise to the short exact sequence

\[ 0 \longrightarrow E(\mathbb{Q})/p^n E(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E[p^n]) \longrightarrow H^1(\mathbb{Q}, E)[p^n] \longrightarrow 0 \]

for every integer \( n \). Taking the direct limit of these groups as \( n \) grows gives the short exact sequence

\[ (1.1.1) \quad 0 \longrightarrow E(\mathbb{Q}) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(\mathbb{Q}, E[p^\infty]) \longrightarrow H^1(\mathbb{Q}, E)[p^\infty] \longrightarrow 0 \]

The first term in this sequence is isomorphic to \((\mathbb{Q}_p/\mathbb{Z}_p)^{r_E}\), so our interest in \( r_E \) leads naturally to the study of the remaining two terms. However, \( H^1(\mathbb{Q}, E[p^\infty]) \) is intractable as an object of study, in the sense that its Pontryagin dual\(^1\) is not finitely generated over \( \mathbb{Z}_p \). It is therefore common practice to consider the subgroup of \( H^1(\mathbb{Q}, E[p^\infty]) \) whose restrictions to the local cohomology groups \( H^1(\mathbb{Q}_t, E[p^\infty]) \) lie in the image of the map

\[ E(\mathbb{Q}_t) \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1(\mathbb{Q}_t, E[p^\infty]). \]

\(^1\)The Pontryagin dual of a \( \mathbb{Z}_p \)-module \( M \), which we denote by \( M^\vee \), is \( \text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p) \).
for every prime ℓ. The subgroup of such classes is called the Selmer group associated to E and is denoted Sel(Q, E[p∞]). We then get an exact sequence

\[(1.1.2) \quad 0 \rightarrow E(\mathbb{Q}) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \rightarrow \text{Sel}(\mathbb{Q}, E[p^\infty]) \rightarrow \text{III}(E/\mathbb{Q})[p^\infty] \rightarrow 0,\]

where III(E/\mathbb{Q})[p^\infty] is the image of Sel(\mathbb{Q}, E[p^\infty]) under the map H^1(\mathbb{Q}, E[p^\infty]) \rightarrow H^1(\mathbb{Q}, E)[p^\infty]. The advantage of (1.1.2) over (1.1.1) is that Sel(\mathbb{Q}, E[p^\infty]) is a cofinitely generated \(\mathbb{Z}_p\)-module (i.e., its Pontryagin dual is finitely generated) and it is a standard conjecture that III(E/\mathbb{Q})[p^\infty] is finite. Assuming that III(E/\mathbb{Q})[p^\infty] is finite, we arrive at a restatement of Conjecture 1.1.1

**Conjecture 1.1.2.** For any elliptic curve E defined over \(\mathbb{Q}\),

\[\text{rk}_{\mathbb{Z}_p} \text{Sel}(\mathbb{Q}, E[p^\infty])^{\vee} = \text{ord}_{s=1} L(E, s).\]

The value of this restatement is that the tools of Galois cohomology can be brought to bear on the problem, as both the L-function \(L(E, s)\) and the Selmer group Sel(\mathbb{Q}, E[p^\infty]) can be defined entirely in terms of the \(p\)-adic Tate module \(T_p(E) = \varprojlim E[p^n]\), viewed as a \(\mathbb{Z}_p[G_\mathbb{Q}]\)-module.

Another benefit of Conjecture 1.1.2 is that the statement can easily be generalized to a conjecture about any \(p\)-adic Galois representation \(\rho : G_F \rightarrow \text{GL}_n(\mathbb{Z}_p)\) over a number field \(F\) which "arises from geometry", in the sense that it is attached to an arithmetic object \(M\). Let \(T\) be the representation space of \(\rho\) and set \(W = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p\). Bloch-Kato, Greenberg, and others have introduced a systematic way of defining local conditions \(H^1_t(F_v, W) \subseteq H^1(F_v, W)\) for places \(v\) of \(F\). As in the case of elliptic curves, we can define the subgroup Sel(\(F, W\)) \subseteq H^1(F, W) of classes whose restrictions to \(H^1(F_v, W)\) lie in the local conditions \(H^1_t(F_v, W)\) for every place \(v\) of \(F\). If \(\rho = \rho_{E,p}\) gives the action of \(G_\mathbb{Q}\) on the Tate module of an elliptic curve \(E\) over \(\mathbb{Q}\), we have that \(T = T_p(E),\ W = E[p^\infty]\), and the resulting Selmer group Sel(\(\mathbb{Q}, W\)) is the same as the one which appears in Conjecture 1.1.2. To \(\rho\) is also associated an L-function \(L(\rho, s)\) which, initially defined in terms of an Euler product converging on
some half-plane \( \{ s \in \mathbb{C} \mid \text{Re}(s) > 0 \} \), can conjecturally be extended to a meromorphic function defined on all of \( \mathbb{C} \) which satisfies a functional equation relating the values \( L(\rho, s) \) and \( L(\rho^*, k - s) \) for some integer \( k \), where \( \rho^* \) is the Tate dual representation \( \rho^* = \text{Hom}(\rho, \mathbb{Z}_p(1)) \). One can then make a conjecture similar to Conjecture 1.1.2 relating the \( \mathbb{Z}_p \)-rank of \( \text{Sel}(F, W)^\vee \) and the order of vanishing of \( L(\rho, s) \) at its central point \( s = k/2 \).

### 1.2. Iwasawa theory

One method for attacking such problems is Iwasawa theory, which is, roughly speaking, the study of how Selmer groups behave with respect to certain towers of extensions of \( F \). Let \( M \) be an arithmetic object as above and let \( \rho_M \) be its associated \( p \)-adic Galois representation, with \( T \) and \( W \) likewise as above. Choose an (infinite) Galois extension \( F_\infty/F \) such that Galois group \( \text{Gal}(F_\infty/F) \) is isomorphic to the group of \( p \)-adic integers \( \mathbb{Z}_p \). Then \( F_\infty = \bigcup F_n \), where \( \text{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z} \). One then defines the Iwasawa-theoretic Selmer group \( \text{Sel}(F_\infty, W) \) as the limit (in a suitable sense) of the groups \( \text{Sel}(F_n, W) \); \( \text{Sel}(F_\infty, W) \) can be related to the “usual” Selmer group \( \text{Sel}(F, W) \) by various descent arguments commonly referred to as control theorems.

As \( M \) is defined over \( F \), the \( \mathbb{Z}_p \)-module \( \text{Sel}(F_\infty, W) \) carries a continuous action of \( \Gamma = \text{Gal}(F_\infty/F) \) and can thus be considered as a module over the completed group ring \( \Lambda = \mathbb{Z}_p[[\Gamma]] \), called the Iwasawa algebra of \( F_\infty/F \).

Iwasawa theory is concerned with the structure of \( \text{Sel}(F_\infty, W)^\vee \) as a \( \Lambda \)-module. The structure theory of finitely generated modules over \( \Lambda \) is the same, up to finite error, as that for finitely generated modules over a PID. In particular, when the Selmer group \( \text{Sel}(F_\infty, W)^\vee \) is a finitely generated \( \Lambda \)-module (as is frequently the case), there is a homomorphism with finite kernel and cokernel from \( \text{Sel}(F_\infty, W)^\vee \) to a sum of cyclic modules

\[
\Lambda^\vee \oplus \bigoplus_{i=1}^n \Lambda/(f_i).
\]
The positive integer $r$ (the rank) and the ideal $(\prod f_i)$ are uniquely determined. When the rank is 0, $(\prod f_i)$ is called the characteristic ideal of $\text{Sel}(F_\infty, W)^\vee$. (When the rank is positive, the characteristic ideal is defined to be 0.)

On the analytic side, there are, for a few special choices of $M$, $F$, and $F_\infty$, elements $L_p(M) \in \Lambda$ called $p$-adic $L$-functions which $p$-adically interpolate special values of the classical $L$-functions $L(M \otimes \phi, s)$ associated to twists of $M$ by characters $\phi$ of $\text{Gal}(F_\infty/F)$.

One goal of Iwasawa theory is to prove the so-called “main conjecture” for $M$ by determining the $\Lambda$-rank of $\text{Sel}(F_\infty, W)^\vee$ and expressing the characteristic ideal of the $\Lambda$-torsion submodule of $\text{Sel}(F_\infty, W)^\vee$ in terms of the $p$-adic $L$-function of $M$. Iwasawa theory can thus be motivated diagrammatically as follows:

\[
\begin{array}{ccc}
\text{Selmer group} & \xleftarrow{\text{main conjecture}} & (p\text{-adic } L\text{-function}) \\
\text{control} & \downarrow & \\
\text{theorems} & \leftarrow & (\text{usual } \text{Selmer group}) \\
\end{array}
\]

In other words, by proving statements in the context of Iwasawa theory, one can often deduce a relationship between the algebraic and analytic avatars of an arithmetic object.

Though we will use in Chapter 2 the basic language introduced above, this language can be reformulated to allow the methods of Iwasawa theory to be employed in more general situations. Let $T$ be the representation space of $\rho_M$, a finite free $\mathbf{Z}_p$-module of rank $n$. The study of the $\Lambda$-module structure of cohomology groups associated to $T$ over $F_\infty$ is equivalent, by Shapiro’s Lemma, to studying the $\Lambda$-module structure of cohomology groups associated to $T \otimes_{\mathbf{Z}_p} \Lambda$ over $F$. Note that $T \otimes_{\mathbf{Z}_p} \Lambda$ can be viewed as the representation space of a Galois representation $\rho_{M,\Lambda} : G_F \to \text{GL}_n(\Lambda)$.  

5
We can thus generalize the setup discussed above by allowing \( \Lambda \) to be an arbitrary complete local Noetherian ring and replacing \( T \otimes_{\mathbb{Z}_p} \Lambda \) with any finite free \( \Lambda \)-module equipped with a continuous action of \( G_F \). This point of view is useful when studying \( p \)-adic deformations of ordinary modular forms, as we do in Chapter 3. In this setting, the ring \( \Lambda \) is constructed from a \( p \)-adic Hecke algebra and has no purely Galois-theoretic interpretation. It may no longer be the case that finitely generated \( \Lambda \)-modules have a nice structure theory. This is not a serious impediment, however, as given a torsion \( \Lambda \)-module \( S \) (arising as a piece of a Selmer group associated to \( M \), say), we can instead compare the lengths of the \( \Lambda_p \)-modules \( S_p \) and \( \Lambda_p/L_p(M) \) for height 1 primes \( p \subseteq \Lambda \).

1.3. The method

We now describe a method developed by Agboola and Howard [1] for proving 1-variable main conjectures, i.e., main conjectures over rings \( \Lambda \) finite and flat over \( \mathbb{Z}_p[[T]] \). The two key inputs into this method are (1) an Euler system and (2) a 2-variable main conjecture. The existence of a non-trivial Euler system for the Galois representation under consideration allows one (via an appropriate general theory of Euler systems) to calculate the rank of the relevant Selmer group and show one divisibility in the main conjecture in the case that this rank is 0. In order to get the other divisibility, one must assume that the 1-variable Iwasawa algebra \( \Lambda \) arises naturally as the quotient of a 2-variable Iwasawa algebra (i.e., a finite flat \( \mathbb{Z}_p[[S,T]] \)-algebra) for which the associated 2-variable main conjecture is known. A descent argument then provides the remaining divisibility.

The rings \( \Lambda \) which we will be concerned with are those which are anticyclotomic for the Galois representations under consideration in a sense which we now indicate. We say that \( L(M,s) \) (or simply \( M \)) has a sign if its functional equation gives rise to an equality of the form \( L(M,k/2) = \varepsilon_M L(M,k/2) \cdot (*) \), where \( \varepsilon_M = \pm 1 \) is the sign of \( M \) and \((*)\) is a non-zero constant. This will be the case, e.g., if \( M = f \) is a cuspidal
newform with trivial character. Suppose there is a deformation $\rho_{M,\tilde{\Lambda}} : G_\mathbb{Q} \to \text{GL}_2(\tilde{\Lambda})$ of the Galois representation $\rho_M : G_\mathbb{Q} \to \text{GL}_2(\mathcal{O}_F)$ attached to $M$ for some 2-variable Iwasawa algebra $\tilde{\Lambda}$. Assume moreover that there is a 2-variable $p$-adic $L$-function $L_p(M) \in \tilde{\Lambda}$ interpolating the special values of $L(M_\chi, s)$ for arithmetic characters $\chi : \tilde{\Lambda} \to \mathbb{C}_p$, i.e., characters for which the representation $\rho_{M,\tilde{\Lambda}} \otimes \chi \mathbb{C}_p$ is associated to an arithmetic object $M_\chi$. We consider a 1-variable quotient $\Lambda = \tilde{\Lambda}/I$ of $\tilde{\Lambda}$ to be anticyclotomic if $I$ is contained in the kernel of those arithmetic characters $\chi : \Lambda \to \mathbb{C}_p$ for which $M_\chi$ has a sign and $\chi(L_p(M))$ is related via the interpolation property of $L_p(M)$ to the central value of $L(M_\chi, s)$. The main conjecture over $\Lambda$ then predicts that the Iwasawa-theoretic Selmer group $\text{Sel}_\Lambda(M)^\vee$ attached to $M$ over $\Lambda$ is a torsion $\Lambda$-module when the sign of $M$ is 1 and has generic rank 1 when the sign of $M$ is $-1$.

In Chapter 2, we apply the method described above to prove main conjectures for Selmer groups associated to modular forms $f$ which have CM by an imaginary quadratic field $K$. In this chapter, the two variables are provided by the cyclotomic and anticyclotomic $\mathbb{Z}_p$-extensions of the quadratic imaginary field $K$, where the variable of interest is the anticyclotomic one. Since the Galois representation associated to $f$ splits as the sum of two characters when restricted to $G_K$, the problem reduces to proving anticyclotomic main conjectures for Grössencharaktere of quadratic imaginary fields. The Euler system in this case comes from elliptic units attached to the quadratic imaginary field $K$ (cf. [3], e.g.). The associated 2-variable main conjecture in this case (suitably twisted) was proved by Rubin [14].

Chapter 3 sketches a method for applying the techniques outlined above to the Selmer groups of arbitrary modular eigenforms $f$. This chapter is to be considered work in progress, as the final results depend on several conjectures, the most serious of which being the non-vanishing of certain cohomology classes arising from the Euler system of Kato. The 2-variable Iwasawa algebra in this case is a piece of Hida’s nearly ordinary $p$-adic Hecke algebra. Roughly speaking, the 2 variables consist of a cyclotomic variable (coming from the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$) and a variable.
parametrizing the Hida family of which \( f \) is a member. The “Hida variable” is the variable of interest, as the sign of \( f \) persists in the Hida family. The Euler system we use was constructed by Kato [8], and work of Skinner-Urban (cf. [18]) gives the needed 2-variable main conjecture (under some additional assumptions).

1.4. Iwasawa theory of CM forms

Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) with complex multiplication by the ring of integers in a quadratic imaginary field \( K \). Agboola and Howard [1] have proved a main conjecture for the Selmer group of \( E \) over the anticyclotomic \( \mathbb{Z}_p \)-extension of \( K \) for primes \( p \) where \( E \) has good, ordinary reduction. The main conjecture computes the rank of the anticyclotomic Selmer group as a module over the Iwasawa algebra and describes the characteristic ideal of the torsion submodule of this Selmer group in terms of a \( p \)-adic \( L \)-function.

As the results of Agboola-Howard can be phrased entirely in terms of the Grössencharakter \( \psi = \psi_E \) of \( K \) associated to \( E \), it is natural to ask whether their methods can be generalized to “higher weight” Grössencharaktere, i.e., Grössencharaktere of type \( (w - 1, 0) \), \( w \geq 2 \) (all of which are associated to cuspidal newforms of weight \( w \)). The purpose of Chapter 2 is to give an affirmative answer to this question. In particular, we show that the anticyclotomic Selmer group associated to certain Tate twists of a Grössencharakter \( \psi \) of \( K \) of type \( (w - 1, 0) \) is usually a torsion Iwasawa module with characteristic ideal generated by the constant term of the associated (2-variable) \( p \)-adic \( L \)-function. The exceptions occur when the twist is chosen to be a specific value (depending on the weight) and the sign in the functional equation of \( \psi \) is equal to \(-1\); in this case, the rank of the Selmer group is 1, and the characteristic ideal of the torsion submodule is related to the linear term of the \( p \)-adic \( L \)-function via a \( p \)-adic regulator.

As a consequence of the above, we are able to prove a statement towards a generalization of the Birch and Swinnerton-Dyer conjecture. We show that the \( L \)-function
$L(f, s)$ of a modular form of even weight vanishes at its central point if and only if a Selmer group associated to $f$ over $\mathbb{Q}$ has positive rank. See Theorem 2.3.11 for a precise statement.

Much of the difficulty involved in generalizing the methods of Agboola-Howard lies in the fact that information arising from the geometry of CM elliptic curves is not available for Grössencharaktere associated to higher-weight CM forms. For example, the representations we consider are not in general self-dual, and there is no analogue of the fact that the $p$-torsion of a CM elliptic curve over $\mathbb{Q}$ is a non-trivial Galois module locally at $p$. In addition, we have had to take a slightly different approach to prove non-vanishing results about the $p$-adic $L$-functions with which we work.

1.5. Iwasawa theory for Hida families

Suppose $f$ is an arbitrary cuspidal, new Hecke eigenform for $\Gamma_0(N)$ of even weight $k > 2$ and let $p > 2$ be an ordinary prime for $f$. Our motivation is again a generalization of the conjecture of Birch and Swinnerton-Dyer: the order of vanishing of $L(f, s)$ at its central point should be equal to the rank of a Selmer group associated to $f$. The approach to proving such statements that we explore in Chapter 3 is to replace $f$ by Hida’s nearly ordinary $p$-adic family $\mathcal{F}^{no}$ associated to $f$. To $\mathcal{F}^{no}$ one can associate a local domain $\mathbf{H}^{no}$ finite and flat over $\mathbb{Z}_p[[S, T]]$ (playing the role of a 2-variable Iwasawa algebra), a Galois representation $\rho_{\mathcal{F}^{no}} : G_{\mathbb{Q}} \to \text{GL}_2(\mathbf{H}^{no})$, and a $p$-adic $L$-function $L_p(\mathcal{F}^{no}) \in \mathbf{H}^{no}$ interpolating the values of $L(f_{\kappa}, s)$ at integer arguments (up to some normalizing factor) for members $f_{\kappa}$ of the family $\mathcal{F}^{no}$.

In Chapter 2, we define an “anticyclotomic quotient” $\mathbf{H}^{no}_I = \mathbf{H}^{no}/I$, which is, roughly, the 1-variable quotient of $\mathbf{H}^{no}$ through which factor characters giving rise to a central $L$-value when applied to $L_p(\mathcal{F}^{no})$. Let $T_I$ be the representation space of $\rho_{\mathcal{F}^{no}}$ and set $W_I = T_I \otimes_{\mathbf{H}^{no}_I} (\mathbf{H}^{no}_I)^\vee$. The anticyclotomic main conjecture in this context is the following: $\text{Sel}(\mathbb{Q}, W_I)^\vee$ is a torsion $\mathbf{H}^{no}_I$-module if the sign of $f$ is 1 and has generic rank 1 if the sign of $f$ is $-1$; moreover, the divisorial support of $\text{Sel}(\mathbb{Q}, W_I)^\vee$
over $H_{p^{0}}$ coincides with that of $H_{p^{0}}/(L_{p}(\mathcal{F}^{\text{no}}))$. The goal of Chapter 3 is to describe how the method of Agboola-Howard might be used to prove this main conjecture (away from primes containing $p$) and explain how the main conjecture might be used to show a result about the Selmer group $\text{Sel}(\mathbb{Q}, f)$ of $f$ over $\mathbb{Q}$, namely that $L(f, s)$ vanishes at its central point if and only if $\text{Sel}(\mathbb{Q}, f)$ has positive rank.

In order to employ a method analogous to that of Agboola-Howard in the case of an arbitrary modular form $f$, which is naturally an object defined over $\mathbb{Q}$ and has no canonically associated quadratic imaginary field, it is necessary to find a suitable replacement for the anticyclotomic extension; this is provided by the ordinary Hida deformation associated to the modular form. The analogue of Rubin's 2-variable main conjecture is then (under some additional hypotheses, though certainly conjectured in general) work of Skinner-Urban on the main conjecture of Iwasawa theory for ordinary modular forms [18] (the 2 variables in this case being given by the Hida family and the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$). Again, a descent argument gives one divisibility of the main conjecture. The theory of Euler systems is then used to give the remaining divisibility. The Euler system we employ was constructed by Kato [8] and can be related to a $p$-adic $L$-function for $f$ by the work of Ochiai [11] on the Coleman map for Hida deformations.
CHAPTER 2

CM forms

This chapter is devoted to generalizing work of Agboola-Howard on CM elliptic curves to CM modular forms of higher weight. We prove a version of the main conjecture of Iwasawa theory over the anticyclotomic $\mathbb{Z}_p$-extension of a quadratic imaginary field $K$ for Selmer groups attached to modular forms with complex multiplication by $K$. This implies a statement to the effect that the $L$-function of a CM modular form $f$ of even weight vanishes at its central point if and only if a Selmer group attached to $f$ over $\mathbb{Q}$ is infinite.

For precise statements of the main theorems and outlines of their proofs, see 2.2.1 (Theorem 2.3.11 is the statement regarding Selmer groups over $\mathbb{Q}$ alluded to above). The reader familiar with Iwasawa theory is advised to proceed to §2.2 after reading 2.1.1, returning to §2.1 as needed to review notation.

2.1. Notation and definitions

Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. We view algebraic extensions of $\mathbb{Q}$ as being contained in $\overline{\mathbb{Q}}$. If $F$ is such an extension, we denote by $G_F$ the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/F)$ of $F$. Given a $G_F$-module $M$ and an algebraic extension $F'/F$, we denote by $M(F')$ the module of $G_{F'}$-invariants $M^{G_{F'}} = H^0(G_{F'}, M)$. In this chapter, $\text{Frob}_\ell$ will always denote an arithmetic Frobenius element associated to a rational prime $\ell$.

2.1.1. CM forms and representations. Let $f \in S_w(N, \chi)$ be a normalized newform of level $\Gamma_1(N)$, weight $w \geq 2$, and character $\chi$ and let $K_f$ be the number field generated by the Fourier coefficients of $f$. Then, by work of Deligne [4], there
is for each prime \( \mathfrak{p} \) of \( K_f \) (which we fix in the sequel) a representation \( \rho_f = \rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to \text{GL}_2(K_f,\mathfrak{p}) \) whose trace and determinant satisfy

\[
(2.1.1) \quad \text{trace } \rho_f(\text{Frob}_\ell) = a_\ell(f), \quad \det \rho_f(\text{Frob}_\ell) = \ell^{w-1} \chi(\ell),
\]

for any \( \ell \nmid Np \), where \( p \) is the rational prime below \( \mathfrak{p} \) and \( a_\ell(f) \) is the \( \ell \)th Fourier coefficient of \( f \). This representation is unramified outside of \( Np \).

Recall that \( f \) is said to be \( \mathfrak{p} \)-ordinary for a prime \( \mathfrak{p} \mid p \) of \( K_f \) if \( a_p(f) \) is a unit at \( \mathfrak{p} \). If \( f \) is \( \mathfrak{p} \)-ordinary, then Deligne showed that the restriction of \( \rho_f \) to the decomposition group \( D_p \) at \( p \) takes the form

\[
\rho_f|_{D_p} \cong \begin{pmatrix} \alpha & * \\ \beta & \end{pmatrix},
\]

with \( \beta \) unramified.

We say that \( f \) has complex multiplication, or is a CM form, if there is a quadratic imaginary field \( K \) and Grössencharakter \( \psi \) of \( K \) of type \((w - 1, 0)\) such that \( f \) is the cusp form associated to \( \psi \) (see, e.g., [13, p. 34]). In this case, the representation associated to \( f \) will satisfy \( \rho_f \cong \rho_f \otimes \chi_K \), where \( \chi_K \) is the Dirichlet character associated to \( K \). This implies that

\[
(2.1.2) \quad \rho_f|_{G_K} \cong \begin{pmatrix} \psi_p \\ \psi_p^{\tau} \end{pmatrix}
\]

for some character \( \psi_p \), where \( \psi_p^{\tau} = \psi_p \circ \tau \) is the conjugate character of \( \psi_p \) (\( \tau \) denotes the involution of \( G_K \) induced by complex conjugation).

For each split prime \( \mathfrak{q} \) of \( K \) lying over a rational prime \( q \), choose an embedding \( i_q : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_q \) in such a way that \( i_q \) and \( i_q^{-1} \) are conjugate. Given a Grössencharakter \( \phi \) of \( K \) and a split prime \( \mathfrak{q} \) of \( K \), one associates a \( p \)-adic Galois character \( \phi_q : G_K \to \mathbb{C}_p^\times \) by the rule \( \phi_q(\sigma_a) = i_q(\phi(a)) \), where \( \sigma_a \) is the Frobenius associated to a fractional ideal \( a \) of \( K \) prime to \( Np \). This notation is consistent with (2.1.2) in the sense that
the Galois character \( \psi_p \) of (2.1.2) is exactly the \( p \)-adic Galois character of \( K \) induced by the Grössencharakter \( \psi \) with respect to the prime \( p \) (provided that \( \mathfrak{P} \) is the prime of \( K_f \) induced by the embedding \( i_p \)). From this and the above formula (2.1.1) for the determinant of \( \rho_f \), we see that \( \psi_p \psi_p^\tau = \varepsilon^{w-1} \chi \), where \( \varepsilon \) is the \( p \)-adic cyclotomic character.

If \( f \) is \( \mathfrak{P} \)-ordinary for \( \mathfrak{P} \mid p \), then \( p \) splits in \( K \): \( \psi_p \) is ramified at \( p \), whereas \( \psi_p^\tau \) is unramified at \( p \), so \( p \neq p^\tau \). Set \( p^* = p^\tau \), so \( p\mathcal{O}_K = pp^* \). Denote by \( \mathcal{O} \) the integers of \( \Phi = K_f, \mathfrak{p} \). Given a character \( \xi : G_K \to \mathcal{O}^\times \), we denote by \( \mathcal{O}_\xi \) a free \( \mathcal{O} \)-module of rank 1 on which \( G_K \) acts via \( \xi \). The \( G_K \)-module we study in the sequel is \( T = \mathcal{O}_{\psi_p^\tau \chi^{-1}}(2 - w + c) \), where \( c \neq \frac{w-1}{2} \) is any integer (the assumption that \( c \neq \frac{w-1}{2} \) is needed to ensure that our representations do not split locally; see Lemma 2.2.5).

Actually, we are more interested in the Tate dual \( T^* = \mathcal{O}_{\psi_p}(-c) \) of \( T \), especially in the case \( c = \frac{1}{2}w - 1 \). For ease of notation, we set \( \eta = \psi_p^\tau \varepsilon^{2-w+c} \chi^{-1} \) and \( \eta^* = \psi_p \varepsilon^{-c} \).

Additionally, define \( V = T \otimes_{\mathcal{O}} \Phi \) and \( W = V/T = T \otimes_{\mathcal{O}} (\Phi/\mathcal{O}) \), and similarly for \( V^* \) and \( W^* \). Note that when \( \psi = \bar{\psi} \circ \tau \), we have \( \psi_p^\tau = \psi_p^* \) (so that \( \chi \) is trivial), \( \mathfrak{f} = \bar{f} \) where \( \mathfrak{f} \) denotes the conductor of \( \psi \), and the places ramified for \( T \) are the same as the places ramified for \( T^* \).

Remark. In order to make our notation consistent with [16], we have switched the roles of \( T \) and \( T^* \) compared to the corresponding notation in [1]. A similar remark will apply when we define the associated \( p \)-adic measures \( \mu \) and \( \mu^* \).

In what follows, we choose a prime \( \mathfrak{P} \nmid 6N \) at which \( f \) is ordinary and let \( p \) be the rational prime over which \( \mathfrak{P} \) lies. We moreover choose an isomorphism \( \mathbb{C}_p \cong \mathbb{C} \) which is compatible with the embedding \( i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \).
2.1.2. Selmer groups. Let $F$ be a finite extension of $K$. Following Greenberg [6], Rubin [16, §1.3], and others, we define local conditions for our representations as follows:

$$
H^1_v(F_v, V) = \begin{cases} 
H^1_{ur}(F_v, V) & \text{if } v \nmid p \\
0 & \text{if } v \mid p \\
H^1(F_v, V) & \text{if } v \mid p^* 
\end{cases}
$$

$$
H^1_v(F_v, V^*) = \begin{cases} 
H^1_{ur}(F_v, V^*) & \text{if } v \nmid p \\
H^1(F_v, V^*) & \text{if } v \mid p \\
0 & \text{if } v \mid p^* 
\end{cases}
$$

The exact sequence

$$
0 \rightarrow T \rightarrow V \rightarrow W \rightarrow 0
$$

gives the sequence of cohomology groups (exact in the middle)

$$
H^1(F_v, T) \rightarrow H^1(F_v, V) \rightarrow H^1(F_v, W).
$$

We define the local conditions $H^1_v(K_v, W)$, resp. $H^1_v(K_v, T)$, as the image, resp. preimage, of $H^1_v(K_v, V)$ under the maps in this sequence, and similarly for $W^*$ and $T^*$. Let $\Sigma = \Sigma_F$ be the set of primes of $F$ lying over $p$. Then for any $M$ for which the notation has been defined, we define Selmer groups

$$
\text{Sel}^\Sigma(F, M) = \ker \left( H^1(F, M) \rightarrow \bigoplus_{v \mid p} H^1(F_v, M)/H^1_v(F_v, M) \right)
$$

$$
\text{Sel}(F, M) = \ker \left( \text{Sel}^\Sigma(F, M) \rightarrow \bigoplus_{v \mid p} H^1(F_v, M)/H^1_v(F_v, M) \right)
$$

$$
\text{Sel}_\Sigma(F, M) = \ker \left( \text{Sel}(F, M) \rightarrow \bigoplus_{v \mid p} H^1(F_v, M) \right)
$$

2.1.3. Iwasawa modules. For any abelian extension $F/K$ (in practice $F$ will always be a finite extension of a $\mathbb{Z}_p$- or $\mathbb{Z}_p^2$-extension of $K$), define the Iwasawa algebra $\Lambda(F)$ to be the completed group ring $\mathcal{O}[[\text{Gal}(F/K)]] = \varprojlim \mathcal{O}[\text{Gal}(F'/K)]$, where the
limit is taken over fields $F' \subseteq F$ which are finite over $K$. This $\mathcal{O}$-algebra has an involution $\iota : \Lambda(F) \to \Lambda(F)$ which acts as $\iota(\gamma) = \gamma^{-1}$ on $\gamma \in \text{Gal}(F/K)$. Given any $\Lambda(F)$-module $M$, we can define 

$$M' = M \otimes_{\Lambda(F)} \Lambda(F),$$

where we view $\Lambda(F)$ as an algebra over itself via $\iota$.

If $M = T$ or $T^*$ and $F$ is as above, we define

$$\text{Sel}(F, M) = \lim \text{Sel}(F', M),$$

where the limit is taken with respect to corestriction maps between finite extensions $F'$ of $K$. Similarly, if $M = W$ or $W^*$, we define the $\Lambda(F)$-module

$$\text{Sel}(F, M) = \lim \text{Sel}(F', M),$$

the limit now being taken with respect to restriction maps. We define

$$X(F) = \text{Hom}_\mathcal{O}(\text{Sel}(F, W), \Phi/\mathcal{O})$$

$$X^*(F) = \text{Hom}_\mathcal{O}(\text{Sel}(F, W^*), \Phi/\mathcal{O}),$$

and make the analogous definitions for $X^\Sigma(F)$, $X_\Sigma(F)$, $X_*^\Sigma(F)$, and $X_*^\Sigma(F)$. We will also have occasion to use the semi-local cohomology groups

$$H^1(F_q, M) = \begin{cases} 
\lim \bigoplus_{v|q} H^1(F'_v, M) & \text{if } M \text{ is compact} \\
\lim \bigoplus_{v|q} H^1(F'_v, M) & \text{if } M \text{ is discrete}
\end{cases}$$

where $q$ is a prime of $K$. Tate local duality gives a perfect pairing

$$H^1(F_q, T) \times H^1(F_q, W^*) \longrightarrow \Phi/\mathcal{O}$$
satisfying \((\lambda x, y) = (x, \iota(\lambda)y)\) for any \(\lambda \in \Lambda(F)\). In order to make the Tate pairing \(\Lambda(F)\)-equivariant, we agree to view \(X(F)\) as a \(\Lambda(F)\)-module via \((\lambda f)(x) = f(\iota(\lambda)x)\) and similarly for \(X^*(F), X^{\Sigma}(F)\), etc.

Denote by \(C_{\infty}, D_{\infty},\) and \(K_{\infty}\) the cyclotomic \(\mathbb{Z}_p\)-extension, the anticyclotomic \(\mathbb{Z}_p\)-extension, and the unique \(\mathbb{Z}_p^2\)-extension of \(K\), respectively. Set \(\Gamma = \text{Gal}(D_{\infty}/K)\), so \(\Gamma \cong \mathbb{Z}_p\). Thus we have a field diagram:

\[
\begin{array}{c}
K_{\infty} \\
\downarrow \\
C_{\infty} \\
\downarrow \\
D_{\infty} \\
\downarrow \\
K \\
\downarrow \Gamma
\end{array}
\]

We will often work with the Iwasawa algebras \(\Lambda(K_{\infty})\) and \(\Lambda(D_{\infty})\), so it is convenient to define the ideal \(I \subseteq \Lambda(K_{\infty})\) to be the kernel of the (surjective) restriction map \(\Lambda(K_{\infty}) \rightarrow \Lambda(D_{\infty})\).

We need one further definition in order to define the \(p\)-adic \(L\)-functions we use. Let \(Q_{p}^{ur}\) be the maximal unramified extension of \(Q_p\), and let \(\bar{\mathcal{O}}\) be the integers in the completion \(\bar{\Phi}\) of \(Q_{p}^{ur} \cdot \Phi\). We define \(\bar{\Lambda}(F) = \bar{\mathcal{O}}[\text{Gal}(F/K)\} for any abelian extension \(F/K\).

### 2.1.4. \(p\)-adic \(L\)-functions

This and the following subsection are substantially similar to their counterparts in [1]. The \(p\)-adic \(L\)-function we work with is defined as a suitable “twist” of the (2-variable) \(p\)-adic \(L\)-function of Katz interpolating the \(L\)-functions of Grössencharaktere of \(K\).

For any nonzero integral ideal \(\mathfrak{f}\) of \(K\), denote by \(K(\mathfrak{f}^{p^\infty})\) the union of the ray class fields \(K(\mathfrak{f}^{p^n})\) of conductor \(\mathfrak{f}^{p^n}\). The Katz \(p\)-adic \(L\)-function is a measure

\[
\mu \in \bar{\Lambda}(K(\mathfrak{f}^{p^\infty}))
\]
which has the property that for any Grössencharakter $\phi$ of $K$ of type $(k,j)$ and conductor dividing $fp^\infty$ such that

\begin{equation}
(2.1.3) \quad k > 0 \quad \text{and} \quad j \leq 0,
\end{equation}

there is an interpolation formula

$$
\phi_p(\mu) = d(\phi) \left(1 - \frac{\phi(p)}{p}\right) L_{\infty,fp^\infty}(\phi^{-1}, 0),
$$

where $\phi_p$ is the $p$-adic character associated to $\phi$ and $d(\phi)$ is an explicit nonzero constant. (Note that to make sense of this equation, we need to make use of our chosen isomorphism $\mathbb{C}_p \cong \mathbb{C}$.) For more information about these $L$-functions, see the book of de Shalit [3, Ch. II], especially II.4.14. Note that II.6.7 of [3] extends the interpolation range to that given in (2.1.3).

For any fractional ideal $f$ of $K$ and any character $\xi$ of $\text{Gal}(K(fp^\infty)/K)$ with values in $\mathcal{O}^\times$, define the $\mathcal{O}$-algebra automorphism of $\tilde{\Lambda}(K(fp^\infty))$

$$
\text{Tw}_\xi : \tilde{\Lambda}(K(fp^\infty)) \longrightarrow \tilde{\Lambda}(K(fp^\infty))
$$

by the rule $\text{Tw}_\xi(\gamma) = \xi(\gamma)\gamma$ for all $\gamma \in \text{Gal}(K(fp^\infty)/K)$. If $L \subseteq K(fp^\infty)$ is any extension of $K$, we denote by $\mu(L, \xi)$ the image of $\text{Tw}_\xi(\mu)$ under the projection $\tilde{\Lambda}(K(fp^\infty)) \twoheadrightarrow \tilde{\Lambda}(L)$. Additionally, we define, for every integral ideal $a \subseteq \mathcal{O}_K$ prime to $fp$, the element $\lambda(L, \xi, a)$ to be the image of $\text{Tw}_\xi(\sigma_a - Na)$ in $\Lambda(L)$ ($\sigma_a$ is the Frobenius associated to $a$). Then set $\mu(L, \xi, a) = \mu(L, \xi)\lambda(L, \xi, a)$.

If we assume in addition that the ideal $f$ satisfies $f \equiv f$, then complex conjugation defines an involution $\tau$ of $\tilde{\Lambda}(K(fp^\infty))$. We set $\mu^* = \tau(\mu)$ and define in the same way as above the measures $\mu^*(L, \xi)$ and $\mu^*(L, \xi, a) = \mu^*(L, \xi)\lambda(F, \xi, a)$. As noted above, the roles of $\mu$ and $\mu^*$ are switched from the corresponding notation in [1].

These twisted $L$-functions of course also satisfy interpolation properties. Suppose that $\xi = \theta_p$ is the $p$-adic character associated to a Grössencharakter $\theta$. Then for any
Grössencharakter $\phi$ such that $\phi_p$, resp. $\phi_{p^*}$, factors through $L$, we have

$$\phi_p(\mu(L, \xi, a)) = (\phi \theta(a) - Na)(\phi \theta)_p(\mu),$$

resp.

$$\phi_{p^*}(\mu^*(L, \xi, a)) = (\phi \overline{\theta}(a) - Na)(\phi \overline{\theta})_{p^*}(\mu^*).$$

If we take $\xi$ to be the $p$-adic character $\eta^*$ associated to the Grössencharakter $\psi N^{-c}$, then provided that $\phi \psi N^{-c}$, resp. $\overline{\psi} N^{-c}$, has type $(k, j)$ satisfying (2.1.3), we get

(2.1.4)

$$\phi_p(\mu(L, \eta^*, a)) = d(\phi \psi N^{-c})(\phi \psi N^{-c}(a) - Na) \left(1 - \frac{\phi \psi(p)}{p^{1+c}}\right) L_{\infty, fp^*}(\phi^{-1} \psi^{-1}, -c),$$

resp.

(2.1.5)

$$\phi_{p^*}(\mu^*(L, \eta^*, a)) = d(\phi \overline{\psi} N^{-c})(\phi \overline{\psi} N^{-c}(a) - Na) \left(1 - \frac{\phi \overline{\psi}(p^*)}{p^{1+c}}\right) L_{\infty, fp}(\phi^{-1} \overline{\psi}^{-1}, -c).$$

In case $L = K_{\infty}$, if we choose a topological generator $\gamma$ of $\text{Gal}(K_{\infty}/D_{\infty})$, we get power series expansions

$$\mu(K_{\infty}, \eta^*, a) = L_{a, 0} + L_{a, 1}(\gamma - 1) + L_{a, 2}(\gamma - 1)^2 + \cdots,$$

$$\mu(K_{\infty}, \eta^*) = L_0 + L_1(\gamma - 1) + L_2(\gamma - 1)^2 + \cdots,$$

where $L_{a, i}$ and $L_i$ are elements of $\tilde{\Lambda}(D_{\infty})$.

2.1.5. Euler systems. The Katz $p$-adic $L$-function is related by a theorem of Yager to the so-called Euler system of elliptic units. It is therefore not surprising that the twisted $L$-functions constructed in 2.1.4 are related to a twisted version of the elliptic unit Euler system. It is not instructive to give the construction of this Euler system, so we content ourselves by simply stating its properties.

Let $a \subseteq \mathcal{O}_K$ be an ideal prime to $fp$. The elliptic unit Euler system (with respect to $a$) consists of, for each ideal $i \subseteq \mathcal{O}_K$ prime to $a$, a certain unit $\Theta(i, a)$ in the ray

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
class field $K(i)$ of $K$ of conductor $i$. These units satisfy the following relations:

\[(2.1.6) \quad \text{Nm}_{K(i^j)/K(i)} \Theta(i^j, a)^{e} = \begin{cases} 
\Theta(i, a) & \text{if } j \mid i \\
\Theta(i, a)^{1-\sigma_j} & \text{if } j \nmid i
\end{cases}\]

where $\sigma_j$ is the Frobenius of $j$ and $e = w_i/w_{ij}$ ($w_?$ being the number of roots of unity of $K$ congruent to 1 mod $?$).

If $q = p$ or $p^*$ and $F$ is a finite abelian extension of $K$, we define

\[U_q(F) = \bigoplus_{v \mid q} O^{(1)}_{F_v},\]

where $O^{(1)}_{F_v}$ is the group of units of $F_v$ congruent to 1 mod $v$. If $F$ is an infinite abelian extension of $K$, we define

\[U_q(F) = \lim U_q(F'),\]

where the limit is taken with respect to norm maps between finite extensions $F'$ of $K$ contained in $F$. Since the relations (2.1.6) show that the $\Theta(fp^n, a)$ are norm-compatible for $n > 0$, we may define $\theta(a)$, resp. $\theta^*(a)$, to be the image of this sequence in $U_p(K(fp^\infty))$, resp. $U_{p^*}(K(fp^\infty))$. The following theorem of Yager relates this Euler system to the Katz $p$-adic $L$-function:

**Theorem 2.1.1.** There is an injection of $\tilde{\Lambda}(K(fp^\infty))$-modules

\[U_q(K(fp^\infty)) \otimes_{\mathbb{Z}_p} \tilde{\mathcal{O}} \rightarrow \tilde{\Lambda}(K(fp^\infty))\]

with image the ideal $J \subseteq \tilde{\Lambda}(K(fp^\infty))$ generated by \{$(\sigma_b - Nb | (b, fp) = 1)$\}. The image of $\theta(a)$, resp. $\theta^*(a)$, under this map is $(\sigma_a - Na)\mu$, resp. $(\sigma_a - Na)\mu^*$.

**Proof.** This theorem is proved in [3, Proposition III.1.4]. (As remarked there, our assumption that $p \neq 2, 3$ allows us to avoid taking 12th roots.)
By Kummer theory, we may view the unit $\theta(i, a) = \text{Nm}_{K(i)^p/K(i)} \Theta(i^p, a)$ as being an element of $H^1(K(i), \mathbb{Z}_p(1))$. If we define $K_a = \bigcup_{(i,a)=1} K(i)$, then the relations (2.1.6) show that the $\theta(i, a)$ form an Euler system for $(\mathbb{Z}_p(1), fp, K_a)$ in the sense of Rubin’s book [16, §2.1]. The following proposition (essentially Proposition 2.3.1 of [1]) shows that we can twist this Euler system into an Euler system for $T$ which is related to the twisted $p$-adic $L$-function defined in 2.1.4.

**Proposition 2.1.2.** There is an Euler system $c_a$ for $(T, fp, K_a)$ and injective “Coleman” maps

$$\text{Col} : H^1(K(fp^\infty)_p, T) \otimes_{\mathcal{O}} \mathcal{O} \to \tilde{\Lambda}(K(fp^\infty))$$

$$\text{Col}^* : H^1(K(fp^\infty)_p^*, T) \otimes_{\mathcal{O}} \mathcal{O} \to \tilde{\Lambda}(K(fp^\infty))$$

such that if we define $z$, resp. $z^*$, to be the local image of

$$c_a(K(fp^\infty)) = \lim_k c_a(K(fp^k)) \in \lim_k H^1(K(fp^k), T)$$

in $H^1(K(fp^\infty)_p, T)$, resp. $H^1(K(fp^\infty)_p^*, T)$, then $\text{Col}(z \otimes 1) = \mu(K(fp^\infty), \eta^*, a)$ and $\text{Col}^*(z^* \otimes 1) = \mu^*(K(fp^\infty), \eta^*, a)$. The image of these maps is the ideal $Tw_{\eta^*}(J)$ generated by \{\(\sigma_b - \eta(\sigma_b)\mid (b, fp) = 1\).

**Proof.** Recall that $\eta = \psi_p^{-2-w+c}\chi^{-1} = \varepsilon(\eta^*)^{-1}$, so there is a commutative diagram of $\mathcal{O}$-modules

$$\begin{array}{ccc}
\varprojlim_{\text{loc}_p} H^1(K(fp^\infty), \mathcal{O}(1)) & \xrightarrow{\beta} & \varprojlim_{\text{loc}_p} H^1(K(fp^\infty), T) \\
\downarrow & & \downarrow \\
U_p(K(fp^\infty)) \cong H^1(K(fp^\infty)_p, \mathcal{O}(1)) & \xrightarrow{\beta_p} & H^1(K(fp^\infty)_p, T)
\end{array}$$

where $\beta$ and $\beta_p$ are $\mathcal{O}$-isomorphisms satisfying $\beta \circ Tw_{\eta^*}^{-1}(\lambda) = \lambda \circ \beta$ for $\lambda \in \Lambda(K(fp^\infty))$ and similarly for $\beta_p$.

20
We define the Euler system $c_{a}$ to be the twist of $\theta(i,a)$ in the sense of [16, Theorem 6.3.5], so that $z = \beta_{p}(\theta(a))$. The map $\text{Col}$ is just the composite

$$
H^{1}(K(p^{\infty})_{p}, T) \xrightarrow{\beta_{p}^{-1}} U_{p}(K(p^{\infty})) \longrightarrow J \xrightarrow{T_{w_{a}}^{-1}} T_{w_{a}}(J),
$$

where the second arrow is the isomorphism of Theorem 2.1.1. The construction of $\text{Col}^{*}$ is analogous. □

We will need to view this Euler system as an Euler system for $(D_{\infty}, T)$, but this is potentially problematic: Rubin’s definition of Euler system requires that all primes of $K$ be finitely decomposed in $D_{\infty}$, which is not the case. In order to apply main results of [16], we make use of [16, §9.2], which states that it is enough to show that for every prime $q$ of $K$ splitting completely in $D_{\infty}/K$ and every field $F \subseteq K_{a}$ finite over $K$, the class $c_{a}(F)$ is locally unramified at every place above $q$. Thus the following lemma certainly suffices.

**Lemma 2.1.3.** For every field $F \subseteq K_{a}$ finite over $K$, the class $c_{a}(F)$ is locally unramified at every place of $F$ not lying over $p$.

**Proof.** Use Corollary B.3.5 of [16] and the fact that $c_{a}(F)$ is a universal norm in the cyclotomic direction. □

### 2.2. Divisibility from Euler systems

#### 2.2.1. Statement of results.
Recall that we have chosen an integer $c \neq \frac{w-1}{2}$ and have set $T^{*} = \mathcal{O}_{\psi_{c}}(-c)$, $W^{*} = T^{*} \otimes (\Phi/\mathcal{O})$, and $\eta^{*} = \psi_{p}e^{-c}$. We are mostly interested in the structure of $X^{*}(D_{\infty}) = \text{Hom}_{\mathcal{O}}(\text{Sel}(D_{\infty}, W^{*}), \Phi/\mathcal{O})$ when $c = \frac{1}{2}w - 1$ and $\overline{\psi} \circ \tau = \psi$, i.e., the “sign” in the functional equation of $\psi$ (and hence of the modular form $f$ associated to $\psi$) makes sense.

**Theorem 2.2.1.** Assume that if $\overline{\psi} \circ \tau = \psi$ and $c = \frac{1}{2}w - 1$, then the sign in the functional equation of $\psi$ is $+1$. Then $\text{Sel}(D_{\infty}, T) = 0$ and $X^{*}(D_{\infty})$ is a torsion...
\( \Lambda(D_\infty) \)-module. Moreover there is an equality of ideals in \( \tilde{\Lambda}(D_\infty) \otimes_{\tilde{\phi}} \tilde{\Phi} \)

\[
(\text{char } X^*(D_\infty)) = (\mu(D_\infty, \eta^*)).
\]

In this section, we will prove the first two claims and that the characteristic ideal of \( X^*(D_\infty) \) divides the \( p \)-adic \( L \)-function using some Galois cohomology and the theory of Euler systems as exposed in Rubin’s book [16]. The key point is to prove that the Euler system employed, a twisted version of the elliptic unit Euler system, is nontrivial. This will be achieved by using a theorem of Greenberg on the non-vanishing of \( L \)-functions of Grössencharaktere of \( K \). The next section, §2.3, will be devoted to the proof of the remaining divisibility. We use the two variable main conjecture together with a descent argument to achieve this.

The next result shows what happens in the exceptional case:

**Theorem 2.2.2.** Assume that \( \overline{\psi} \circ \tau = \psi \), \( c = \frac{1}{2} w - 1 \), and the sign in the functional equation of \( \psi \) is \(-1\). Then \( X^*(D_\infty) \) is a \( \Lambda(D_\infty) \)-module of rank 1. Moreover, there is an equality of ideals in \( \tilde{\Lambda}(D_\infty) \otimes_{\tilde{\phi}} \tilde{\Phi} \)

\[
(\text{char } X^*(D_\infty)_{\text{tors}}) \cdot R = (L_1).
\]

Here \( R \) denotes a certain \( p \)-adic regulator, defined in §2.4. The rank statement of Theorem 2.2.2 will be proved simultaneously with Theorem 2.2.1. In §2.4, we use the theory of \( p \)-adic heights to prove the statement about the characteristic ideal.

**2.2.2. Non-triviality of \( p \)-adic \( L \)-functions.** In order for the general theorems of Rubin [16] on Euler systems to provide non-trivial information, we need to prove the non-vanishing over \( D_\infty \) of the Euler system \( c_\alpha \) constructed in Proposition 2.1.2. What we first prove is the non-vanishing over \( D_\infty \) of the associated \( p \)-adic \( L \)-function.
We would then like to be able, roughly speaking, to fill in a diagram like

\[
\begin{array}{ccc}
H^1(K(f^p \infty)_{f_p}, T) & \xrightarrow{\text{Col}} & \tilde{\Lambda}(K(f^p \infty)) \\
\downarrow \text{cor} & & \downarrow \\
H^1(D_{\infty,f_p}, T) & \xrightarrow{} & \tilde{\Lambda}(D_{\infty})
\end{array}
\]

(2.2.1)

in order to conclude the non-vanishing of the restriction of the Euler system to \(D_{\infty}\) on the left from the non-vanishing of an appropriate \(p\)-adic \(L\)-function on the right. Such a map will exist after extending scalars to \(\tilde{\Phi}\). Our immediate goal, therefore, is to show:

**Proposition 2.2.3.** If \(\psi \circ \tau = \psi\) and \(c = \frac{1}{2}w - 1\), then \(\mu(D_{\infty}, \eta^*)\) is nonzero if and only if the sign in the functional equation of \(\psi\) is +1 and \(\mu^*(D_{\infty}, \eta^*)\) is nonzero if and only if the sign in the functional equation of \(\psi\) is −1. Otherwise, i.e., if \(c \neq \frac{1}{2}w - 1\) or \(\psi \circ \tau \neq \psi\), both measures are nonzero.

**Proof.** Let \(\phi_0 = \psi/\psi\). This is a Grössencharakter of type \((w - 1, 1 - w)\) and, as such, its corresponding \(p\)-adic character \(\phi_{0,p}\) factors through a finite extension of \(D_{\infty}\). Choose a positive integer \(m\) (which we may enlarge later on) such that \(\phi_0^m\) has trivial conductor and \((\phi_0^m)_p\) factors through \(D_{\infty}\). Set \(\phi = \phi_0^m\). We will apply the interpolation formulas \((2.1.4)\) and \((2.1.5)\) to the characters \(\phi^\ell\) (which have appropriate type for \(\ell \gg 0\)).

Since \(\phi^\ell \psi N^{-c}\), resp. \(\phi^\ell \psi N^{-c}\), has type \(((\ell m + 1)(w - 1) - c, \ell m(1 - w) - c)\), resp. \((\ell m(w - 1) - c, (\ell m - 1)(1 - w) - c)\), we can apply equation \((2.1.4)\), resp. \((2.1.5)\), to get the formula

\[
\phi^\ell_p(\mu(D_{\infty}, \eta^*)) = (\ast) L_{\infty,f_p}^*(\phi^{-1}\psi^{-1}, -c)
\]

(2.2.2)

\[
= (\ast) L_{\infty,f_p}^*(\psi^{2\ell m + 1}, c + 1 + \ell m(w - 1))
\]
\[
\phi_{\ell^*}(\mu^*(D_{\infty}, \eta^*)) = (*) L_{\infty, fp}(\phi^{-1} \psi^{-1}, -c) \\
(*) L_{\infty, fp}(\psi^{2\ell_m - 1}, c + 1 + (\ell m - 1)(w - 1)),
\]

where for the second equalities in each formula we have used the functional equation and the fact that \(N^{w-1}\) (here \((*)\) represents a nonzero constant consisting of gamma factors and Euler factors at \(p\)). In both cases, as \(\psi\) has type \((w - 1, 0)\), the given \(L\)-values are central if and only if \(c = \frac{1}{2} w - 1\).

Equations (2.2.2) and (2.2.3) hold for all \(\ell \gg 0\) (and in particular for infinitely many characters). The proposition will then follow from work of Greenberg [5, Theorem 1] on the (non)vanishing of classical \(L\)-values of Grössencharaktere of type \((n, 0)\) if we can show that the sign in the functional equation of \(\psi^{2\ell_m + 1}\), resp. \(\psi^{2\ell_m - 1}\), is the same as, resp. the negative of, the sign in the functional equation of \(\psi\) whenever the sign makes sense. To show this, we use the following formula of Weil [19, p. 161] as stated in [1, Proposition 2.1.6]:

**Proposition 2.2.4.** For two \(C^\infty\)-valued idèle class characters \(\theta_1, \theta_2\) of types \((k_1, j_1)\) and \((k_2, j_2)\), with relatively prime conductors \(f_1\) and \(f_2\), and of absolute value 1, we have

\[
W(\theta_1)W(\theta_2)\theta_1(f_2)\theta_2(f_1) = \begin{cases} 
W(\theta_1\theta_2) & \text{if } (k_1 - j_1)(k_2 - j_2) \geq 0 \\
(-1)^\nu W(\theta_1\theta_2) & \text{if } (k_1 - j_1)(k_2 - j_2) < 0,
\end{cases}
\]

where \(W(\theta_i)\) is the root number of \(\theta_i\) and \(\nu = \min\{|k_1 - j_1|, |k_2 - j_2|\} \). \(\square\)

We proceed as in [5, p. 83], making use of the fact that \(W(\theta) = W(\theta/|\theta|)\) for any Grössencharakter \(\theta\). By the proposition, since \(\psi^m\) has trivial conductor, we have that \(W(\psi^{mr}) = W(\psi^m)^r\) for all \(r \geq 0\). Moreover, the fact that \(\psi^m\) is unramified everywhere shows that \(W(\psi^m)\) is a root of unity. Thus by enlarging \(m\) we may assume that \(W(\psi^m) = 1\).
To deal with the $\psi^{2\ell m+1}$ case, we take $\theta_1 = \psi^{2\ell m}/|\psi^{2\ell m}|$ (which has trivial conductor) and $\theta_2 = \psi/|\psi|$. In this case $(k_1 - j_1)(k_2 - j_2) \geq 0$. By choice of $m$, we have $f_1 = 1$, so $\theta_2(f_1) = 1$, and Weil's formula gives that

$$W(\psi^{2\ell m+1}) = W(\psi)\alpha^\ell,$$

where $\alpha = \psi^{2m}(f_2)/|\psi^{2m}(f_2)|$. In the case we are concerned about (i.e., when $\overline{\psi} \circ \tau = \psi$), we have that $f_2 = \overline{f}_2$, which implies that $\alpha = \pm 1$. Replacing $m$ with $2m$, we may assume that $\alpha = 1$, which is what we want.

Finally, in the $\psi^{2\ell m-1}$ case, we take $\theta_1$ as before and $\theta_2 = \psi^{-1}/|\psi^{-1}|$. Then $(k_1 - j_1)(k_2 - j_2) < 0$. Proceeding as above, we apply Weil's formula to get

$$W(\psi^{2\ell m-1}) = -W(\psi^{-1}) = -W(\overline{\psi}) = -W(\psi).$$

2.2.3. Cohomological preparations. The following lemma is used throughout the sequel, and explains our assumption that $c \neq \frac{w-1}{2}$, which ensures that the hypotheses of the lemma are satisfied for the characters $\eta$ and $\eta^*$ defined in 2.1.1.

**Lemma 2.2.5.** Suppose $\chi = \theta_p$ is the $p$-adic character associated to a Grössencharakter $\theta$ of $K$ of type $(a, b)$ with $a \neq -b$. Then $\chi|_{G_{D_\infty}} \neq 1$ and for any prime $q$ of $K$, $\chi|_{G_{K_q}} \neq 1$. If $q | p$, then moreover $\chi|_{D_{\infty, v}} \neq 1$ for any place $v$ of $D_{\infty}$ lying over $q$.

**Proof.** If $\chi|_{G_{D_{\infty}}} = 1$, then $\chi \circ \tau = \chi^{-1}$, which implies that $a = -b$. Suppose first that $q | p$ and choose an abelian extension $L$ of $K$ which is finite over $K_{\infty}$ and over which $\chi$ splits. It follows from [3, Proposition II.1.9], e.g., that $q$ is finitely decomposed in $L$, so $\text{Gal}(L_v/K_q)$ is a finite-index subgroup of $\text{Gal}(L/K)$ (for any place $v$ of $L$ over $q$). Thus if $\chi$ were to split over $D_{\infty, v}$, some power of $\chi$ would split over $D_{\infty}$, so again $a = -b$. 

25
If \( q \nmid p \), then by raising \( \chi \) to a suitable power, we may assume that \( \chi \) is unramified at \( q \). Let \( \pi \in \mathcal{O}_K \) be a generator of some power \( q^d \) of \( q \). Then, as \( a \neq -b \),

\[
\chi(\text{Frob}_q^d) = \theta(\pi)^d = (\pi^{a-b})^d \neq 1,
\]
so \( \chi|_{G_{K\pi}} \neq 1 \). \( \square \)

As mentioned above, we cannot fill in diagram (2.2.1); however, after tensoring with \( \widetilde{\Phi} \), we can prove

**Proposition 2.2.6.** For \( q = p \) or \( p^* \), there is an isomorphism of \( \widetilde{\Lambda}(D_\infty) \otimes \widetilde{\Phi} \)-modules

\[
H^1(D_{\infty, q}, T) \otimes \widetilde{\Phi} \longrightarrow \widetilde{\Lambda}(D_{\infty}) \otimes \widetilde{\Phi}
\]

which maps \( \text{loc}_q c_\alpha(D_\infty) \) to \( \mu(D_\infty, \eta^*, a) \) if \( q = p \) or to \( \mu^*(D_\infty, \eta^*, a) \) if \( q = p^* \).

**Proof.** We use the \( \widetilde{\Lambda}(D_\infty) \)-module map induced by the Coleman map of Proposition 2.1.2

\[
H^1(K(fp^\infty)_q, T) \otimes \widetilde{\Lambda}(D_\infty) \longrightarrow \widetilde{\Lambda}(D_\infty),
\]

where the tensor product is taken over the ring \( \widetilde{\Lambda}(K(fp^\infty)) \). Thus we would like a map filling in the diagram

\[
\begin{array}{ccc}
H^1(K(fp^\infty)_q, T) & \otimes \widetilde{\Lambda}(D_\infty) & \longrightarrow \widetilde{\Lambda}(D_\infty) \\
& \downarrow & \\
H^1(D_{\infty, q}, T) & \otimes \widetilde{O} &
\end{array}
\]

which we construct by proving that the left hand map (the natural corestriction map) is an isomorphism, at least after tensoring with \( \widetilde{\Phi} \).

We break up the extension \( K(fp^\infty)/D_\infty \) into two pieces and deal with each separately. First consider the finite extension \( K(fp^\infty)/K_\infty \). The inflation-restriction
sequence shows that the restriction map

\[
\text{res} : \prod_{v \mid q} H^1(K_{\infty, v}, W^*) \longrightarrow \prod_{v \mid q} H^1(K(\mathbb{f}p^\infty)_v, W^*)
\]

has finite kernel and cokernel since there are only finitely many primes of \(K(\mathbb{f}p^\infty)\) over \(p\), and is an isomorphism if \(p \nmid [K(\mathbb{f}) : K]\). (Note \(p \nmid [K(\mathbb{f}) : K]\) if and only if \(p \mid [K(\mathbb{f}p^\infty) : K_{\infty}]\).) Thus, by local duality, the map

\[
H^1(K(\mathbb{f}p^\infty)_q, T) \otimes_{\Lambda(K(\mathbb{f}p^\infty))} \Lambda(K_{\infty}) \longrightarrow H^1(K_{\infty, q}, T)
\]

has the same property.

Now we consider the \(\mathbb{Z}_p\)-extension \(K_{\infty}/D_{\infty}\). We claim that the corestriction map

(2.2.4) \[
H^1(K_{\infty, q}, T) \otimes_{\Lambda(K_{\infty})} \Lambda(D_{\infty}) \longrightarrow H^1(D_{\infty, v}, T)
\]

is injective with finite cokernel. If \(v\) is any of the finitely many places of \(K_{\infty}\) above \(q\), we have the local inflation-restriction sequence

\[
0 \longrightarrow H^1(K_{\infty, v}/D_{\infty, v}, W^*(K_{\infty, v})) \longrightarrow H^1(D_{\infty, v}, W^*) \longrightarrow \]

\[
\longrightarrow H^1(K_{\infty, v}, W^*)\text{Gal}(K_{\infty, v}/D_{\infty, v}) \longrightarrow 0,
\]

where the final map is surjective because \(\text{Gal}(K_{\infty, v}/D_{\infty, v}) \cong \mathbb{Z}_p\) has cohomological dimension 1. Set \(M = W^*(K_{\infty, v})\), which is either finite or equal to \(W^*\). By Lemma B.2.8 of [16],

\[
H^1(K_{\infty, v}/D_{\infty, v}, M) \cong M/(\gamma - 1)M,
\]

where \(\gamma\) is a topological generator of \(\text{Gal}(K_{\infty, v}/D_{\infty, v})\). \(M/(\gamma - 1)M\) is finite in the case \(M\) is finite and trivial in the case \(M = W^*\), since \(\gamma\) does not act trivially on \(W^*\) by Lemma 2.2.5. Our claim thus follows from local duality.
Hence, if we apply $\widetilde{\Phi}$ to the map

$$H^1(K(fp^{\infty})_q, T) \otimes_{\Lambda(K(fp^{\infty}))} \Lambda(D_\infty) \longrightarrow H^1(D_\infty, q, T),$$

it becomes an isomorphism. Taking the inverse and composing with the appropriate Coleman map (i.e., Col or Col*) of Proposition 2.1.2 yields the desired map, a priori an injection (since the Coleman maps are). Proposition 2.1.2 also describes the image of the Coleman map as $Tw_{\eta}(J)$. Since $K(\eta)D_\infty \supseteq K_\infty$ by Lemma 2.2.5, we can certainly find $\gamma_1, \gamma_2 \in \text{Gal}(K(fp^{\infty})/K)$ such that $\eta(\gamma_1) \neq \eta(\gamma_2)$ but $\gamma_1|_{D_\infty} = \gamma_2|_{D_\infty}$. This shows that the map is also surjective.

2.2.4. Non-triviality of Euler systems. We can use Proposition 2.2.6 to show the nontriviality of the Euler systems we constructed in Proposition 2.1.2. After establishing the relevant notation, we first prove Lemma 2.2.8, which will be used often in the sequel. Fix an integral ideal $a$ of $K$ prime to $fp$ and for any extension $F \subseteq K_\infty$ of $K$, set

$$c_a(F) = \lim_{\overleftarrow{\nu}} c_a(F^\nu) \in H^1(F, T),$$

the inverse limit being taken over finite extensions $F^\nu \subseteq F$ of $K$.

**Proposition 2.2.7.** For any $F \subseteq K_a$, we have

$$c_a(F) \in \text{Sel}^\Sigma(F, T).$$

**Proof.** This follows from Lemma 2.1.3 and [16, Lemma 2.3.5(ii)].

Hence the $\Lambda(F)$-submodule $C_a(F)$ of $H^1(F, T)$ generated by $c_a(F)$ is contained in $\text{Sel}^\Sigma(F, T)$. Define $C(F) \subseteq \text{Sel}^\Sigma(F, T)$ to be the $\Lambda(F)$-submodule generated by \{c_a(F) \mid (a, fp) = 1\} and set

$$Z_a(F) = \text{Sel}^\Sigma(F, T)/C_a(F)$$

$$Z(F) = \text{Sel}^\Sigma(F, T)/C(F).$$
Lemma 2.2.8. For \( q = p \) or \( p^* \), \( H^1(D_{\infty,q}, T) \) is torsion-free of rank 1 over \( \Lambda(D_{\infty}) \).

PROOF. The proofs of Propositions 2.1.3 and 2.1.6 in Perrin-Riou’s article [12] work without modification if the representation under consideration has coefficients in \( \Phi \) rather than \( \mathbb{Q}_p \). Thus the former implies that \( H^1(D_{\infty,q}, T) \) is of rank 1, and the latter implies that, for any place \( v \) of \( D_{\infty} \) over \( q \), the torsion submodule of \( H^1(D_{\infty,v}, T) \) is naturally isomorphic to \( T(D_{\infty,v}) \), which is trivial by Lemma 2.2.5. \( \square \)

Proposition 2.2.9. If \( \overline{\psi} \circ \tau = \psi \) and \( c = \frac{1}{2}w - 1 \), then for \( q = p \), resp. \( p^* \), the localization \( \text{loc}_q C(D_{\infty}) \subseteq H^1(D_{\infty,q}, T) \) is nonzero if and only if the sign in the functional equation of \( \psi \) is \( +1 \), resp. \( -1 \). Otherwise, \( \text{loc}_q C(D_{\infty}) \) is always nonzero.

PROOF. If \( c = \frac{1}{2}w - 1 \) and the sign is \( +1 \), Proposition 2.2.3 shows that \( \mu(D_{\infty}, \eta^*) \neq 0 \). Choosing \( a \) so that \( \mu(D_{\infty}, \eta^*, a) \neq 0 \) and applying Proposition 2.2.6, we see that \( \text{loc}_p c_a(D_{\infty}) \neq 0 \). Thus \( \text{loc}_p C(D_{\infty}) \neq 0 \). To see that in this case \( \text{loc}_p^* C(D_{\infty}) = 0 \), note that Proposition 2.2.3 implies that for any \( a \), the measure \( \mu^*(D_{\infty}, \eta^*, a) \) vanishes. Thus Proposition 2.2.3, together with Lemma 2.2.8, shows that \( \text{loc}_p^* C_a(D_{\infty}) = 0 \) for all \( a \). A similar argument applies when the sign is \( -1 \) or when \( c \neq \frac{1}{2}w - 1 \). \( \square \)

2.2.5. Towards the main conjecture. After proving several preliminary results relating the various Selmer groups we have defined, we will be in a position to apply the main results of [16] over the anticyclotomic extension \( D_{\infty}/K \) to show that the characteristic ideal of \( X^*(D_{\infty}) \) is contained in the characteristic ideal of \( Z(D_{\infty}) \).

Proposition 2.2.10. Let \( F \) be a finite extension of \( K \), \( v \) a prime of \( F \) not dividing \( p \), and \( V \) a \( \Phi[G_{F_v}] \)-module, finite as vector space over \( \Phi \). If \( V \) and \( V^* \) (Tate dual) both have no \( G_{F_v} \)-invariants, then \( H^1(F_v, V) = 0 \).

PROOF. By Lemma B.2.4 of [16], it suffices to show that \( H^1(F_v, T) \) is torsion provided that \( T(F_v) \) and \( T^*(F_v) \) are trivial. By Lemma B.2.3 of [16], it therefore suffices to show that \( H^1(F_v, T/p^n T) \) is bounded independently of \( n \). The triviality of the local Euler characteristic [17, Ch. II, Proposition 17], together with local duality,
shows that

$$\#H^1(F_v, T/p^n T) = \#(T/p^n T)(F_v) \cdot \#(T^*/p^n T^*)(F_v),$$

which is bounded independently of $n$ whenever $T(F_v) = T^*(F_v) = 0$. \qed

The next lemma, in conjunction with Lemma 2.2.8, will be fundamental in extracting information from the general results on Euler systems in [16, §2.3].

**Lemma 2.2.11.** There are canonical 5-term exact sequences

$$(2.2.5) \quad 0 \longrightarrow \text{Sel}(D_\infty, T) \longrightarrow \text{Sel}^\Sigma(D_\infty, T) \longrightarrow H^1(D_\infty, p, T) \longrightarrow X^*(D_\infty) \longrightarrow X^*_\Sigma(D_\infty) \longrightarrow 0$$

and

$$(2.2.6) \quad 0 \longrightarrow \text{Sel}_\Sigma(D_\infty, T) \longrightarrow \text{Sel}(D_\infty, T) \longrightarrow H^1(D_\infty, p^*, T) \longrightarrow X^*(D_\infty, p^*) \longrightarrow X^*(D_\infty) \longrightarrow 0$$

**Proof.** If we show that $H^1_1(D_\infty, p, T) = 0$, then we have that $H^1_1(D_\infty, p, W^*) = H^1(D_\infty, p, W^*)$ by local duality. Also, by global duality, the images of the maps

$$\text{Sel}(D_\infty, T) \xrightarrow{\text{loc}_p} H^1(D_\infty, p, T)$$

$$\text{Sel}(D_\infty, W^*) \xrightarrow{\text{loc}_p} H^1(D_\infty, p, W^*)$$

are exact orthogonal complements (see [16, Theorem 1.7.3]). Thus the exact sequences $(2.2.5)$ and $(2.2.6)$ will follow from the definition of the Selmer groups.

To show that $H^1_1(D_\infty, p, T) = 0$, let $v$ be a place of $D_\infty$ above $p$. The fact that $D_{\infty,v}$ does not split $V$ (Lemma 2.2.5) together with the cohomology sequence associated to

$$0 \longrightarrow T \longrightarrow V \longrightarrow W \longrightarrow 0$$
shows that, for any $F \subseteq D_{\infty,v}$ finite over $K_p$, 

$$H^1_c(F, T) \cong H^0(F, W).$$

We want to show that taking the inverse limit (with respect to corestriction) over all such $F$ gives $\varprojlim H^1(F, T) = 0$. The extension of $K_p$ generated by $W$ is unramified (recall that by assumption $p$ is coprime to the conductors of $\psi$ and $\chi$), but $D_{\infty,v}$ contains an infinite ramified pro-$p$ extension of $K_p$. Thus the intersection of $D_{\infty,v}$ with $K_p(W)$ is finite over $K_p$. This gives what we want, since $K_p(W)$ is not finite over $K_p$ (the primes over $p$ are finitely decomposed in $K_\infty$). \hfill \Box

In order to make full use of the previous lemma (especially in the case $\psi = \overline{\psi} \circ \tau$), we will need to establish some relationship between the compact and discrete Selmer groups (Proposition 2.2.13).

**Lemma 2.2.12.** Let $S$ be the set of places of $K$ which divide $p\infty$ or are ramified for $T$. If $K_S/K$ is the maximal extension of $K$ unramified outside of $S$, then for any finite extension $L/K$ contained in $K_S$,

$$\text{Sel}^\Sigma(L, T) = H^1(K_S/L, T).$$

**Proof.** If $v \notin S$, then $H^1_c(L_v, T) = H^1_{ur}(L_v, T)$ by Lemma 1.3.5 of [16], which shows one inclusion. For $v \in S$ not dividing $p\infty$, both $V$ and $V^*$ are ramified at $v$, so that $H^1(L_v, V) = 0$ by Proposition 2.2.10 (since $L_v/K_v$ is unramified). Thus $H^1_c(L_v, T) = H^1(L_v, T)$, which gives equality. \hfill \Box

**Proposition 2.2.13.** There is a canonical isomorphism of $\Lambda(D_\infty)$-modules

$$\text{Sel}^\Sigma(D_\infty, T) \longrightarrow \text{Hom}_{\Lambda(D_\infty)}(X^\Sigma(D_\infty), \Lambda(D_\infty)).$$

**Proof.** This is Lemma 1.1.9 of [1], the proof of which follows Proposition 4.2.3 of [12]. Let $L \subseteq D_\infty$ be a finite extension of $K$ and let $S$ be the set of places of $K$ dividing $fp\infty$, where $f = \text{cond} \psi$. Note that $S$ is also the the set of places which
are either ramified for $T^*$ or divide $p \infty$. Let $K_S$ be the maximal extension of $K$ unramified outside of $S$. Then Lemma 2.2.12 gives an equality

$$\text{Sel}^\Sigma(L, T) = H^1(K_S/L, T) = \varprojlim_k H^1(K_S/L, T/p^kT).$$

The cohomology sequence associated to

$$0 \longrightarrow T/p^kT \longrightarrow W \xrightarrow{p^k} W \longrightarrow 0$$

gives a surjective map $H^1(K_S/L, T/p^kT) \rightarrow H^1(K_S/L, W)[p^k]$, the kernel of which is $W(L)/p^kW(L)$. Define $X_S(L) = H^1(K_S/L, W)^\vee$. Then the augmentation map $\Lambda(L) \rightarrow \mathcal{O}$ induces an isomorphism

$$\text{Hom}_{\Lambda(L)}(X_S(L), \Lambda(L)) \cong \text{Hom}_{\mathcal{O}}(X_S(L), \mathcal{O}).$$

Moreover, there is an isomorphism

$$\text{Hom}_{\mathcal{O}}(X_S(L), \mathcal{O}) \cong \varprojlim_k H^1(K_S/L, W)[p^k].$$

Putting all this together gives a short exact sequence

$$0 \longrightarrow \varprojlim_k W(L)/p^kW(L) \longrightarrow H^1(K_S/L, T) \longrightarrow \text{Hom}_{\Lambda(L)}(X_S(L), \Lambda(L)) \longrightarrow 0.$$

Note that the size of $\varprojlim_k W(L)/p^kW(L) = W(L)$ is finite and bounded independently of $L \subseteq D_\infty$ because $D_\infty$ does not split $W$ by Lemma 2.2.5. We claim that taking the inverse limit over $L \subseteq D_\infty$ gives an isomorphism

$$(2.2.7) \quad \text{Sel}^\Sigma(D_\infty, T) \longrightarrow \text{Hom}_{\Lambda(D_\infty)}(X_S(D_\infty), \Lambda(D_\infty)).$$

Indeed, if $L'$ is large enough that $W(L') = W(D_\infty)$, then for $L \subseteq D_\infty$ a finite extension of $L'$, the corestriction map $W(L) \rightarrow W(L')$ is multiplication by $[L : L']$. It follows that $\varprojlim W(L) \rightarrow W(L')$ is the zero map for all $L'$ sufficiently large, so $\varprojlim W(L) = 0$. 

32
By Lemma 1.3.5 of [16], we have $H^1_f(L_v, W) = H^1_{ur}(L_v, W)$ whenever $v$ does not lie over a place in $S$. Thus we get an exact sequence

$$(2.2.8) \quad 0 \longrightarrow \text{Sel}^\Sigma(L, W) \longrightarrow H^1(K_S/L, W) \longrightarrow \bigoplus_{v \mid f} H^1(L_v, W).$$

By local Tate duality, the last term in this sequence is isomorphic to the Pontryagin dual of $\bigoplus_{v \mid f} H^1(L_v, T^*)$. The $L_v$ Galois cohomology sequence associated to

$$0 \longrightarrow T^* \longrightarrow V^* \longrightarrow W^* \longrightarrow 0$$

contains the exact sequence

$$V^*(L_v) \longrightarrow W^*(L_v) \longrightarrow H^1(L_v, T^*) \longrightarrow H^1(L_v, V^*).$$

The first term in the sequence is 0 since $V^*$ is ramified at $v$ and $L_v/K_v$ is unramified, and the last term is likewise 0 by Proposition 2.2.10, so the middle two terms are isomorphic.

Taking the Pontryagin dual of the sequence (2.2.8) and taking the direct limit over $L$ then gives us a sequence

$$\bigoplus_{v \mid f} W^*(D_{\infty, v}) \longrightarrow X_S(D_{\infty}) \longrightarrow X^\Sigma(D_{\infty}) \longrightarrow 0.$$ 

The first term in this sequence is a torsion $O$-module (since $W^*$ is) and a fortiori torsion over $\Lambda(D_{\infty})$. Applying the functor $\text{Hom}_{\Lambda(D_{\infty})}(-, \Lambda(D_{\infty}))$ then gives an isomorphism

$$\text{Hom}_{\Lambda(D_{\infty})}(X^\Sigma(D_{\infty}), \Lambda(D_{\infty})) \cong \text{Hom}_{\Lambda(D_{\infty})}(X_S(D_{\infty}), \Lambda(D_{\infty})).$$

Comparing this with (2.2.7) gives the proposition. \hfill \Box

The following theorem gives all of the information which we will obtain from applying the Euler system machinery directly over $D_{\infty}$. 

33
Theorem 2.2.14. $X^*_\Sigma(D_\infty)$ and $Z(D_\infty)$ are torsion $\Lambda(D_\infty)$-modules and there is a divisibility of characteristic ideals $\text{char } X^*_\Sigma(D_\infty) | \text{char } Z(D_\infty)$. Moreover, $\text{Sel}^\Sigma(D_\infty, T)$ is torsion-free of rank 1 over $\Lambda(D_\infty)$.

If $\psi = \bar{\psi} \circ \tau$, $c = \frac{1}{2}w - 1$, and the sign in the functional equation of $\psi$ is $-1$, then $X^*(D_\infty)$ has rank 1 over $\Lambda(D_\infty)$ and $\text{Sel}(D_\infty, T) = \text{Sel}^\Sigma(D_\infty, T)$. Otherwise, $X^*(D_\infty)$ is a torsion $\Lambda(D_\infty)$-module.

Proof. Choose $a$ such that $C_a(D_\infty) \neq 0$ (possible by Proposition 2.2.9). The fact that $X^*_\Sigma(D_\infty)$ is a torsion $\Lambda(D_\infty)$-module follows from [16, Theorem 2.3.2] (cf. the discussion preceding Lemma 2.1.3). The divisibility of characteristic ideals follows from [16, Theorem 2.3.3]. That $Z(D_\infty)$ is a torsion $\Lambda(D_\infty)$-module will follow from Proposition 2.2.9 once we show that $\text{Sel}^\Sigma(D_\infty, T)$ is torsion-free of rank 1 over $\Lambda(D_\infty)$. The fact that $\text{Sel}^\Sigma(D_\infty, T)$ is torsion free of positive rank follows from Propositions 2.2.13 and 2.2.9 (given that Proposition 2.2.7 holds). The exact sequence (2.2.5), together with Lemma 2.2.8 and that fact that $X^*_\Sigma(D_\infty)$ is torsion, shows that the rank of $X^*(D_\infty)$ is at most 1.

Note that if $X^*(D_\infty)$ has rank 1, then $\text{loc}_p$ must be trivial, as $H^1(D_{\infty, p}, T)$ is torsion-free. If this occurs, Proposition 2.2.9 shows that we must have $\bar{\psi} \circ \tau = \psi$, $c = \frac{1}{2}w - 1$, and the sign in the functional equation of $\psi$ is $-1$, so $\text{loc}_p$ is non-trivial. Thus, the exact sequence (2.2.6) and Lemma 2.2.8 imply that $X^{*, \Sigma}(D_\infty)$ has rank 1. Otherwise, if $X^*(D_\infty)$ is torsion, we see (again from (2.2.6) and Lemma 2.2.8) that $X^{*, \Sigma}(D_\infty)$ has rank at most 1. Briefly interchanging the roles of $T$ and $T^*$, $p$ and $p^*$, we see that $X^{\Sigma}(D_\infty)$ has rank at most 1 as well. Thus Proposition 2.2.13 implies that $\text{Sel}^\Sigma(D_\infty, T)$ must have rank exactly 1.

The remainder of the proof will be a study of the 5-term exact sequences in Lemma 2.2.11 using Lemma 2.2.8 and Propositions 2.2.9 and 2.2.13. We first deal with the “otherwise” case, i.e., assume that if $\psi = \bar{\psi} \circ \tau$ and $c = \frac{1}{2}w - 1$, then the sign in the functional equation of $\psi$ is $+1$. In this case, the map $\text{loc}_p$ in (2.2.5) is nonzero.
by Proposition 2.2.9. Thus Lemma 2.2.8, together with the fact that $X^*_E(D_\infty)$ is torsion, shows that $X^*(D_\infty)$ is likewise torsion over $\Lambda(D_\infty)$.

We now turn to the case that $c = \frac{1}{2}w - 1$, $\psi = \overline{\psi} \circ \tau$, and the sign in the functional equation of $\psi$ is $-1$. We know that for some $a$, the class $c_a(D_\infty)$ (which lies in $\text{Sel}(D_\infty, T)$ by Proposition 2.2.9) is not torsion, since its image under $\text{loc}_p$ is nonzero and $H^1(D_{\infty,p}, T)$ is torsion-free of rank 1. But then $\text{Sel}^\Sigma(D_\infty, T)/\text{Sel}(D_\infty, T)$ is torsion, and so must be zero, since it injects via $\text{loc}_p$ into the torsion-free module $H^1(D_{\infty,p}, T)$. Hence $\text{loc}_p$ is trivial and $X^*(D_\infty)$ has rank 1. □

2.3. Divisibility from descent

In this section, we prove the reverse divisibility of the first part of Theorem 2.2.14 and determine the characteristic ideal of $X^*(D_\infty)$ when the sign in the functional equation of $\psi$ is not $-1$. The method involves twisting Rubin's 2-variable main conjecture [14] to give a 2-variable main conjecture for $T$ over $K_\infty$. We descend from $K_\infty$ to $D_\infty$ to complete the description of $\text{char } X^*_E(D_\infty)$. This section closely follows Section 2.4 of [1].

2.3.1. Twisting the 2-variable main conjecture. In order to apply the main results of Rubin's paper [14], we first need to establish some notation.

Let $L_\infty$ be an abelian extension of $K$ which is finite over $K_\infty$ and splits both $V$ and $V^*$. There is a decomposition $\text{Gal}(L_\infty/K) \cong \text{Gal}(K_\infty/K) \times \Delta$, where $\Delta \cong \text{Gal}(L_\infty/K_\infty)$ is finite. (This decomposition is not canonical if $p \mid [L_\infty : K_\infty]$.) For any $F \subseteq L_\infty$, define $M^\Sigma(F)$, resp. $M(F)$, resp. $M_\Sigma(F)$, to be the maximal abelian $p$-extension of $F$ unramified outside of $p$, resp. outside of $p$, resp. everywhere.

For an extension $F \subseteq L_\infty$ finite over $K$, let $\mathcal{E}(F)$ be the completion of the global units $\mathcal{O}_k^\times \otimes \mathcal{O}$. If $F \subseteq L_\infty$ is infinite over $K$, set $\mathcal{E}(F) = \lim \downarrow \mathcal{E}(F')$ (the inverse limit being taken, as always, over subextensions $F' \subseteq F$ finite over $K$). If $a \subseteq K$ is an integral ideal prime to $fp$, we define $\mathcal{U}_a(F) \subseteq \mathcal{E}(F)$ to be the submodule generated by
the elliptic unit Euler system \( \{ \theta(i, a) \} \) discussed in 2.1.5. We further let \( \mathcal{U}(F) \) be the submodule generated by all the \( \mathcal{U}_a(F) \).

**Lemma 2.3.1.** There are \( \mathcal{O} \)-module isomorphisms

\[
\alpha : H^1(L_\infty, \Phi/\mathcal{O}) \longrightarrow H^1(L_\infty, W^*)
\]
\[
\beta : \lim\limits_{\rightarrow} H^1(L, \mathcal{O}(1)) \longrightarrow \lim\limits_{\rightarrow} H^1(L, T)
\]

(the inverse limits being taken with respect to fields \( L \subseteq L_{\infty} \) finite over \( K \)) satisfying \( \alpha \circ \text{Tw}_{\nu^*}(\lambda) = \lambda \circ \alpha \) and \( \beta \circ \text{Tw}_{\nu^*}^{-1}(\lambda) = \lambda \circ \beta \) for all \( \lambda \in \Lambda(L_\infty) \). Moreover, the restriction of \( \alpha \) gives an \( (\mathcal{O} \text{-module}) \) isomorphism

\[
\alpha : \text{Hom}(\text{Gal}(M_{\infty}(L_\infty)/L_\infty), \Phi/\mathcal{O}) \longrightarrow \text{Sel}^{\infty}(L_\infty, W^*),
\]

and similarly for \( M(L_\infty) \) and \( M_{\Sigma}(L_\infty) \). The restriction of \( \beta \) gives isomorphisms

\[
\beta : \mathcal{E}(L_\infty) \otimes \mathcal{O} \longrightarrow \text{Sel}^{\infty}(L_\infty, T)
\]
\[
\beta : \mathcal{U}(L_\infty) \otimes \mathcal{O} \longrightarrow C(L_\infty).
\]

(See 2.2.4 for the definition of \( C(K_\infty) \)).

**Proof.** This is Lemma 2.4.5 of [1]. The existence of \( \alpha \) and \( \beta \) is clear from the fact that \( W^* \) and \( T \) are trivial as \( G_{L_\infty} \)-modules and isomorphic as groups to \( \Phi/\mathcal{O} \) and \( \mathcal{O} \), respectively (note that the characters defining \( W^* \) and \( T \) are Tate duals of each other). In order to prove the statements about \( \alpha \), it suffices by Lemma 1.3.5 of [16] to check that the condition of being unramified at a prime \( v \) of \( L_\infty \) is equivalent to being locally trivial at \( v \). This is Lemma B.3.3 of [16]: \( L_{\infty,v} \) contains the unique unramified \( \mathbb{Z}_p \)-extension of \( K_v \), so that \( \text{Gal}(L_{\infty,v}/L_{\infty,v}) \) has trivial pro-\( p \) part, whence \( H^1(L_{\infty,v}^{ur}, \Phi/\mathcal{O}) = 0 \) (see the proof of [16, Lemma B.3.3] for more details). Turning our attention to \( \beta \), we see that by the above and local duality, the local conditions defining \( \text{Sel}^{\infty}(L_\infty, T) \) are the same as the unramified conditions,
whence the first isomorphism. That $\beta$ maps $\mathcal{U}(L_\infty) \otimes \mathcal{O}$ onto $C(L_\infty)$ follows from the definition of our Euler systems $c_a$ (cf. the proof of Proposition 2.1.2). \hfill \Box

This lemma allows us to apply the main results of Rubin's paper [14] to get a 2-variable main conjecture for our representation $W^*$.

**Theorem 2.3.2.** $X^*(K_\infty)$ is a torsion $\Lambda(K_\infty)$-module, $\text{Sel}^\Sigma(K_\infty, T)$ has rank 1 over $\Lambda(K_\infty)$, and there are equalities of ideals in $\Lambda(K_\infty) \otimes \Phi$

$$\text{char } X^*(K_\infty) = \text{char } \left( H^1(K_{\infty, p}, T)/\text{loc}_p C(K_\infty) \right)$$

and

$$\text{char } X^*_p(K_\infty) = \text{char } Z(K_\infty).$$

(See 2.2.4 for the definition of $Z(K_\infty)$.)

**Proof.** We view $\eta^*$ as a character of the group $\text{Gal}(L_\infty/K) \cong \text{Gal}(K_\infty/K) \times \Delta$, and so write $\eta^* = \kappa^* \nu^*$, where $\nu^*$ is a character of the finite group $\Delta$. Taking $\Delta$-invariants of the various $\Lambda(L_\infty)$-modules of Lemma 2.3.1 (and keeping in mind how we have defined the action of $\Lambda(L_\infty)$ on the $Xs$ in 2.1.3) yields the following formulas:

$$\text{Tw}_{\eta^*}^{-1}(\text{char}(\text{Gal}(M^\Sigma(L_\infty)/L_\infty))^{\nu^*}) = \text{char } X^*\Sigma(K_\infty)^t,$$

similarly for $M(L_\infty)$ and $M^\Sigma(L_\infty)$, and

$$\text{Tw}_{\eta^*}^{-1}(\text{char}(\mathcal{E}(L_\infty)/\mathcal{U}(L_\infty))^{\nu^*}) = \text{char } Z(K_\infty)^t.$$

For the descent of Selmer groups from $L_\infty$ to $K_\infty$, see the proof of Proposition 2.2.6. The statement of the theorem is then a consequence of the usual 2-variable main conjecture for $K$ ([14, Theorem 4.1(i)]; also cf. Theorems 3.3.1 and 3.3.2 of [16]) via the twisting theorems of Ch. 6 of [16]. \hfill \Box

37
2.3.2. Preparations for descent. Unfortunately, we will need several technical results in order to extract information about our situation over $D_{\infty}$ from Theorem 2.3.2, which deals with the 2-variable situation over $K_{\infty}$. Recall that we have defined the ideal $I \subseteq \Lambda(K_{\infty})$ to be the kernel of the natural surjective map $r : \Lambda(K_{\infty}) \to \Lambda(D_{\infty})$, so that $I = (\gamma - 1)$ for any topological generator $\gamma$ of $\text{Gal}(K_{\infty}/D_{\infty})$.

Lemma 2.3.3. If $q = p$ or $p^*$, then the restriction map

$$H^1(D_{\infty,q}, W^*) \to H^1(K_{\infty,q}, W^*)$$

has finite kernel.

PROOF. This map is dual to the map (2.2.4) in the proof of Proposition 2.2.6, the cokernel of which was proved to be finite. \qed

Lemma 2.3.4. The kernel of the restriction map

$$\bigoplus_{v|f} H^1(D_{\infty,v}, W^*) \to \bigoplus_{v|f} H^1(K_{\infty,v}, W^*)$$

has finite exponent.

PROOF. By the inflation-restriction sequence, the kernel is

$$\bigoplus_{v|f} H^1(K_{\infty,v}/D_{\infty,v}, W^*(K_{\infty,v})).$$

Note that $K_{\infty,v}/D_{\infty,v}$ is a $\mathbb{Z}_p$-extension, so by Lemma B.2.8 of [16] this group is isomorphic to

$$\bigoplus_{v|f} W^*(K_{\infty,v})/(\gamma - 1)W^*(K_{\infty,v}),$$

where $\gamma$ is a topological generator of $\text{Gal}(K_{\infty,v}/D_{\infty,v})$. Also, $K_{\infty,v}/K_v$ is the unique unramified $\mathbb{Z}_p$-extension of $K_v$. By definition of $f$, $W^*$ is ramified at $v$, so $W^*(K_{\infty,v})$ is finite. The size of $W^*(K_{\infty,v})$ only depends on the prime of $K$ over which $v$ lies. \qed
Proposition 2.3.5. The Pontryagin dual of the restriction map

\[ \text{Sel}^\Sigma(D_\infty, W^*) \longrightarrow \text{Sel}^\Sigma(K_\infty, W^*)[I], \]

i.e., the \( \Lambda(D_\infty) \)-module homomorphism

\[ X^* \Sigma(K_\infty)/IX^* \Sigma(K_\infty) \longrightarrow X^* \Sigma(D_\infty), \]

has finite cokernel and finite-exponent kernel. The same is true of \( X^* \) and \( X^*_\Sigma \).

In particular, \( X^*_\Sigma(D_\infty) \) is a torsion \( \Lambda(D_\infty) \)-module exactly when the quotient \( X^*_\Sigma(K_\infty)/IX^*_\Sigma(K_\infty) \) is.

**Proof.** Let \( S \) be the set of places of \( K \) dividing \( f_{\infty} \) and let \( K_S \) be the maximal extension of \( K \) unramified outside \( S \). The definition of \( \text{Sel}^\Sigma \) gives a commutative diagram with exact rows:

\[
\begin{array}{cccccc}
0 & \longrightarrow & \text{Sel}^\Sigma(D_\infty, W^*) & \longrightarrow & H^1(K_S/D_\infty, W^*) & \longrightarrow & \bigoplus_{v|f} H^1(D_\infty, W^*) \\
& & \text{res} \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \text{Sel}^\Sigma(K_\infty, W^*)[I] & \longrightarrow & H^1(K_S/K_\infty, W^*)[I] & \longrightarrow & \bigoplus_{v|f} H^1(K_\infty, W^*)
\end{array}
\]

The kernel of the middle vertical map is

\[ H^1(K_\infty/D_\infty, W^*(K_\infty)) \cong W^*(K_\infty)/IW^*(K_\infty), \]

which is finite: if \( K_\infty \) splits \( W^* \), then (by Lemma 2.2.5) a topological generator \( \gamma \) of \( \text{Gal}(K_\infty/D_\infty) \) acts nontrivially on \( W^* \), which is divisible, so \( W^*(K_\infty)/IW^*(K_\infty) = 0 \). Thus the restriction map (the leftmost vertical arrow) likewise has finite kernel.

By Lemma 2.3.4, the kernel of the right-hand vertical map is finite-exponent. Note that the middle vertical map is surjective by the inflation-restriction sequence, as \( \text{Gal}(K_\infty/D_\infty) \cong \mathbb{Z}_p \) has cohomological dimension 1. Thus (by the snake lemma), the cokernel of the restriction map also has finite exponent. Since the Pontryagin
dual of a finite-exponent module is likewise of finite exponent, we have proved the claim for $X^\ast, \Sigma$.

To prove the claim for $X^\ast$, we use the commutative diagram

$$
\begin{array}{c}
0 \longrightarrow \text{Sel}(D_{\infty}, W^\ast) \longrightarrow \text{Sel}^\Sigma(D_{\infty}, W^\ast) \longrightarrow H^1(D_{\infty, p^\ast}, W^\ast) \\
\downarrow \text{res} \quad \downarrow \quad \downarrow \\
0 \longrightarrow \text{Sel}(K_{\infty}, W^\ast)[I] \longrightarrow \text{Sel}^\Sigma(K_{\infty}, W^\ast)[I] \longrightarrow H^1(K_{\infty, p^\ast}, W^\ast)
\end{array}
$$

with exact rows (cf. Lemma 2.2.11). The kernel of the middle vertical map is finite by the above, as is the kernel of the right-hand vertical map (Lemma 2.3.3). Moreover, the cokernel of the middle map is of finite exponent (again by the above), so that another application of the snake lemma proves the claim for $X^\ast$. The proof for $X^\ast, \Sigma$ is the same using the diagram

$$
\begin{array}{c}
0 \longrightarrow \text{Sel}^\Sigma(D_{\infty}, W^\ast) \longrightarrow \text{Sel}(D_{\infty}, W^\ast) \longrightarrow H^1(D_{\infty, p}, W^\ast) \\
\downarrow \text{res} \quad \downarrow \quad \downarrow \\
0 \longrightarrow \text{Sel}^\Sigma(K_{\infty}, W^\ast)[I] \longrightarrow \text{Sel}(K_{\infty}, W^\ast)[I] \longrightarrow H^1(K_{\infty, p}, W^\ast)
\end{array}
$$

(again cf. Lemma 2.2.11). □

Following [1], we define the decent defect

$$
\mathcal{D} = \text{char}_{\Lambda(D_{\infty})} X^\ast_{\Sigma}(K_{\infty})[I].
$$

Recall that we have denoted by $r : \Lambda(K_{\infty}) \rightarrow \Lambda(D_{\infty})$ the natural map.

**Corollary 2.3.6.** $\mathcal{D}$ is nonzero and

$$
\text{char}_{\Lambda(D_{\infty})} X^\ast_{\Sigma}(D_{\infty}) = \mathcal{D} \cdot r(\text{char}_{\Lambda(K_{\infty})} X^\ast_{\Sigma}(K_{\infty}))
$$

as ideals in $\Lambda(D_{\infty})$.

**Proof.** By Theorem 2.2.14, $X^\ast_{\Sigma}(D_{\infty})$ is a torsion $\Lambda(D_{\infty})$-module. The previous proposition (Proposition 2.3.5) implies that $X^\ast_{\Sigma}(K_{\infty})/IX^\ast_{\Sigma}(K_{\infty})$ is likewise torsion.
The fact that $\mathcal{D}$ is nonzero now follows from [14, Lemma 6.2(i)], and the equality of characteristic ideals is [14, Lemma 6.2(ii)]. \[ \square \]

2.3.3. Descent to the anticyclotomic tower. Using the results of 2.3.2 we descend the twisted 2-variable main conjecture to the anticyclotomic tower. The ultimate goal will be Proposition 2.3.8, of which the main theorem of §2.3, Theorem 2.3.9, is an easy consequence. Recall that we have defined $Z(F) = \text{Sel}^E(F, T)/C(F)$, where $C(F)$ is the module generated by the Euler systems $c_a(F)$ as $a$ runs over ideals of $K$ prime to $\mathfrak{p}$ (cf. 2.2.4).

**Proposition 2.3.7.** The $\Lambda(D_{\infty})$-module homomorphisms

$$\text{Sel}^E(K_{\infty}, T)/I\text{Sel}^E(K_{\infty}, T) \longrightarrow \text{Sel}^E(D_{\infty}, T)$$

$$Z(K_{\infty})/IZ(K_{\infty}) \longrightarrow Z(D_{\infty})$$

are injective and the cokernels are torsion of characteristic ideal divisible by $\mathcal{D}$.

**Proof.** This is essentially Proposition 2.4.15 of [1]. As before, let $S$ be the set of places of $K$ dividing $\mathfrak{p}\mathcal{O}_{\infty}$ and denote by $K_S$ the maximal extension of $K$ unramified outside of $S$. For any $L \subseteq K_{\infty}$ finite over $K$, Proposition 4.1.1 of [12] shows there is an exact sequence

$$0 \longrightarrow X_1^+(L) \longrightarrow H^2(K_S/L, T) \longrightarrow \bigoplus_{v \in S_L} H^0(L_v, W^*)^\vee,$$

where $S_L$ is the set of places of $L$ lying over places in $S$. Taking the inverse limit over $L$ yields

$$0 \longrightarrow X_1^+(K_{\infty}) \longrightarrow \varprojlim_v H^2(K_S/L, T) \longrightarrow \bigoplus_{v | \mathfrak{p}} H^0(K_{\infty,v}, W^*)^\vee.$$

Shapiro’s Lemma gives

$$\varprojlim_v H^2(K_S/L, T) \cong H^2(K_S/K, T \otimes \varprojlim \Lambda(K_{\infty})).$$
so taking $I$-torsion of the above exact sequence yields

$$0 \longrightarrow X^*_\Sigma(K_\infty)[I] \longrightarrow H^2(K_S/K, T \otimes \Lambda(K_\infty))[I] \longrightarrow \bigoplus_{v|\mathcal{P}} H^0(K_{\infty,v}, W^*)^\vee[I].$$

The final term of this sequence is dual to

$$\bigoplus_{v|\mathcal{P}} W^*(K_{\infty,v})/IW^*(K_{\infty,v}) \cong \bigoplus_{v|\mathcal{P}} H^1(K_{\infty,v}/D_{\infty,v}, W^*(K_{\infty,v})).$$

i.e., the kernel of the restriction map

$$\bigoplus_{v|\mathcal{P}} H^1(D_{\infty,v}, W^*) \longrightarrow \bigoplus_{v|\mathcal{P}} H^1(K_{\infty,v}, W^*).$$

This kernel has finite exponent by Lemmas 2.3.3 and 2.3.4, so that Corollary 2.3.6 shows that $H^2(K_S/K, T \otimes \Lambda(K_\infty))[I]$ is torsion over $\Lambda(D_\infty)$ with characteristic ideal divisible by $\mathcal{D}$.

Taking the Galois cohomology of the sequence

$$0 \longrightarrow T \otimes \Lambda(K_\infty) \overset{\gamma-1}{\longrightarrow} T \otimes \Lambda(K_\infty) \longrightarrow T \otimes \Lambda(D_\infty) \longrightarrow 0$$

gives the exact sequence

$$0 \longrightarrow H^1(K_S/K, T \otimes \Lambda(K_\infty)) \otimes_{\Lambda(K_\infty)} \Lambda(D_\infty) \longrightarrow$$

$$\longrightarrow H^1(K_S/K, T \otimes \Lambda(D_\infty)) \longrightarrow H^2(K_S/K, T \otimes \Lambda(K_\infty))[I] \longrightarrow 0.$$

Thus, Lemma 2.2.12 and another application of Shapiro’s Lemma shows that the natural map

$$\text{Sel}^\Sigma(K_\infty, T)/I \text{Sel}^\Sigma(K_\infty, T) \longrightarrow \text{Sel}^\Sigma(D_\infty, T)$$

is injective with torsion cokernel of characteristic ideal divisible by $\mathcal{D}$. The map

$$C(K_\infty)/IC(K_\infty) \longrightarrow C(D_\infty)$$
is surjective (since the elliptic units are universal norms in the cyclotomic direction), so the snake lemma implies the statement for $Z$.

\begin{proposition}
There is an equality of ideals in $\Lambda(D_{\infty})$
\[ \operatorname{char} X_2^*(D_{\infty}) = \operatorname{char} Z(D_{\infty}). \]
\end{proposition}

\begin{proof}
The divisibility
\[ \operatorname{char} X_2^*(D_{\infty}) \mid \operatorname{char} Z(D_{\infty}) \]

is part of Theorem 2.2.14. Proposition 2.3.7 implies $Z(K_{\infty})/IZ(K_{\infty})$ is a torsion $\Lambda(D_{\infty})$-module (because $Z(D_{\infty})$ is by Theorem 2.2.14). Thus Lemma 6.2(i) of [14] shows that $Z(K_{\infty})[I]$ is likewise a torsion $\Lambda(D_{\infty})$-module. An application of Lemma 6.2(ii) of [14] gives an equality of characteristic ideals
\[ r(\operatorname{char}_{\Lambda(K_{\infty})} Z(K_{\infty})) \operatorname{char}_{\Lambda(D_{\infty})} Z(K_{\infty})[I] = \operatorname{char}_{\Lambda(D_{\infty})} Z(K_{\infty})/IZ(K_{\infty}). \]

By Proposition 2.3.7, we may write the characteristic ideal of the cokernel of
\[ Z(K_{\infty})/IZ_a(K_{\infty}) \longrightarrow Z(D_{\infty}) \]
as the product $J\mathfrak{D}$ for some ideal $J \subseteq \Lambda(D_{\infty})$. Using the above, we then get the equality
\[ \operatorname{char}_{\Lambda(D_{\infty})} Z(D_{\infty}) = J\mathfrak{D} \operatorname{char}_{\Lambda(D_{\infty})} Z(K_{\infty})/IZ(K_{\infty}) \]
\[ = J\mathfrak{D}r(\operatorname{char}_{\Lambda(K_{\infty})} Z(K_{\infty})) \operatorname{char}_{\Lambda(D_{\infty})} Z(K_{\infty})[I]. \]

The 2-variable main conjecture, Theorem 2.3.2, gives the equality
\[ r(\operatorname{char}_{\Lambda(K_{\infty})} Z(K_{\infty})) = r(\operatorname{char}_{\Lambda(K_{\infty})} X_2^*(K_{\infty})), \]
so that we may apply Corollary 2.3.6 to get

$$\text{char}_{\Lambda(D_{\infty})} Z(D_{\infty}) = J \text{char}_{\Lambda(D_{\infty})} X_{\Sigma}^*(D_{\infty}) \text{char}_{\Lambda(D_{\infty})} Z(K_{\infty})[I],$$

which proves the remaining divisibility. \(\square\)

We can now prove what one might refer to as the “anticyclotomic main conjecture” for Grössencharaktere of \(K\), i.e., Theorem 2.2.1 and the rank statement of Theorem 2.2.2. Unfortunately, information about the associated “\(\mu\)-invariant conjecture” is lost in Proposition 2.2.6 (though the proof shows that this holds in some special cases: e.g., when \(p\) does not divide \([K(f) : K]\) and \(K_{q}(W^{*}[\pi]) \neq K_{q}\) for \(q = p\) and \(p^{*}\), \(\pi\) a uniformizer of \(O\)).

**Theorem 2.3.9.** If \(c = \frac{1}{2}w - 1\), \(\psi = \overline{\psi} \circ \tau\), and the sign in the function equation of \(\psi\) is \(-1\), then \(\text{Sel}(D_{\infty}, T)\) is torsion free of rank 1 over \(\Lambda(D_{\infty})\), \(X^{*}(D_{\infty})\) has rank 1, and there is an equality of characteristic ideals

$$\text{char} X_{\Sigma}^{*}(D_{\infty}) = \text{char}(\text{Sel}(D_{\infty}, T)/C(D_{\infty})).$$

Otherwise, \(X^{*}(D_{\infty})\) is a torsion \(\Lambda(D_{\infty})\)-module and there is an equality of ideals in \(\tilde{\Lambda}(D_{\infty}) \otimes_{\tilde{\Theta}} \tilde{\Phi}\)

$$(\text{char}_{\Lambda(D_{\infty})} X^{*}(D_{\infty})) = (\mu(D_{\infty}, \eta^{*})).$$

**Proof.** In the case that \(c = \frac{1}{2}w - 1\), \(\psi = \overline{\psi} \circ \tau\), and the sign in the function equation of \(\psi\) is \(-1\), the statements follow from Theorem 2.2.14 and Proposition 2.3.8.

In the remaining case, the fact that \(X^{*}(D_{\infty})\) is torsion is once again part of Theorem 2.2.14, and we can compute its characteristic ideal by considering the exact sequence

$$0 \longrightarrow Z(D_{\infty}) \longrightarrow H^{1}(D_{\infty,p}, T)/\text{loc}_{p} C(D_{\infty}) \longrightarrow X^{*}(D_{\infty}) \longrightarrow X_{\Sigma}^{*}(D_{\infty}) \longrightarrow 0$$
coming from the sequence (2.2.5) of Lemma 2.2.11. Proposition 2.3.8 shows that the middle two terms have the same characteristic ideals, so the theorem now follows from Proposition 2.2.6. □

To complete the proof of Theorem 2.2.2, it remains to identify the characteristic ideal of $X^*(D_\infty)_{\text{tors}}$ in the case that the sign in the functional equation of $\psi$ is $-1$. §2.4 will be devoted to showing that this characteristic ideal is generated by the linear term of the associated 2-variable $p$-adic $L$-function.

2.3.4. Application to Selmer groups over $\mathbb{Q}$. Before proceeding to the proof of Theorem 2.2.2, we explore a consequence of Theorem 2.3.9 towards a generalization to CM modular forms of the Birch and Swinnerton-Dyer conjecture. This will follow from the following “control theorem”.

**Proposition 2.3.10.** $X^*(K)$ has positive rank as an $O$-module if and only if the augmentation ideal $I \subseteq \Lambda(D_\infty)$ divides $\text{char } X^*(D_\infty)$.

(Note that in the case $X^*(D_\infty)$ has positive $\Lambda(D_\infty)$-rank, $\text{char } X^*(D_\infty) = 0$ is divisible by $I$.)

**Proof.** By Proposition 2.4.3, the natural map

$$X^*(D_\infty)/IX^*(D_\infty) \longrightarrow X^*(K)$$

has finite kernel and cokernel. Hence, if $n$ denotes the number of summands killed by a power of $I$ in a cyclic decomposition (up to pseudo-isomorphism) of $X^*(D_\infty)$ as a $\Lambda(D_\infty)$-module, then we have the formula

$$\text{rk}_O X^*(K) = n + \text{rk}_{\Lambda(D_\infty)} X^*(D_\infty).$$

The proposition follows. □

As in 2.1.1, we let $\rho_f : G_\mathbb{Q} \rightarrow \text{GL}_2(K_f, \mathbb{Q}_p)$ be the $p$-adic representation associated to a $\mathbb{Z}$-ordinary newform $f \in S_w(N, \chi)$. Choose a stable lattice $T$ in the representation
space $\mathcal{V}$ of $\rho_f(-c)$ and denote by $\mathcal{W}$ the discrete $G_Q$-module $\mathcal{V}/T$. We can then define the Selmer groups $\text{Sel}(F, \mathcal{W})$ for finite extensions $F$ of $Q$ as in 2.1.2, where the finite conditions $H^1_f(F_v, \mathcal{W})$ are defined as in Greenberg’s article [6], for example. Finally, we denote by $W^r$ the discrete $G_K$-module $(\Phi/\mathcal{O}) \otimes \mathcal{O}_{\psi^r_p}(-c)$.

**Theorem 2.3.11.** Let $f$ be a CM modular form of even weight $w$ with associated Grössencharakter $\psi$. If $c = \frac{1}{2}w - 1$, then the central $L$-value $L(f, w/2)$ vanishes if and only if $\text{Sel}(Q, \mathcal{W})^\vee$ has positive rank as an $\mathcal{O}$-module.

**Proof.** Recall that $\rho_f|_{G_K} = \psi_p \oplus \psi_p^r$, so

$$\text{Sel}(K, \mathcal{W}) = \text{Sel}(K, W^*) \oplus \text{Sel}(K, W^r).$$

Since $\rho_f$ is a representation of $G_Q$, complex conjugation $\tau \in G_Q$ acts on this Selmer group by exchanging the summands (so that in particular the summands are isomorphic as $\mathcal{O}$-modules). When $c = \frac{1}{2}w - 1$, Theorem 2.3.9 and Proposition 2.3.10 imply that $\text{Sel}(K, W^*)^\vee$ has positive $\mathcal{O}$-rank if and only if $L(f, w/2) = 0$, as the interpolation property of $\mu(D_\infty, \eta^*)$ shows this $L$-value vanishes if and only if $I$ divides $(\mu(D_\infty, \eta^*))$. Since $p$ is odd, we have $\text{Sel}(K, \mathcal{W})^{\text{Gal}(K/Q)} = \text{Sel}(Q, \mathcal{W})$. If $L(f, w/2) \neq 0$, then $\text{Sel}(K, \mathcal{W})$ and $\text{Sel}(Q, \mathcal{W})$ are cotorsion $\mathcal{O}$-modules. If $L(f, w/2) = 0$, then the $\text{Gal}(K/Q)$-invariant submodule $\{(b, \tau b) \mid b \in \text{Sel}(K, W^*)\}$ of $\text{Sel}(K, \mathcal{W})$ is of positive $\mathcal{O}$-corank, which shows that $\text{Sel}(Q, \mathcal{W})$ also has positive $\mathcal{O}$-corank, as desired. \hfill $\square$

### 2.4. $p$-adic heights and the linear term

Theorem 2.3.9 gives, in case the sign in the functional equation of $\psi$ is not $-1$, a description of the characteristic ideal of $X^*(D_\infty)$ in terms of a suitable $p$-adic $L$-function. In the case that the sign is $-1$, we would like to similarly determine the characteristic ideal of the torsion submodule $X^*(D_\infty)_{\text{tors}}$ of $X^*(D_\infty)$. To do so, we must first determine the extent to which $X^*(D_\infty)_{\text{tors}}$ and $X^*_S(D_\infty)$ differ; this is achieved by using various duality results. Properties of the $p$-adic height pairing then allow us to express this difference in terms of the linear term of the twisted Katz
$p$-adic $L$-function of 2.1.4. In what follows, we assume that $c = \frac{1}{2} w - 1$, $\psi = \overline{\psi} \circ \tau$, and the sign in the function equation of $\psi$ is $-1$.

2.4.1. Duality. The main results of this section, Propositions 2.4.1 and 2.4.2, can be thought of as $p$-adic functional equations for characteristic ideals of Selmer groups. The proofs of both propositions use ideas of Greenberg (cf. the proof of Theorem 2 of [6]) and follow Section 1.2 of [1]. Recall our convention (made in 2.1.3) that $\Lambda(D_\infty)$ acts on the modules $X^* \Sigma(D_\infty)$, $X^*(D_\infty)$, and $X^*_\Sigma(D_\infty)$ via the involution $\iota$.

**Proposition 2.4.1.** $X(D_\infty)$ and $X^*(D_\infty)$ have the same rank over $\Lambda(D_\infty)$, and there is an equality of characteristic ideals

$$\text{char } X(D_\infty)^t_{\text{tors}} = \text{char } X^*(D_\infty)_{\text{tors}},$$

viewed as ideals in $\Lambda(D_\infty) \otimes \Phi$ (i.e., equality as ideals of $\Lambda(D_\infty)$ up to powers of a uniformizer of $\mathcal{O}$).

**Proposition 2.4.2.** The $\Lambda(D_\infty)$-rank of $X^\Sigma(D_\infty)$ is one greater than the $\Lambda(D_\infty)$-rank of $X^*_\Sigma(D_\infty)$, and there is an equality of characteristic ideals

$$\text{char } X^\Sigma(D_\infty)^t_{\text{tors}} = \text{char } X^*_\Sigma(D_\infty),$$

viewed as ideals in $\Lambda(D_\infty) \otimes \Phi$.

We reduce the problem, via suitable control theorems, to one of comparing the Selmer groups of finite $G_K$-modules, and then use a formula of Wiles relating these groups. We consider Selmer groups attached to twists of $W$ and $W^*$ by characters of $\Gamma = \text{Gal}(D_\infty/K)$. To be precise, suppose $\chi : \text{Gal}(D_\infty/K) \rightarrow (\mathcal{O}')^\times$ is a continuous character, where $\mathcal{O}'$ is a (fixed) extension of $\mathcal{O}$ in which some polynomial generators of the characteristic ideals of $X(D_\infty)_{\text{tors}}$, $X^*(D_\infty)_{\text{tors}}$, $X^\Sigma(D_\infty)_{\text{tors}}$, and $X^*_\Sigma(D_\infty)_{\text{tors}}$ split into linear factors. Given such a $\chi$, let $\mathcal{O}'_\chi$ be $\mathcal{O}'$ with the $G_K$-module structure
for which which $\gamma \in G_K$ acts by multiplication by $\chi(\gamma)$. If $M$ is an $O[G_K]$-module, we define $M(\chi) = M \otimes_{O} O'(\chi)$.

Given any such $\chi$, we define the Selmer groups associated to $W(\chi)$ and $W^*(\chi^{-1})$ exactly as in 2.1.2 (i.e., using the analogous local conditions). Because the local conditions defining the Selmer groups $\text{Sel}^E(F,W)$ and $\text{Sel}^E(F,T^*)$ are not orthogonal under the Tate pairing, we will need to define the auxiliary Selmer group

$$\text{Sel}'(K, W(\chi)) \subseteq \text{Sel}^E(K, W(\chi))$$

to be the set of classes $\tau \in \text{Sel}^E(K, W(\chi))$ such that $\text{loc}_q \tau$ lies in $H^1(K_q, W(\chi))_{\text{div}}$ for $q = p$ or $p^*$. Because $\chi$ is a character of $\text{Gal}(D_\infty/K)$, we have an identification of $\Lambda(D_\infty)$-modules

$$H^1(D_\infty, W(\chi)) = H^1(D_\infty, W)(\chi),$$

and similarly for $W^*$ and for the local cohomology groups. This restricts to an identification of Selmer groups

$$\text{Sel}(D_\infty, W(\chi)) = \text{Sel}(D_\infty, W)(\chi),$$

and similarly for the other Selmer groups defined over $D_\infty$.

**Proposition 2.4.3.** *The natural restriction homomorphism*

$$H^1(K, W(\chi)) \longrightarrow H^1(D_\infty, W)(\chi)^\Gamma$$

*induces maps*

$$\text{Sel}'(K, W(\chi)) \longrightarrow \text{Sel}^E(D_\infty, W)(\chi)^\Gamma$$

$$\text{Sel}(K, W(\chi)) \longrightarrow \text{Sel}(D_\infty, W)(\chi)^\Gamma$$

$$\text{Sel}_\Sigma(K, W(\chi)) \longrightarrow \text{Sel}_\Sigma(D_\infty, W)(\chi)^\Gamma$$

*whose kernels and cokernels are finite, of cardinality bounded independently of $\chi$.***
Remark. Of course, the same statements hold when $W(\chi)$ is replaced by $W^*(\chi^{-1})$.

Proof. By the inflation-restriction sequence, the homomorphism

$$H^1(K, W(\chi)) \rightarrow H^1(D_\infty, W(\chi)^\Gamma)$$

is surjective with kernel bounded by the size of $W(\chi)(D_\infty)$. Since $D_\infty$ does not split $W$ (by Lemma 2.2.5) and $\chi$ is a character of $\text{Gal}(D_\infty/K)$, $W(\chi)(D_\infty)$ has finite order bounded independently of $\chi$.

We first show that the restriction map

$$\text{Sel}(K, W(\chi)) \rightarrow \text{Sel}(D_\infty, W(\chi)^\Gamma)$$

has finite cokernel, and then explain how to modify the argument to prove the same is true for the other maps of the proposition. Any element $c \in \text{Sel}(D_\infty, W)^\Gamma(\chi)$ is the restriction of some $d \in H^1(K, W(\chi))$, and any such $d$ satisfies $\text{res}\_v d \in H^1_f(D_{\infty,v}, W(\chi))$ for any prime $v$ of $D_\infty$. As $\text{Sel}(D_\infty, W(\chi)^\Gamma)$ is a cofinitely generated $\mathbb{Z}_p$-module, it therefore suffices to find a bound (uniform in $\chi$ and $v$) for the index of $H^1_f(K_v, W(\chi))$ in $\text{res}^{-1}(H^1_f(D_{\infty,v}, W(\chi)))$.

If $v \nmid p^*$, then $H^1_f(D_{\infty,v}, W(\chi)) = 0$, so we need to bound the size of $\text{ker}\_v\text{res} = H^1(D_{\infty,v}/K_v, W(\chi)(D_{\infty,v}))$. First note that we may assume $\text{Gal}(D_{\infty,v}/K_v) \cong \mathbb{Z}_p$, as otherwise this Galois group is trivial. We first consider those $v \nmid p$ at which $W(\chi)$ is unramified. For such $v$, either $W(\chi)(D_{\infty,v})$ or $W(\chi)(D_{\infty,v}) = W(\chi)$ (depending on whether $W(\chi)[\pi] \not\subseteq W(\chi)(K_v)$ or $W(\chi)[\pi] \subseteq W(\chi)(K_v)$, respectively, for a uniformizer $\pi$ of $\mathcal{O}$), since $K_v(W(\chi))$ must contain $D_{\infty,v}$, the maximal unramified abelian $p$-extension of $K_v$. In case $W(\chi)(D_{\infty,v}) = W(\chi)$, we have

$$H^1(D_{\infty,v}/K_v, W(\chi)(D_{\infty,v})) = W(\chi)/(\gamma - 1)W(\chi)$$

for a topological generator $\gamma$ of $\text{Gal}(D_{\infty,v}/K_v)$. This group is trivial, since $\gamma$ acts by a non-trivial scalar and $W(\chi)$ is divisible. Thus it remains to uniformly bound
ker $\rho$ for each of the finitely many primes $v$ of $D_\infty$ such that either $v \mid p$ or all of the following hold: $\text{Gal}(D_{\infty,v}/K_v) \cong \mathbb{Z}_p$, $W(\chi)$ is ramified, and $W(\chi)(D_{\infty,v})$ is finite. In either of these cases,

$$H^1(D_{\infty,v}/K_v, W(\chi)(D_{\infty,v})) = W(\chi)(D_{\infty,v})/(\gamma - 1)W(\chi)(D_{\infty,v}),$$

which is finite, bounded independently of $\chi$.

If $v \mid p^*$, then we consider the larger group $\text{Sel}^{(p^*)}(K, W(\chi)) \supseteq \text{Sel}(K, W(\chi))$ (defined in the same way as the usual Selmer group, save that we pose no condition locally at $p^*$). We claim that $\text{Sel}(K, W(\chi))$ has finite index in $\text{Sel}^{(p^*)}(K, W(\chi))$. From the definitions, we see that the quotient of these two groups injects into

$$H^1(K_{p^*}, W(\chi))/H^1(K_{p^*}, W(\chi))_{\text{div}},$$

which is finite, as $H^1(K_{p^*}, W(\chi))$ is a cofinitely generated $\mathcal{O}$-module. Thus we see that some finite multiple of $\text{loc}_{p^*} d$ lies in $H^1(K_{p^*}, W(\chi))$, as desired.

The restriction

$$\text{Sel}^{(p^*)}(K, W(\chi)) \longrightarrow \text{Sel}^\Sigma(D_\infty, W)(\chi)^\Gamma$$

likewise has finite cokernel: if $q = p$ or $p^*$, then we argue as above that

$$H^1(K_q, W(\chi))/H^1(K_q, W(\chi))_{\text{div}}$$

is finite, which gives what we want, since

$$H^1(K_q, W(\chi)) = H^1(K_q, W(\chi))_{\text{div}}.$$

The rest of the argument (i.e., for primes $v \nmid p$) is the same.

Similarly, to show that the map

$$\text{Sel}_\Sigma(K, W(\chi)) \longrightarrow \text{Sel}_\Sigma(D_\infty, W)(\chi)^\Gamma$$

50
has finite cokernel, it suffices (given the above) to note that the kernel

$$W(\chi)(D_{\infty,p^*})/(\gamma - 1)W(\chi)(D_{\infty,p^*})$$

of the restriction map over $p^*$ is finite. □

The essential content of the proofs of Propositions 2.4.1 and 2.4.2 is a formula of Wiles for the Selmer groups of finite Galois modules. The following lemma will allow us to relate our Selmer groups to the Selmer groups of the associated finite Galois modules.

**Lemma 2.4.4.** The natural maps

$$\text{Sel}(K, W(\chi)[p^k]) \longrightarrow \text{Sel}(K, W(\chi))[p^k]$$

$$\text{Sel}'(K, W(\chi)[p^k]) \longrightarrow \text{Sel}'(K, W(\chi))[p^k]$$

$$\text{Sel}_\Sigma(K, W(\chi)[p^k]) \longrightarrow \text{Sel}_\Sigma(K, W(\chi))[p^k]$$

are surjective with kernels of order bounded independently of $\chi$ and $k$. The same is true for $W^*(\chi^{-1})$.

**Remark.** We define the various Selmer groups associated to $W(\chi)[p^k]$ by the local conditions induced from those defining the Selmer groups associated to $W(\chi)$ (cf. §1.1 of Mazur-Rubin [9]).

**Proof.** The short exact sequence

$$0 \longrightarrow W(\chi)[p^k] \longrightarrow W(\chi) \overset{p^k}{\longrightarrow} W(\chi) \longrightarrow 0$$

gives rise to the exact sequence of cohomology groups

$$W(\chi)(K) \longrightarrow H^1(K, W(\chi)[p^k]) \longrightarrow H^1(K, W(\chi))[p^k] \longrightarrow 0.$$
proves the statement about the kernels. The surjectivity follows from the definition of the local conditions cutting out the Selmer groups associated to \(W(\chi)[p^k]\); cf. Lemma 3.5.3 of [9].

\[\square\]

**Proposition 2.4.5.** The difference between the orders of the torsion submodules of \(\text{Sel}(K, W(\chi))^\vee\) and \(\text{Sel}(K, W^*(\chi^{-1}))^\vee\) is bounded as \(\chi\) varies. The same is true of the torsion submodules of \(\text{Sel}'(K, W(\chi))^\vee\) and \(\text{Sel}_{\Sigma}(K, W^*(\chi^{-1}))^\vee\). Moreover, for any \(\chi\),

\[
\begin{align*}
\text{rk}_{\mathcal{O}'} \text{Sel}(K, W(\chi))^\vee &= \text{rk}_{\mathcal{O}'} \text{Sel}(K, W^*(\chi^{-1}))^\vee, \\
\text{rk}_{\mathcal{O}'} \text{Sel}'(K, W(\chi))^\vee &= 1 + \text{rk}_{\mathcal{O}'} \text{Sel}_{\Sigma}(K, W^*(\chi^{-1}))^\vee.
\end{align*}
\]

**Proof.** In view of Lemma 2.4.4, it suffices to show that

\[
\text{length}_{\mathcal{O}'} \text{Sel}(K, W(\chi)[p^k]) - \text{length}_{\mathcal{O}'} \text{Sel}(K, W^*(\chi^{-1})[p^k]) = c(k)
\]

and

\[
\text{length}_{\mathcal{O}'} \text{Sel}'(K, W(\chi)[p^k]) - \text{length}_{\mathcal{O}'} \text{Sel}_{\Sigma}(K, W^*(\chi^{-1})[p^k]) = v'(p)k + d(k),
\]

where \(v'(p)\) is the \(\mathcal{O}'\)-valuation of \(p\) and \(|c(k)|\) and \(|d(k)|\) are bounded independently of \(k\) and \(\chi\). From Wiles’s formula [9, Proposition 2.3.5], we get the formula

\[
\text{length}_{\mathcal{O}'} \text{Sel}(K, W(\chi)[p^k]) - \text{length}_{\mathcal{O}'} \text{Sel}(K, W^*(\chi^{-1})[p^k]) =
\]

\[
\begin{align*}
&\text{length}_{\mathcal{O}'} W(\chi)[p^k](K) - \text{length}_{\mathcal{O}'} W^*(\chi^{-1})[p^k](K) - \\
&\sum_{v|p^\infty} (\text{length}_{\mathcal{O}'} W(\chi)[p^k](K_v) - \text{length}_{\mathcal{O}'} H^1_f(K_v, W(\chi)[p^k]))
\end{align*}
\]

and a similar formula relating \(\text{Sel}'\) and \(\text{Sel}_{\Sigma}\). In the former case, this formula gives

\[
\text{length}_{\mathcal{O}'} \text{Sel}(K, W(\chi)[p^k]) - \text{length}_{\mathcal{O}'} \text{Sel}(K, W^*(\chi^{-1})[p^k]) =
\]

\[
c(k) + \text{length}_{\mathcal{O}'} H^1_f(K_p, W(\chi)[p^k]) - \text{length}_{\mathcal{O}'} W(\chi)[p^k](\mathbf{C}),
\]

\[52\]
whereas the latter case gives

\[
\text{length}_{\mathcal{O}'} \left( \text{Sel}'(K, W(\chi)[p^k]) \right) - \text{length}_{\mathcal{O}'} \left( \text{Sel}_\Sigma(K, W^*(\chi^{-1})[p^k]) \right) = \\
d(k) + \text{length}_{\mathcal{O}'} H^1_f(K_p, W(\chi)[p^k]) + \\
\text{length}_{\mathcal{O}'} H^1_f(K_p^*, W(\chi)[p^k]) - \text{length}_{\mathcal{O}'} W(\chi)[p^k](C)
\]

for functions \( c(k) \) and \( d(k) \) with the desired properties. The proposition follows. \( \square \)

We now prove Proposition 2.4.1; the proof of Proposition 2.4.2 is similar. For ease of notation, set \( X_{\mathcal{O}'} = X(D_{\infty}) \otimes_{\mathcal{O}} \mathcal{O}' \) and \( X_{\mathcal{O}'}^{*,r} = X^*(D_{\infty}) \otimes_{\mathcal{O}} \mathcal{O}' \). Let \( m \) be the maximal ideal of \( \mathcal{O}' \). By our choice of \( \mathcal{O}' \), we have pseudo-isomorphisms of modules over \( \Lambda_{\mathcal{O}'} = \Lambda(D_{\infty}) \otimes_{\mathcal{O}} \mathcal{O}' \)

\[
X_{\mathcal{O}'} \sim \bigoplus_{\zeta \in m} \bigoplus_{i=1}^{m(\zeta)} \Lambda_{\mathcal{O}'} / ((\gamma - 1) - \zeta)^{e(i, \zeta)} \oplus \Lambda^r_{\mathcal{O}'} \oplus (\mathcal{O}'-\text{torsion})
\]

\[
X_{\mathcal{O}'}^{*,r} \sim \bigoplus_{\zeta \in m} \bigoplus_{j=1}^{n(\zeta)} \Lambda_{\mathcal{O}'} / ((\gamma - 1) - \zeta)^{f(j, \zeta)} \oplus \Lambda^s_{\mathcal{O}'} \oplus (\mathcal{O}'-\text{torsion}),
\]

where \( \gamma \) is a topological generator of \( \text{Gal}(D_{\infty}/K) \); only finitely many summands are nonzero. Proposition 2.4.1 is the assertion that \( r = s \) and that

\[
(2.4.1) \quad \sum_{i=1}^{m(\zeta)} e(i, \zeta) = \sum_{j=1}^{n(\zeta)} f(j, \zeta)
\]

for all \( \zeta \in m \). Let \( A \subseteq m \) be the subset of all \( \zeta \) such that \( e(i, \zeta) = 0 \) for all \( 1 \leq i \leq m(\zeta) \) and \( f(i, \zeta) = 0 \) for all \( 1 \leq i \leq m(\zeta) \). For each \( \zeta \in A \) define a character \( \chi_\zeta : \text{Gal}(D_{\infty}/K) \to \mathcal{O}' \) by the rule \( \chi_\zeta(\gamma) = (1 + \zeta)^{-1} \).

To see that \( r = s \), note that

\[
X_{\mathcal{O}'} / ((\gamma - 1) - \zeta)X_{\mathcal{O}'} = \left( \text{Sel}(D_{\infty}, W)(\chi_\zeta)^r \right)^\vee
\]

53
for any $\zeta \in A$. In particular,

$$r = \text{rk}_{\varpi'}(\text{Sel}(D_\infty, W)(\chi_{\zeta}^\Gamma)^\vee).$$

Similarly,

$$s = \text{rk}_{\varpi'}(\text{Sel}(D_\infty, W^*)((\chi_{\zeta}^{-1})^\Gamma)^\vee).$$

Propositions 2.4.3 and 2.4.5 then imply that $r = s$.

We now prove (2.4.1). Let $\zeta \in \mathfrak{m}$ be such that one of $e(i, \zeta)$ or $f(j, \zeta)$ is nonzero (for some $i$ or $j$). Choose any sequence $\{\zeta_k\} \subseteq A$ converging to $\zeta$, and for each $k$ define $v(k)$ to be the valuation of $\zeta - \zeta_k$. Then

$$\text{length}_{\varpi'}(X_{\varpi'}/((\gamma - 1) - \zeta_k)X_{\varpi'})_{\text{tors}} = v(k) \sum_{i=1}^{m(\zeta)} e(i, \zeta) + c(k)$$

and

$$\text{length}_{\varpi'}(X_{\varpi'}^{*e}/((\gamma - 1) - \zeta_k)X_{\varpi'}^{*e})_{\text{tors}} = v(k) \sum_{j=1}^{n(\zeta)} f(j, \zeta) + d(k),$$

where $|c(k)|$ and $|d(k)|$ are bounded independently of $k$. Applying Propositions 2.4.3 and 2.4.5, we see that

$$\sum_{i=1}^{m(\zeta)} e(i, \zeta) + \frac{c'(k)}{v(k)} = \sum_{j=1}^{n(\zeta)} f(j, \zeta) + \frac{d'(k)}{v(k)},$$

where $|c'(k)|$ and $|d'(k)|$ are bounded independently of $k$. Proposition 2.4.1 follows by letting $k \to \infty$.

2.4.2. The $p$-adic height pairing. There is, quite generally, a $p$-adic height pairing on the Selmer groups associated to any suitably nice $p$-adic Galois representation of a number field. Following [1] and an article of Rubin [15], we prove a formula for how this height pairing behaves when evaluated on classes arising from the Euler system of twisted elliptic units constructed in 2.1.5. First we establish some notation.

Set $\Gamma = \text{Gal}(D_\infty/K)$ and $G = \text{Gal}(C_\infty/K)$. We choose an isomorphism $\lambda : G \cong \mathbb{Z}_p$ sending a chosen topological generator $\gamma$ of $G$ to $1 \in \mathbb{Z}_p$. Recall from 2.1.4 the
power series expansions (for a prime to $fp$)

$$
\mu(K_\infty, \eta^*, a) = L_{a,0} + L_{a,1}(\gamma - 1) + L_{a,2}(\gamma - 1)^2 + \cdots
$$

$$
\mu(K_\infty, \eta^*) = L_0 + L_1(\gamma - 1) + L_2(\gamma - 1)^2 + \cdots,
$$

where $L_{a,i}$ and $L_i$ are elements of $\tilde{\Lambda}(D_\infty)$ and $L_0 = \mu(D_\infty, \eta^*)$. Because we are assuming that $c = \frac{1}{2}w - 1$, $\psi = \bar{\psi} \circ \tau$ and the sign in the function equation of $\psi$ is $-1$, we see that

$$
L_0 = L_{a,0} = 0
$$

by Proposition 2.2.9. We write $D_\infty = \bigcup D_n$, where $[D_n : K] = p^n$ and set $F_n = D_nC_\infty$.

**Lemma 2.4.6.** For each $n$ there is a unique element $\beta_n \in H^1(F_{n,p}, T) \otimes \tilde{\Phi}$ satisfying

$$
(\gamma - 1)\beta_n = \text{loc}_p c_a(F_n).
$$

If $\alpha_n$ is the image of $\beta_n$ in $H^1(D_{n,p}, T) \otimes \tilde{\Phi}$, then the $\alpha_n$ are norm-compatible. The induced element $\alpha_\infty \in H^1(D_{\infty,p}, T) \otimes \tilde{\Phi}$ maps under the isomorphism of Proposition 2.2.6 to $L_{a,1}$.

**PROOF.** This is Lemma 3.1.1 of [1]. Given that $L_{a,0} = 0$, it follows directly from Proposition 2.2.6 and the definition of $L_{a,1}$. $\Box$

Recall that local Tate duality provides, for each finite extension $F$ of $K$, a pairing

$$
\langle \cdot, \cdot \rangle_{F_p} : H^1(F_p, T) \times H^1(F_p, T^*) \longrightarrow \mathcal{O}
$$

which becomes perfect after taking the quotient by the $\mathcal{O}$-torsion submodule on each side. For notational convenience, we set $\langle \cdot, \cdot \rangle_n = \langle \cdot, \cdot \rangle_{D_{n,p}}$.

**Theorem 2.4.7.** For each $n$, there is a $p$-adic height pairing

$$
h_n : \text{Sel}(D_n, T) \times \text{Sel}(D_n, T^*) \longrightarrow \Phi,
$$

canonically determined by $\lambda$ up to sign, satisfying
(1) (bounded image) there is an integer $k$, independent of $n$, such that the image of $h_n$ lies in $p^{-k}O$;

(2) (Galois-equivariance) for any $a \in \text{Sel}(D_n, T)$, $b \in \text{Sel}(D_n, T^*)$, and $\sigma \in \text{Gal}(D_n/K)$, we have

$$h_n(a^\sigma, b^\sigma) = h_n(a, b);$$

(3) (compatibility) for $a_n \in \text{Sel}(D_n, T)$ and $b_{n+1} \in \text{Sel}(D_{n+1}, T^*)$, we have

$$h_n(a_n, \text{cor}(b_{n+1})) = h_{n+1}(\text{res}(a_n), b_{n+1}),$$

where $\text{res}$ and $\text{cor}$ are the restriction, resp. corestriction, maps with respect to $D_{n+1}/D_n$;

(4) (height formula) if $b \in \text{Sel}(D_n, T^*)$, then (after extending scalars to $\widetilde{\Phi}$)

$$h_n(c_a(D_n), b) = (\alpha_n, \text{loc}_p b)_n.$$

This and the next subsection will be devoted to the proof of part (4) of this theorem (parts (1)–(3) are proved in [12, §1.2]). We first recall Perrin-Riou’s construction of the height pairing and give Rubin’s proof of the height formula in 2.4.3. Those readers not concerned with the proof are advised to proceed to 2.4.4. In what follows, we fix $n$ and let $L_k = C_k D_n$.

**Lemma 2.4.8.** Let $\nu$ be a place of $L_\infty$. Then the module of universal norms

$$H^1_I(D_{n,v}, T)\text{u} = \bigcap \text{cor } H^1_I(L_{k,v}, T)$$

has finite index in $H^1_I(D_{n,v}, T)$ which is bounded independently of $\nu$ and $n$.

**Proof.** If $\nu \mid p$, then the definitions show that $H^1_I(D_{n,v}, T)$ is the image under the connecting homomorphism of $W(D_{n,v})$. The size of $W(D_{n,v})$ is bounded independently of $n$ since $W$ generates an infinite unramified extension of $K_p$ and $D_{\infty,v}$ is a ramified $\mathbb{Z}_p$-extension of $K_p$. 

56
If \( v \mid p^* \), then we have \( H_1^1(L_{k,v}, T) = H_1^1(L_{k,v}, T) \), so it suffices by local duality to bound the kernel of the restriction map

\[
H^1(\mathcal{D}_{n,v}, W^*) \rightarrow H^1(\mathcal{L}_{\infty,v}, W^*).
\]

By the inflation-restriction sequence, this kernel is \( H^1(\mathcal{L}_{\infty,v}/\mathcal{D}_{n,v}, W^*(\mathcal{L}_{\infty,v})) \), which is isomorphic to \( W^*(\mathcal{L}_{\infty,v})/(\gamma - 1)W^*(\mathcal{L}_{\infty,v}) \), where \( \gamma \) is a topological generator of \( \text{Gal}(\mathcal{L}_{\infty,v}/\mathcal{D}_{n,v}) \). Using the exact sequence

\[
0 \rightarrow W^*(\mathcal{D}_{n,v}) \rightarrow W^*(\mathcal{L}_{\infty,v}) \xrightarrow{\gamma - 1} W^*(\mathcal{L}_{\infty,v}) \rightarrow \rightarrow W^*(\mathcal{L}_{\infty,v})/(\gamma - 1)W^*(\mathcal{L}_{\infty,v}) \rightarrow 0,
\]

we see that \( W^*(\mathcal{L}_{\infty,v})/(\gamma - 1)W^*(\mathcal{L}_{\infty,v}) \) has the same size as \( W^*(\mathcal{D}_{n,v}) \), which is bounded independent of \( n \), since, as above, \( \mathcal{D}_{n,v} \) is a ramified \( \mathbb{Z}_p \)-extension of \( \mathcal{K}_p \).

Finally, suppose \( v \nmid p \). The fact that \( V \) and \( V^* \) are not split locally at \( v \) (Lemma 2.2.5) together with Proposition 2.2.10 show that \( H^1(L_{k,v}, V) = 0 \), so we again have \( H_1^1(L_{k,v}, T) = H_1^1(L_{k,v}, T) \). As above, we therefore must bound the order of \( W^*(\mathcal{L}_{\infty,v})/(\gamma - 1)W^*(\mathcal{L}_{\infty,v}) \) independently of \( v \) and \( n \), where \( \gamma \) is a topological generator of \( \text{Gal}(\mathcal{L}_{\infty,v}/\mathcal{D}_{n,v}) \). Because \( v \nmid p \), \( \mathcal{L}_{\infty,v} \) is the unique unramified \( \mathbb{Z}_p \)-extension of \( \mathcal{K}_v \) and in particular does not change as \( n \) varies, so that any bound for the order of \( W^*(\mathcal{L}_{\infty,v})/(\gamma - 1)W^*(\mathcal{L}_{\infty,v}) \) will be independent of \( n \). If \( v \) is ramified for \( W^* \), then \( W^*(\mathcal{L}_{\infty,v}) \) is finite, and its order only depends on the prime of \( K \) over which \( v \) lies, of which there are finitely many. If \( K_v(W^*[\pi]) \neq K_v \) where \( \pi \) is a uniformizer of \( \mathcal{O} \), then clearly \( W^*(\mathcal{L}_{\infty,v}) = 0 \), since \( [K_v(W^*[\pi]) : K_v] \) is prime to \( p \). Thus we may assume that \( v \) is unramified for \( W^* \) and that \( K(W^*[\pi]) = K \). But in this case, we have \( W^*(\mathcal{L}_{\infty,v}) = W^* \), since \( W^* \) generates an unramified abelian \( p \)-extension of \( K_v \). Thus, \( W^*/(\gamma - 1)W^* = 0 \) since \( \gamma \) acts nontrivially on \( W^* \), which is divisible. 

\( \square \)
The importance of the previous lemma is that it suffices to define $h_n(a, b)$ for $a \in \text{Sel}(D_n, T)$ and $b \in \text{Sel}(D_n, T^*)$ which are everywhere locally contained in $H^1_f(D_{n,v}, T)^u$, resp. $H^1_f(D_{n,v}, T^*)^u$. In what follows, we fix such $a$ and $b$.

We may view $b$ as an element of $H^1(D_n, T^*)$, which corresponds to an extension of $G_{D_n}$-modules

$$0 \longrightarrow T^* \longrightarrow M_b^* \longrightarrow \mathcal{O} \longrightarrow 0. $$

Taking the Tate dual gives the sequence

(2.4.2) $0 \longrightarrow \mathcal{O}(1) \longrightarrow M_b \longrightarrow T \longrightarrow 0.$

For any finite extension $L$ of $D_n$ and any place $v$ of $L$, we have a commutative diagram with exact rows

$$
\begin{array}{cccccc}
H^1(L, \mathcal{O}(1)) & \longrightarrow & H^1(L, M_b) & \longrightarrow & H^1(L, T) & \longrightarrow & H^2(L, \mathcal{O}(1)) \\
\downarrow & & \downarrow \pi_L & & \downarrow \delta_L & & \downarrow \\
H^1(L_v, \mathcal{O}(1)) & \longrightarrow & H^1(L_v, M_b) & \longrightarrow & H^1(L_v, T) & \longrightarrow & H^2(L_v, \mathcal{O}(1)) \\
\end{array}
$$

(2.4.3)

Lemma 2.4.9. If $L$ is a finite Galois extension of $D_n$ and $a' \in H^1(L, T)$ satisfies $\text{cor}(a') = a$, then $a'$ is in the image of $\pi_L$.

PROOF. The connecting homomorphism $\delta_L$ is given up to sign by applying $\cup \text{res}(b)$, where res is restriction from $D_n$ to $L$. For any place $v$ of $L$, we have

$$\text{loc}_v \delta_L(a') = \text{loc}_v (a' \cup \text{res}(b)) = \text{loc}_v (a \cup b) = 0,$$

since $a$ and $b$ are orthogonal everywhere under the local Tate pairing. This shows that $\delta_L(a')$ is trivial locally everywhere, hence trivial. \qed

Lemma 2.4.10. If $v$ is any place of $L$, then $H^1_f(L_v, T)$ is contained in the image of $\pi_{L_v}$.

PROOF. As in Lemma 2.4.9, $\delta_{L_v}$ is given by $\cup \text{loc}_v \text{res}(b)$, but $\text{loc}_v \text{res}(b)$ lies in $H^1_f(L_v, T^*)$, which is orthogonal to $H^1_f(L_v, T)$. \qed
By class field theory, the map $\text{Gal}(L_{\infty}/D_n) \rightarrow \mathbb{Z}_p \hookrightarrow \mathcal{O}$ gives rise to a map $\rho_v : D_{n,v}^* \otimes \mathcal{O} \rightarrow \mathcal{O}$ for every place $v$ of $D_n$. Kummer theory then allows us to view $\rho_v$ as a homomorphism

$$\rho_v : H^1(D_{n,v}, \mathcal{O}(1)) \rightarrow \mathcal{O}.$$ 

This map can also be described up to sign as

$$(2.4.4) \quad \cup \text{loc}_v \lambda : H^1(D_{n,v}, \mathcal{O}(1)) \rightarrow H^2(D_{n,v}, \mathcal{O}(1)) \cong \mathcal{O},$$

where we view $\lambda$ as an element of $H^1(D_n, \mathcal{O})$.

Setting $L = D_n$ and $a' = a$ in Lemma 2.4.9 allows us to choose a sequence of elements $x_k \in H^1(D_n, M_b)$ such that $\pi_{D_n}(x_k) = a$. Since we are assuming that $a$ is a universal norm locally everywhere, we may choose, for all places $v$ of $K_{\infty}$ and positive integers $k$, elements $y_{k,v} \in H^1_t(L_{k,v}, T)$ satisfying $\text{cor} y_{k,v} = \text{loc}_v a$. Lemma 2.4.10 then gives the existence of $x_{k,v} \in H^1(L_{k,v}, M_b)$ such that $\pi_{L_{k,v}}(x_{k,v}) = y_{k,v}$. From (2.4.3), the difference $\text{loc}_v x_k - \text{cor} x_{k,v}$ is the image of some $w_{k,v} \in H^1(D_{n,v}, \mathcal{O}(1))$, and we define the $p$-adic height pairing as

$$(2.4.5) \quad h_n(a, b) = \lim_k \sum_v \rho_v(w_{k,v}).$$

It can be checked that this definition makes sense and is independent of the choices made (see 1.2.4 of Perrin-Riou’s article [12]).

2.4.3. The height formula. What follows is Rubin’s proof of the height formula, Theorem 2.4.7(4), as given in [15]. We have included a fairly complete proof, as it might not be immediately clear why the proof in [15] works in our more general setting. In the notation of the previous subsection, we will be considering $a = c_a(D_n)$ (where $c_a$ is the Euler system of 2.1.2) and computing its pairing against an arbitrary $b \in \text{Sel}(D_n, T^*)$ which is a universal norm locally everywhere. The formula for $h_n(a, b)$ can be given a particularly simple form:
Proposition 2.4.11. For suitable choices of $x_k$, $x_{k,v}$, and $y_{k,v}$, the height pairing on $a = c_a(D_n)$ can be computed as

$$h_n(a, b) = \lim_k \left( \rho_p(w_{k,p}) + \rho_{p^*}(w_{k,p^*}) \right).$$

Proof. Let $a^{(k)} = c_a(L_k)$, so that $\text{cor } a^{(k)} = a$. As above, Lemma 2.4.9 provides us with $x^{(k)} \in H^1(L_k, M_b)$ mapping to $a^{(k)}$ under $\pi_{L_k}$. We define the sequence $x_k$ by $x_k = \text{cor } x^{(k)}$.

If $v \mid p$, then choose $\xi_{k,v} \in H^1(L_{k,v}, M_b)$ satisfying $\pi_{L_{k,v}}(\xi_{k,v}) = \text{loc}_v a_k - y_{k,v}$, where $y_{k,v} \in H^1_v(L_{k,v}, T)$ as before satisfies $\text{cor } y_{k,v} = \text{loc}_v a$. We then define $x_{k,v} = \text{loc}_v x^{(k)} - \xi_{k,v}$, so $\pi_{L_{k,v}}(x_{k,v}) = y_{k,v} \in H^1_v(L_{k,v}, T)$ by the commutativity of (2.4.3). With this definition of $x_{k,v}$, the image of $w_{k,q}$ in $H^1(D_{n,q}, M_b)$ is equal to $\text{cor } \xi_{k,q}$ ($q = p$ or $p^*$).

If $v \nmid p$, we take

$$x_{k,v} = \sum_{\sigma \in B} \text{loc}_v(x^{(k)})^\sigma,$$

where $B$ is a set of coset representatives for $\text{Gal}(L_k/D_n)/D_v$ and $D_v$ is a decomposition group at $v$. Then $\pi_{L_{k,v}}(x_{k,v}) \in H^1_v(L_{k,v}, T)$ because $H^1_v(L_{k,v}, T) = H^1(L_k, T)$ and $\text{cor } \pi_{L_{k,v}}(x_{k,v}) = \pi_{L_k}(\text{loc}_v x_k) = \text{loc}_v a$, so this choice of $x_{k,v}$ satisfies the requisite properties.

The stated formula for the height pairing now follows from the definition and the fact that for $v \nmid p$, we have $\text{cor } x_{k,v} = \text{loc}_v x_k$, so these terms do not contribute to the sum (2.4.5) defining $h_n(a, b)$. \hfill \Box

For $q = p$ or $p^*$, define the module $H_{k,q}$ as the kernel of the corestriction map

$$H^1(L_{k,q}, T) \xrightarrow{\text{cor}} H^1(D_{n,q}, T).$$

Note in particular that, by definition, $\pi_{L_{k,q}}(\xi_{k,q}) \in H_{k,q}$.

In §4 of Rubin’s article [15], one finds the definition of a “derivative” mapping

$$\text{Der}_{k,q} : H_{k,q} \longrightarrow H^1(D_{n,q}, T/p^k T).$$
(See also the introductory remarks of §5 of [15].) In Rubin’s notation, this is the map \( \sum_{v \mid q} \mathrm{Der}_{L_{k,v} / D_{n,v}, \psi_{k,v}} \), where \( \psi_{k,v} : \text{Gal}(L_{k,v} / D_{n,v}) \to \mathcal{O} / p^k \mathcal{O} \) is induced by \( \lambda \). We now describe several properties that the derivative map enjoys. Let

\[
\text{inv}_q : H^2(D_{n,q}, (\mathcal{O} / p^k \mathcal{O})(1)) \to \mathcal{O} / p^k \mathcal{O}
\]

be the sum of the local invariant maps for \( v \mid q \).

**Proposition 2.4.12.** With the choices made above, there is an equivalence up to sign

\[
\rho_q(w_{k,q}) \equiv \text{inv}_q(\mathrm{Der}_{k,q}(\pi_{L_{k,q}}(\xi_{k,q})) \cup \text{loc}_q b) \quad (\text{mod } p^k).
\]

**Proof.** Proposition 4.3 of [15] gives the formula

\[
(\text{loc}_q \lambda) \cup w_{k,q} = \delta_{D_{n,q}}(\mathrm{Der}_{k,q}(\pi_{L_{k,q}}(\xi_{k,q}))),
\]

where in the notation of that proposition we have \( w_{k,q} = \text{cor}_{K/k}(c) \) and \( \pi_{L_{k,q}}(\xi_{k,q}) = d \). Applying \( \text{inv}_q \) to both sides of this formula gives the result in light of our description (2.4.4) for \( \rho_q \). \( \square \)

**Corollary 2.4.13.** The height pairing on \( a = c_a(D_n) \) can be computed as

\[
h_n(a, b) = \lim_k \rho_p(w_{k,p}).
\]

**Proof.** By definition of the Selmer group \( \text{Sel}(D_n, T^*) \), \( \text{loc}_{p^*} b \) lies in the torsion subgroup \( H^1(D_n, T^*)_{\text{tors}} \), say \( p^m \text{loc}_{p^*} b = 0 \). The proposition implies that \( \rho_{p^*}(w_{k,p^*}) \equiv 0 \ (\text{mod } p^{k-m}) \) for all \( k \), so \( \lim_k \rho_{p^*}(w_{k,p^*}) = 0 \). \( \square \)

**Lemma 2.4.14.** If \( d_k \in H_{k,p} \) is a sequence satisfying \( d_k \cup z = (\text{loc}_p a_k) \cup z \) for all \( k \) and all \( z \in H^1(L_{k,p}, T^*) \) and \( e_k \in H^1_{n}(L_{k,p}, T^*) \) is a sequence satisfying \( \text{cor} e_k = e_0 \in H^1(D_{n,p}, T^*) \) for all \( k \), then

\[
\lim_k \text{inv}_p(\mathrm{Der}_{k,p}(d_k) \cup e_0) = \lim_{\sigma \in \Gamma / p^k \Gamma} \sum_{\sigma} \lambda(\sigma)(\text{loc}_p a_k, \sigma e_k)_{L_{k,p}}.
\]

61

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
PROOF. It suffices to show that

$$\text{inv}_p(\text{Der}_{k,p}(d_k) \cup e_0) \equiv \lim_k \sum_{\sigma \in \Gamma/p^k\Gamma} \lambda(\sigma)\langle \text{loc}_p a_k, \sigma e_k \rangle_{L_{k,p}} \pmod{p^k}.$$ 

Lemma 4.2 of [15] asserts the commutativity of the diagram

$$\begin{array}{ccc}
H_{k,p} & \longrightarrow & H^1(L_{k,p}, T) \\
\text{Der}_{k,p} \downarrow & & \downarrow \sum_{\sigma \in \Gamma/p^k\Gamma} \lambda(\sigma)\sigma^{-1} \\
H^1(D_{n,p}, T/p^kT) & \longrightarrow & H^1(L_{k,p}, T/p^kT) \\
\text{res} & & \\
\end{array}$$

so in particular $\text{res Der}_{k,p} d_k = \sum \lambda(\sigma)\sigma^{-1} d_k$. Applying first $\cup e_k$ and then $\text{inv}_p$ to this equation gives the lemma. \qed

We can now prove the height formula, Theorem 2.4.7(4). In the above lemma, take $d_k = \pi_{L_{k,p}}(\xi_{k,p})$ and let $e_k \in H^1_{\Gamma}(L_{k,p}, T^*)$ be such that $\text{cor } e_k = \text{loc}_p b$. Recall the definition of $\beta_n \in H^1(L_{\infty,p}, T)$ from Lemma 2.4.6. We denote by $\beta_n^{(k)}$ the image of $\beta_n$ in $H^1(L_{k,p}, T)$. In particular, $\beta_n^{(0)} = \alpha_n \in H^1(D_{n,p}, T)$. We have

$$h_n(a, b) = \lim_k \rho_p(w_{k,p})$$

by Cor. 2.4.13

$$= \lim_k \sum_{\sigma \in \Gamma/p^k\Gamma} \lambda(\sigma)\langle \text{loc}_p a_k, \sigma e_k \rangle_{L_{k,p}}$$

by Prop. 2.4.12 and Lemma 2.4.14

$$= \lim_k \sum_{i=0}^{p^k-1} \langle (\gamma - 1)\beta_n^{(k)}, i\gamma^i e_k \rangle_{L_{k,p}}$$

by Lemma 2.4.6

$$= \lim_k \langle \beta_n^{(k)}, \text{res loc}_p b \rangle_{L_{k,p}}$$

since $\lim_k \langle \beta_n^{(k)}, -p^k\gamma^i - e_k \rangle = 0$

$$= \langle \alpha_n, \text{loc}_p b \rangle_n,$$

which is exactly Theorem 2.4.7(4).

2.4.4. The characteristic ideal. We now have at our disposal the $p$-adic height pairing of Theorem 2.4.7. The properties of the pairing together with the duality
results of 2.4.1 render the proof of Theorem 2.2.2 for the most part formal. First, however, we must define an Iwasawa-theoretic version of the pairing.

Following [1], we define an Iwasawa-theoretic Tate pairing

\[(2.4.6) \quad \langle , \rangle_\infty : (H^1(D_{\infty,p}, T) \otimes \bar{\Phi}) \otimes \bar{\Lambda}(D_\infty) \to H^1(D_{\infty,p}, T^*)^c \otimes \bar{\Phi}) \to \bar{\Lambda}(D_\infty)\]

by setting

\[\langle a_\infty, b_\infty \rangle_\infty = \lim_{\sigma \in \text{Gal}(D_\infty/K)} \sum_{a_n, b_n} \langle a_n^\sigma, b_n \rangle_n \sigma^{-1}.\]

This pairing is in fact an isomorphism. We similarly define the Iwasawa-theoretic $p$-adic height pairing

\[h_\infty : (\text{Sel}(D_\infty, T) \otimes \bar{\Phi}) \otimes \bar{\Lambda}(D_\infty) \to \text{Sel}(D_\infty, T^*)^c \otimes \bar{\Phi}) \to \bar{\Lambda}(D_\infty)\]

by setting

\[h_\infty(a_\infty, b_\infty) = \lim_{\sigma \in \text{Gal}(D_\infty/K)} \sum_{a_n, b_n} h_\infty(a_n^\sigma, b_n) \sigma^{-1}.\]

**Lemma 2.4.15.** The element $\alpha_\infty \in H^1(D_{\infty,p}, T) \otimes \bar{\Phi}$ of Lemma 2.4.6 satisfies the equation

\[h_\infty(c_a(D_\infty), b_\infty) = \langle \alpha_\infty, \text{loc}_p \ b_\infty \rangle_\infty\]

for every element $b_\infty \in \text{Sel}(D_\infty, T^*)$.

**Proof.** This follows from the definitions of the Iwasawa-theoretic pairings and the height formula, Theorem 2.4.7(4). □

Let $R$ be the characteristic ideal of the cokernel of $h_\infty$. Recall that, under our assumptions, the image of $c_a(D_\infty)$ in $H^1(D_{\infty,p}, T)$ is trivial (Proposition 2.2.9), so the exact sequence (2.2.5) of Lemma 2.2.11 shows that $c_a(D_\infty) \in \text{Sel}(D_\infty, T)$; thus it makes sense to define $R_a$ as the characteristic ideal of the cokernel of

\[h_\infty|_{C_a(D_\infty)} : C_a(D_\infty) \otimes \bar{\Lambda}(D_\infty) \to \text{Sel}(D_\infty, T^*)^c \to \bar{\Lambda}(D_\infty).\]
We additionally define the ideal \( H \subseteq \Lambda(D_\infty) \) by
\[
H = \text{char}(\mathbb{H}^1(D_{\infty,p}, T^*)/\text{loc}_p \text{Sel}(D_\infty, T^*)).
\]

Note that \( H \neq 0 \), since \( \text{loc}_p \) is nontrivial (Proposition 2.2.9 applied to \( T^* \)).

**Lemma 2.4.16.** As ideals of \( \tilde{\Lambda}(D_\infty) \otimes \tilde{\Phi} \),
\[
R_a = R \cdot \text{char} \text{Sel}(D_\infty, T)/C_a(D_\infty) = (L_{a,1})^{H^*}.
\]

**Proof.** The first equality is clear from the definitions. We show that the first term is the same as the last. The height formula, Theorem 2.4.7(4), shows that
\[
\text{Im}(h_\infty|C_a(D_\infty)) = \langle \alpha_\infty, \text{loc}_p (\text{Sel}(D_\infty, T^*) \otimes \tilde{\Phi})^* \rangle_\infty.
\]
The result then follows from the fact that the Tate pairing (2.4.6) is an isomorphism and the property of \( \alpha_\infty \) described in Lemma 2.4.6. \( \square \)

The following, together with Theorem 2.3.9, completes the proof of Theorem 2.2.2.

**Theorem 2.4.17.** There is an equality of ideals in \( \tilde{\Lambda}(D_\infty) \otimes \tilde{\Phi} \)
\[
(\text{char } X^*(D_\infty)_{\text{tors}}) \cdot R = (L_1).
\]

**Proof.** Interchanging \( T \) and \( T^* \), \( p \) and \( p^* \), in the exact sequence (2.2.6) of Lemma 2.2.11 yields the short exact sequence
\[
0 \rightarrow \mathbb{H}^1(D_{\infty,p}, T^*)/\text{loc}_p \text{Sel}(D_\infty, T^*) \rightarrow X^\Sigma(D_\infty) \rightarrow X(D_\infty) \rightarrow 0.
\]
The leftmost term in this sequence is torsion of characteristic ideal \( H \), so that we get the equality
\[
H \text{ char } X(D_\infty)_{\text{tors}} = \text{char } X^\Sigma(D_\infty)_{\text{tors}}.
\]
Thus, Propositions 2.4.1 and 2.4.2 give
\[
H^* \text{ char } X^*(D_\infty)_{\text{tors}} = \text{char } X^*_\Sigma(D_\infty),
\]

64
but char $X^*_\Sigma(D_\infty) = \text{char}(\text{Sel}(D_\infty, T)/C(D_\infty))$ (this is part of Theorem 2.3.9), so the theorem now follows from Lemma 2.4.16 by letting $a$ vary. $\square$
CHAPTER 3

Hida families

In this chapter, we give a sketch of how the techniques used in Chap. 2 might be generalized so as to apply to arbitrary modular forms, not just those with CM. Our goal is to give a statement of the main conjecture of Iwasawa theory for Hida families associated to ordinary modular forms and to give a rough sketch of how a proof of these conjectures might proceed. We show how such statements are related to generalizations of the conjecture of Birch and Swinnerton-Dyer; namely, if the $L$-function of a $p$-ordinary modular form has odd order of vanishing at its central point, then the Pontryagin dual of the associated $p$-Selmer group (over $Q$) has positive rank.

Warning. The naming conventions for the statements in the chapter are as follows: statements labeled “Theorem”, “Proposition”, “Lemma”, and “Corollary” are conjectures which we believe can be proved by known methods. The statements labeled “Conjecture” are those which we believe to be true but know of no method of proof.

3.1. Background

In this section, we give definitions and notation, as well as statements of results by Skinner-Urban and Ochiai and related conjectures which we will need to apply our method. In 3.1.6 we give the statement of the main theorem. We denote by $\bar{Q}$ analgebraic closure of $Q$ in $C$ and choose isomorphisms $C \cong C_p$ for every prime $p$ (note that this determines embeddings $\bar{Q} \hookrightarrow \bar{Q}_p$). In order to maintain consistency with the papers of Ochiai ([10], [11]), we denote by Froby a geometric Frobenius and normalize our Galois representations accordingly. We denote by $\omega : G_\mathbb{Q} \to \mathbb{Z}_p^\times$ the
Teichmüller character giving the action of $G_\mathcal{Q}$ on the $p$th roots of unity. Finally, if $R$ is a ring and $M$ is an $R$-module, then for any prime $p \subseteq R$, we denote by $\text{length}_{R_p} M$ (or simply $\text{length}_p M$ if the ring $R$ is clear from the context) the length of the $R_p$-module $M_p$.

3.1.1. Modular forms and Galois representations. Choose an integer $N$, a prime $p > 2$ not dividing $N$, and a finite extension $F$ of $\mathbb{Q}_p$. Let $f \in S_k(N; \mathcal{O}_F)$ be a normalized cuspidal newform on $\Gamma_0(N)$ of even weight $k \geq 2$ with Fourier coefficients in $\mathcal{O}_F$. We assume moreover that $f$ is $p$-ordinary in the sense that the $p$th Fourier coefficient $a_p(f)$ of $f$ is a unit in $\mathcal{O}_F$. By work of Deligne [4], to any such $f$ is associated a continuous Galois representation $\rho_f : G_\mathcal{Q} \to \text{GL}_2(\mathcal{O}_F)$ unramified outside $Np$ which satisfies

$$\text{trace} \rho_f(\text{Frob}_\ell) = a_\ell(f), \quad \det \rho_f(\text{Frob}_\ell) = \ell^{k-1}.$$ 

Hida [7] has shown that every modular form $f$ as above can be put into an ordinary $p$-adic family $\mathcal{F}$ of modular forms of Nebentypus $\psi_\mathcal{F} = \omega^{k-2}$, in a sense which we now describe. The form $\mathcal{F}$ can be considered as a formal $q$-expansion $\mathcal{F} = \sum_{n=1}^{\infty} a_n(\mathcal{F}) q^n$ whose coefficients belong to a local domain $\mathcal{H} = \mathcal{H}_F$ finite and flat over $\mathbb{Z}_p[\Gamma_D]$, where $\Gamma_D$ is the group of diamond operators acting on the tower of modular curves $\{Y_1(p^n)\}$. Denote by

$$\chi_D : \Gamma_D \xrightarrow{\cong} 1 + p\mathbb{Z}_p$$

the canonical character. We say that a character $\kappa \in \text{Hom}_{\mathbb{Z}_p}(\mathcal{H}, \mathbb{C}_p)$ is arithmetic if the character

$$\psi_\kappa = \kappa|_{\Gamma_D} \cdot \chi_D^{-w(\kappa)} : \Gamma_D \rightarrow \mathbb{C}_p^\times$$

has finite order for some (uniquely determined) integer $w(\kappa)$, called the weight of $\kappa$. Let $\Gamma_C = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, where $\mathbb{Q}_\infty$ is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and denote by

$$\chi_C : \Gamma_C \xrightarrow{\cong} 1 + p\mathbb{Z}_p$$

67

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
the character $\omega^{-1} \chi_{cyc}$, where $\chi_{cyc}$ is the cyclotomic character. Abusing notation, we consider $\psi_\kappa$ as a character of $\Gamma_C$ by precomposing with the inverse of $\chi_D : \Gamma_D \to 1 + p\mathbb{Z}_p$ and with $\chi_C : \Gamma_C \to 1 + p\mathbb{Z}_p$. Define $p^{r(\kappa)}$ to be the conductor of $\psi_\kappa$. Such a character $\kappa$ is, of course, determined by its kernel $p_\kappa \in \text{Spec} H$. Given an arithmetic character $\kappa$ of weight $w(\kappa) \geq 0$, the specialization $f_\kappa$ of $\mathcal{F}$ at $\kappa$ is a $p$-stabilized eigenform of level $Np^{r(\kappa)}$ and Nebentypus character $\psi_\kappa \rho_\kappa \omega^{-w(\kappa)}$. That the form $f$ belongs to $\mathcal{F}$ means that the $p$-stabilized eigenform $f_p$ associated to $f$ is the specialization of $\mathcal{F}$ at an arithmetic character $\kappa$ of weight $k - 2$.

Let $K = \text{Frac} H$. To $\mathcal{F}$ is associated a continuous (in the sense of Hida) Galois representation $\rho_\mathcal{F} : G_H \to \text{GL}_2(K)$ which is unramified outside of $Np$ and has

$$\text{trace} \rho_\mathcal{F}(\text{Frob}_\ell) = a_\ell(\mathcal{F}), \quad \det \rho_\mathcal{F}(\text{Frob}_\ell) = \psi_\mathcal{F}(\ell) \langle \ell \rangle \ell,$$

where $\langle \ell \rangle$ is the image of $\ell \in \mathbb{Z}_p^\times$ under the composition $\mathbb{Z}_p^\times \to 1 + p\mathbb{Z}_p \overset{\cong}{\leftarrow} \Gamma_D \overset{\cong}{\rightarrow} K^\times$, the second arrow being given by $\chi_D$. In particular, there is a $G_H$-stable lattice $L \subseteq K^2$, i.e., a finitely generated torsion-free $H$-submodule of $K^2$ of generic rank $2$. The specialization of $\rho_\mathcal{F}$ at an arithmetic character $\kappa$ (by which we mean the $G_H$-module $L/p_\kappa L$) is isomorphic to $\rho_{f_\kappa}$ after extending scalars to $\overline{Q}_p$. In what follows, we will need to assume that the $G_H$-stable lattice $L$ can be chosen to be free of rank $2$ over $H$. This will be the case, e.g., if the residual representation of $\rho_f$ is irreducible; see [11, Proposition 2.10] for a few more cases where this is known to happen. We may thus consider $\rho_\mathcal{F}$ as a representation into $\text{GL}_2(H)$.

3.1.2. More rings and modules. We can extend the above setup as follows. A character $\lambda : \Gamma_C \to \overline{Q}_p$ is said to be arithmetic if $\lambda \cdot \chi_{cyc}^{-w(\lambda)}$ has finite order for some (uniquely determined) integer $w(\lambda)$, the weight of $\lambda$. Define the nearly-ordinary Hecke algebra associated to $\mathcal{F}$ to be the ring

$$H^{no} = H \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Gamma_C] = H[\Gamma_C],$$

68

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
which is a local domain finite and flat over $\mathbb{Z}_p[\Gamma_C \times \Gamma_D]$. This ring plays the role of a 2-variable Iwasawa algebra. We define an arithmetic specialization of $H^{\text{no}}$ to be a pair $(\lambda, \kappa)$ where $\lambda$ is an arithmetic character of $\Gamma_C$ and $\kappa$ is an arithmetic character of $H$. Any arithmetic specialization determines a homomorphism $(\lambda, \kappa) : H^{\text{no}} \to \overline{\mathbb{Q}}_p$ with kernel $p_{(\lambda, \kappa)}$; $(\lambda, \kappa)$ is the unique homomorphism which is equal to $\kappa$ when restricted to $H$ and which takes the value $\lambda(\gamma)$ when evaluated at an element $\gamma \in \Gamma_C$. For ease of notation, we set $(j, \kappa) = (\chi_C^j, \kappa)$. Given a $H^{\text{no}}$-module $M$ and any pair $(\lambda, \kappa)$ of continuous characters (of $\Gamma_C$ and $H$, respectively), we define the specialization of $M$ at $(\lambda, \kappa)$ to be the $H^{\text{no}}/p_{(\lambda, \kappa)}$-module $M_{(\lambda, \kappa)} = M/p_{(\lambda, \kappa)}M$.

There is again a Galois representation $\rho_f^{\text{no}} : G_Q \to \text{GL}_2(H^{\text{no}})$ obtained by the formula

$$\rho_f^{\text{no}} = \rho_f \otimes \chi^{\text{univ}},$$

where $\chi^{\text{univ}}$ is the universal character $\chi^{\text{univ}} : \Gamma_C \to \mathbb{Z}_p[\Gamma_C]^\times$ given by $\chi^{\text{univ}}(\gamma) = \gamma$. Let us denote by $T$ the representation space of $\rho_f^{\text{no}}$. The specialization of $\rho_f^{\text{no}}$ at any arithmetic point $(\lambda, \kappa)$ is isomorphic to $\rho_{f, \kappa} \otimes \lambda$ after extending scalars to $\overline{\mathbb{Q}}_p$.

Wiles [20] has shown that there is a filtration $T \supseteq F^+T \supseteq 0$ of $T$ by $H^{\text{no}}[G_{Q_p}]$-submodules such that $F^+T$ and $F^-T = T/F^+T$ are free $H^{\text{no}}$-modules of rank 1. The action of $G_{Q_p}$ on $F^+T$ is via the character $\alpha \otimes \chi^{\text{univ}}$, where $\alpha : G_{Q_p} \to H^\times$ is an unramified character such that $\kappa(\alpha(\text{Frob}_p)) = a_p(f_\kappa)$ for every arithmetic character $\kappa$ of weight $w(\kappa) \geq 0$.

We now discuss the quotient of $H^{\text{no}}$ which will play the role of the anticyclotomic Iwasawa algebra. Set

$$I = (\gamma_C^2 - \gamma_D \cdot (p + 1)^2) \subseteq \mathbb{Z}_p[\Gamma_C \times \Gamma_D],$$

where $\gamma_C$, resp. $\gamma_D$, is the element of $\Gamma_C$, resp. $\Gamma_D$, mapping to $p + 1$ under $\chi_C$, resp. $\chi_D$. For any $\mathbb{Z}_p[\Gamma_C \times \Gamma_D]$-module $M$, we set $M_I = M/IM$. The ring which will play the role of an anticyclotomic Iwasawa algebra is $H^{\text{no}}_I$, which is a finite flat $H$-algebra of generic rank 2. We will explain the relevance of the ring $H^{\text{no}}_I$ in 3.1.4.
A torsion $H^\text{tor}_\ell$- or $H^\text{tor}_i$-module $M$ is said to be \textit{pseudo-null} if it is supported in codimension 2 or greater (note that a pseudo-null $H^\text{tor}_i$-module contains only finitely many elements). A homomorphism $M \to N$ is said to be a \textit{pseudo-isomorphism} if its kernel and cokernel are pseudo-null.

For any $\mathbb{Z}_p$-module $M$, we denote by $M^\vee = \text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ its Pontryagin dual. Let $D$ be the trivial discrete Galois module $(H^\text{tor})^\vee$. We define $W = T \otimes_{H}^\text{tor} D$ to be the discrete module associated to $T$, $T^* = \text{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1))$ to be the Tate dual of $T$, and $W^* = T^* \otimes_{H}^\text{tor} D$. The filtration on $T$ induces in an obvious way a filtration on $W$, the positive part of which we denote by $F^+ W$. There is also an induced filtration on $T^*$ given by $F^+(T^*) = (F^+ T)^* = \text{Hom}_{\mathbb{Z}_p}(F^+ T, \mathbb{Z}_p(1))$, which in turn induces a filtration on $W^*$. Note that we have $(T^*_\lambda)(\lambda, \kappa) = (T_{(\lambda, \kappa)}^*)^*$ for any arithmetic specialization $(\lambda, \kappa)$. We set $V_{(\lambda, \kappa)} = T_{(\lambda, \kappa)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $V^*_{(\lambda, \kappa)} = T^*_{(\lambda, \kappa)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. All these modules have filtrations induced from the filtrations on $T$ and $T^*$.

\textbf{3.1.3. Selmer groups.} We now introduce local conditions and Selmer groups for the Galois representations defined above. Let $K$ be a number field and let $\Sigma_K$ (or simply $\Sigma$ if the field $K$ is clear from the context) be the set of places of $K$ dividing $p$.

Bloch-Kato [2] have defined conditions in the local cohomology groups of the finite $\mathbb{Q}_p$-vector spaces $V_{(\lambda, \kappa)}$ and $V^*_{(\lambda, \kappa)}$ as follows:

\[
H^1_f(K_v, V_{(\lambda, \kappa)}) = \begin{cases} 
H^1_{ur}(K_v, V_{(\lambda, \kappa)}) & v \nmid p \\
\ker(H^1(K_v, V_{(\lambda, \kappa)}) \to H^1(K_v, V_{(\lambda, \kappa)} \otimes \mathbb{Q}_p \otimes \mathbb{B}_{\text{crys}})) & v | p
\end{cases}
\]

and similarly for $V^*_{(\lambda, \kappa)}$, where $B_{\text{crys}}$ is Fontaine’s ring of crystalline periods. We then define the conditions $H^1_f(K_v, T_{(\lambda, \kappa)})$, resp. $H^1_f(K_v, W_{(\lambda, \kappa)})$, to be the image, resp. preimage, of $H^1_f(K_v, V_{(\lambda, \kappa)})$ under the natural maps

\[
H^1(K_v, T_{(\lambda, \kappa)}) \to H^1(K_v, V_{(\lambda, \kappa)}) \to H^1(K_v, W_{(\lambda, \kappa)})
\]
induced by the short exact sequence

\[ 0 \longrightarrow T_{(\lambda, \kappa)} \longrightarrow V_{(\lambda, \kappa)} \longrightarrow W_{(\lambda, \kappa)} \longrightarrow 0. \]

If \( M \) is a finite module over \( R \) for \( R = \mathbb{Z}_p, H^0, \) or \( H^n, \) then we define

\[ H^1(K, M) = \lim_{\rightarrow n} H^1(K, M/m^n_RM) \]

\[ H^1(K_v, M) = \lim_{\rightarrow n} H^1(K_v, M/m^n_RM) \]

for every place \( v \) of \( K, \) where \( m_R \) is the maximal ideal of \( R. \) If \( M \) is finitely generated over one of these rings, the groups \( H^1(K, M) \) and \( H^1(K_v, M) \) denote the usual cohomology groups.

For \( v \nmid p, \) we set

\[ H^1_f(K_v, W) = H^1_{ur}(K_v, W) \]

and set

\[ H^1_f(K_v, W) = \ker(H^1(K_v, W) \longrightarrow H^1(K^ur, F^{-} W)) \]

for \( v \mid p, \) where \( K^ur \) is the maximal unramified extension of \( K_v. \) We make the analogous definitions for \( H^1_f(K_v, W_f), H^1_f(K_v, W^*), \) and \( H^1_f(K_v, W_f^*). \) Recall that for every place \( v \) of \( K \) and every compact \( R \)-module \( M \) for \( R = H^n \) or \( H^0, \) local Tate duality provides a perfect pairing

\[ H^1(K_v, M) \times H^1(K_v, (M^*)^\vee) \longrightarrow R^\vee. \]

We define

\[ H^1_f(K_v, T) = H^1_{ur}(K_v, T) \]

if \( v \nmid p \) and let \( H^1_f(K_v, T) \) be the orthogonal complement of \( H^1_f(K_v, W^*) \) under the Tate pairing if \( v \mid p. \) We make the analogous definitions for \( H^1_f(K_v, T_f), H^1_f(K_v, T^*), \) and \( H^1_f(K_v, T^*_f). \)
For any $G_K$-module $M$ for which the notation has been defined, we set

\[
\text{Sel}^\Sigma(K, M) = \text{ker} \left( H^1(K, M) \rightarrow \bigoplus_{v \in \Sigma} H^1_s(K_v, M) \right)
\]
\[
\text{Sel}(K, M) = \text{ker} \left( \text{Sel}^\Sigma(K, M) \rightarrow \bigoplus_{v \in \Sigma} H^1_s(K_v, M) \right)
\]
\[
\text{Sel}_\Sigma(K, M) = \text{ker} \left( \text{Sel}(K, M) \rightarrow \bigoplus_{v \in \Sigma} H^1(K_v, M) \right),
\]

where $H^1_s(K_v, M) = H^1(K_v, M)/H^1_s(K_v, M)$. If $K = \mathbb{Q}$, we often suppress $K$ from the notation; i.e., Sel($M$) = Sel($\mathbb{Q}, M$), etc.

### 3.1.4. L-functions and Kato’s Euler system

Recall that to any cuspidal eigenform $f = \sum_{n=1}^{\infty} a_n(f) q^n$ of weight $k$ and trivial character, there is attached an $L$-function

\[
L(f, s) = \sum_{n=1}^{\infty} a_n(f) n^{-s} = \prod_{\ell} \frac{1}{1 - a_{\ell}(f) \ell^{-s}}.
\]

which has analytic continuation to all of $\mathbb{C}$ and satisfies a functional equation relating $L(f, s)$ and $L(f, k - s)$. It thus makes sense to speak of the the sign $\varepsilon_f = \pm 1$ in the functional equation of $f$; the sign determines the parity of the order of vanishing of $L(f, s)$ at $s = k/2$. The values of $L(f, s)$ at integer arguments are related via an interpolation property to an Euler system constructed by Kato. This Euler system arises from elements in the $K_2$ groups of modular curves via the Chern class map and comprises elements of the Galois cohomology of the dual representation $T^*$ over cyclotomic extensions of $\mathbb{Q}$.

Let $f$ be an eigenform of weight $k$ with coefficients in $\mathbb{Q}_f$, a finite extension of $\mathbb{Q}$. Attached to $f$ is a de Rham realization $V_{dR}(f)$, which is a 2-dimensional $\mathbb{Q}_f$-vector space equipped with a decreasing filtration $F^i V_{dR}(f)$. This filtration satisfies: $F^0 V_{dR}(f) = V_{dR}(f)$, $F^{k+2} V_{dR}(f) = 0$, and $F^i V_{dR}(f) \cong \mathbb{Q}_f \cdot f$ canonically for $0 < i < k + 2$. We will denote by $\overline{f}$ the conjugate form obtained by applying complex conjugation to the Fourier coefficients of $f$.  

72
Theorem 3.1.1 (Kato [8]). Let $R$ be the set of squarefree natural numbers prime to $\Sigma$. There are elements $z(r) \in \text{Sel}^\Sigma(\mathbb{Q}(\zeta_r), T^*)$ for every $r \in R$ such that if $q \in R$ does not divide $r$, then

$$
\text{Nm}_{\mathbb{Q}(\zeta_q)/\mathbb{Q}(\zeta_r)} z(rq) = P_q(\text{Frob}_q)z(r),
$$

where $P_q(X) = \det(1 - \text{Frob}_q X \mid T) \in H^{no}[X]$.

For each arithmetic specialization $(\lambda, \kappa)$ such that $1 \leq w(\lambda) \leq w(\kappa) + 1$, let $z(\lambda, \kappa)(1) \in \text{Sel}^\Sigma(\mathbb{Q}, T^*_{(\lambda, \kappa)})$ be the specialization of $z(1)$ via the character $(\lambda, \kappa)$. Then the image of $z(\lambda, \kappa)(1)$ under the localization map

$$
\text{loc}_\kappa : \text{Sel}^\Sigma(\mathbb{Q}, T^*_{(\lambda, \kappa)}) \longrightarrow H^1(\mathbb{Q}_p, T^*_{(\lambda, \kappa)})
$$

satisfies

$$
\exp^*\left(\text{loc}_\kappa z(\lambda, \kappa)(1)\right) = c(\lambda, \kappa)L(p, f_{\kappa}, \lambda \chi_{\mathcal{C}}^{-w(\lambda)}, w(\lambda)) \cdot \overline{\delta}_\kappa
$$

as elements of

$$
F^{w(\kappa)+2-w(\lambda)} \text{V}_{dR}(f_{\kappa}) \subseteq F^0 \text{D}_{dR}(V^*_{(\lambda, \kappa)}),
$$

where $\exp^* : H^1(\mathbb{Q}_p, T^*_{(\lambda, \kappa)}) \longrightarrow F^0 \text{D}_{dR}(V^*_{(\lambda, \kappa)})$ is the dual exponential map, $\overline{\delta}_\kappa$ is the basis of $F^{w(\kappa)+2-w(\lambda)} \text{V}_{dR}(f_{\kappa})$ corresponding to $f_{\kappa}$, and $c(j, \kappa)$ is an explicit non-zero constant (involving a complex period).

Recall the definition of the ring $H^0_f$ in 3.1.1. Let $g$ be a modular form of even weight $j \geq 2$ and character $\omega^{k-j}$ which arises as a specialization of the Hida family $\mathcal{F}$, say via the character $\kappa : \mathcal{H} \rightarrow \overline{\mathbb{Q}}_p$ of weight $w(\kappa) = j - 2$. If $j \equiv k \pmod{p-1}$, then $g$ has trivial character, the specialization $(k/2, \kappa) : H^{no} \rightarrow \overline{\mathbb{Q}}_p$ factors through $H^0_f$, and $z(k/2, \kappa)(1)$ interpolates (in the sense of Theorem 3.1.1) the central $L$-value $L(f, k/2)$. If $\varepsilon_f = \pm 1$ is the sign in the functional equation of $f$, then any modular form $g$ of even weight $j$ such that $j \equiv k \pmod{p-1}$ which arises as a specialization of $\mathcal{F}$ has $\varepsilon_g = \varepsilon_f$. We then say that $\varepsilon_f$ is the sign of the Hida family $\mathcal{F}$, and we denote it by $\varepsilon_f$. 

73
3.1.5. The Coleman map and the 2-variable main conjecture. We gather here two results that are fundamental to our method. The first is a construction of Ochiai [11] of a $p$-adic $L$-function for the nearly ordinary Hida deformation $H^{\text{no}}$ discussed in 3.1.1. Ochiai defines a “Coleman” map from a local (at $p$) cohomology group of the Galois representation $T$ of 3.1.3 to the ring $H^{\text{no}}$; the image under this map of the cohomology class arising from Kato’s Euler system attached to $\mathcal{F}$ is the desired $p$-adic $L$-function. We also describe the 2-variable main conjecture of Iwasawa theory for (the Pontryagin dual of) the Selmer group associated to the Galois module $T$, which has been proved by Skinner-Urban in many cases.

**Theorem 3.1.2** (Ochiai [11]). *There exists an injective $H^{\text{no}}$-linear homomorphism

$$\Xi : H^1_s(Q_\mathcal{F}, T^*) \longrightarrow H^{\text{no}}$$

*with pseudo-null cokernel such that the following interpolation formula holds:

$$\Xi(\text{loc}_\alpha z(1))_{(\lambda, \kappa)} = c(\lambda, \kappa)L(f_\kappa, \lambda \chi_C w(\lambda), \nu(\lambda))$$

*for any arithmetic specialization $(\lambda, \kappa)$ satisfying $0 \leq w(\lambda) - 1 \leq w(\kappa)$, where $c(\lambda, \kappa)$ is an explicit non-zero constant.*

The element $\Xi(\text{loc}_\alpha z(1))$ is to be regarded as a $p$-adic $L$-function for the Hida family $H^{\text{no}}$. It is thus natural to ask whether a “main conjecture of Iwasawa theory” relating $\Xi(\text{loc}_\alpha z(1))$ to the Selmer group $\text{Sel}(W)\mathcal{V}$ holds.

**Conjecture 3.1.3.** $\text{Sel}(W)\mathcal{V}$ is a torsion $H^{\text{no}}$-module, and for every prime ideal $\mathfrak{p} \subseteq H^{\text{no}}$ of height 1 not containing $(p)$,

$$\text{length}_\mathfrak{p} \text{Sel}(W)\mathcal{V} = \text{ord}_\mathfrak{p} \Xi(\text{loc}_\alpha z(1)).$$

Skinner-Urban have proved one divisibility of this conjecture in many cases; see [18] for an overview.

74
3.1.6. **Statement of the main result.** The remainder of the chapter will be devoted to proving the following result, which depends on the conjectural non-vanishing of the restriction of Kato's Euler system to the quotient $H^0_I$ of $H^{po}$, Conjectures 3.2.1 and 3.2.3.

**Theorem 3.1.4.** Assume Conjectures 3.1.3, 3.2.1, and 3.2.3. If the sign of $F$ is 1, then $\text{Sel}(W_f)^{\vee}$ is a torsion $H^0_I$-module and for every prime $p \subseteq H^0_I$ of height 1 not containing $(p)$, we have the equality

$$\text{length}_p \text{Sel}(W_f)^{\vee} = \text{ord}_p \Xi(\text{loc}_s z(1))_I.$$

If the sign of $F$ is $-1$, then $\text{Sel}(W_f)^{\vee}$ has generic rank 1 over $H^0_I$.

In 3.3.3, we show how a specialization argument implies the following consequence.

**Corollary 3.1.5.** Assume Conjectures 3.1.3, 3.2.1, and 3.2.3. Let $f$ be a $p$-ordinary modular form of even weight $k \geq 2$ and trivial character. $L(f, s)$ vanishes at $s = k/2$ if and only if the Selmer group $\text{Sel}(W_f(k/2))^{\vee}$ has positive rank as a $\mathbb{Z}_p$-module, where $W_f$ is the discrete $G_{\mathbb{Q}}$-module associated to the representation space $T_f$ of the Galois representation $\rho_f : G_{\mathbb{Q}} \to \text{GL}_2(\mathbb{Z}_p)$ associated to $f$.

This statement is consistent with a generalization of the conjecture of Birch and Swinnerton-Dyer, which predicts that $\text{ord}_{s=k/2} L(f, s) = \text{rk}_{\mathbb{Z}_p} \text{Sel}(W_f(k/2))^{\vee}$.

3.2. **The Euler system argument**

In this section, we use the Euler system of Kato to give one divisibility in the main conjecture. At the end of the section, we show how this divisibility can be used to relate the Selmer group of $f$ over $\mathbb{Q}$ to the $L$-function $L(f, s)$.

3.2.1. **Non-vanishing conjectures.** In order to glean information about the support of the Selmer groups associated to $W_f$ using Kato's Euler system, we need to know that this Euler system remains non-trivial when restricted to the anticyclotomic algebra $H^0_I$. When the sign of the Hida family is equal to 1, then the non-vanishing
of the Euler system follows from a conjecture regarding the non-vanishing of $L$-values of modular forms. When the sign of the Hida family is $-1$, on the other hand, we do not know of any way to relate non-vanishing of the Euler system to the non-vanishing of classical $L$-functions.

**Conjecture 3.2.1.** If the sign of $\mathcal{F}$ is equal to 1, then all but finitely many of the $L$-values $L(f_\kappa, w(\kappa)/2)$ are non-zero as $\kappa$ ranges over all arithmetic characters of $H$ such that $w(\kappa) \equiv k \pmod{p-1}$ and $\psi_\kappa = 1$.

**Corollary 3.2.2.** The image $\text{loc}_s z(1)_I \in H^1_s(Q_p, T^*_I)$ of $\text{loc}_s z(1) \in H^1_s(Q_p, T^*_I)$ under the natural restriction map is non-trivial.

We only use the corollary, which would follow from the existence of one non-vanishing specialization $L(f_\kappa, w(\kappa)/2)$ satisfying the hypotheses of Conjecture 3.2.1. When the sign of $\mathcal{F}$ is $-1$ the $L$-values $L(f_\kappa, w(\kappa)/2)$ are forced to vanish for infinitely many choices of $\kappa$. Thus $\text{loc} z(1)_I \in H^1(Q_p, T^*_I)$ lies in the local condition $H^1_I(Q_p, T^*_I)$ and cannot be related in any obvious way to $L$-values which are expected to be non-vanishing. We do, however, expect this class to be non-trivial.

**Conjecture 3.2.3.** If the sign of $\mathcal{F}$ is $-1$, then $\text{loc} z(1)_I \in H^1_I(Q_p, T^*_I)$ does not lie in the torsion submodule of $H^1_I(Q_p, T^*_I)$.

We will assume Conjectures 3.2.1 and 3.2.3 throughout the remainder of this chapter without further comment.

### 3.2.2. Tools for calculation.

We gather here several results which will be useful in the sequel for calculating the ranks of Selmer groups.

**Proposition 3.2.4.** The $H^1_{\text{tor}}$-module $H^1_s(Q_p, T^*_I)$ is torsion-free of generic rank 1; the $H^1_{\text{tor}}$-torsion submodule of $H^1_I(Q_p, T^*_I)$ is pseudo-null.

The proof of the first claim follows along the lines of the proof of Proposition 4.11 in [11]. The second claim comes from comparing the groups $H^1_I(Q_p, T^*_I)$ and $H^1(Q_p, F^+ T^*_I)$ and applying reasoning similar to Lemma 2.2.8 to the latter.
Proposition 3.2.5. There are canonical 5-term exact sequences

\[(3.2.1) \quad 0 \longrightarrow \text{Sel}(T_i^*) \longrightarrow \text{Sel}^E(T_i^*) \longrightarrow \]
\[\longrightarrow H^1_s(\mathbb{Q}_p, T_i^*) \longrightarrow \text{Sel}(W_i)^\vee \longrightarrow \text{Sel}_E(W_i)^\vee \longrightarrow 0\]

and

\[(3.2.2) \quad 0 \longrightarrow \text{Sel}_E(T_i^*) \longrightarrow \text{Sel}(T_i^*) \longrightarrow \]
\[\longrightarrow H^1_t(\mathbb{Q}_p, T_i^*) \longrightarrow \text{Sel}^E(W_i)^\vee \longrightarrow \text{Sel}(W_i)^\vee \longrightarrow 0\]

PROOF. The existence of these sequences is immediate from the definition of the Selmer groups involved, cf. 3.1.3. \(\Box\)

Proposition 3.2.5 is most useful when combined with the following proposition relating the compact and discrete Selmer groups arising from \(T_i^*\).

Proposition 3.2.6. There is a natural pseudo-isomorphism of \(H_{tQ}^{\text{po}}\)-modules

\[\text{Sel}^E(T_i^*) \longrightarrow \text{Hom}_{H_{tQ}^{\text{po}}}(\text{Sel}^E(W_i)^\vee, H_{tQ}^{\text{po}}).\]

In particular, the \(H_{tQ}^{\text{po}}\)-torsion submodule of \(\text{Sel}^E(T)\) is pseudo-null, and the generic rank of \(\text{Sel}^E(T)\) over \(H_{tQ}^{\text{po}}\) is equal to that of \(\text{Sel}^E(W_i)^\vee\).

3.2.3. Divisibility from Euler systems. The following theorem is the main result of §3.2 and comprises everything from Theorem 3.1.4 that we will prove without appealing to the two variable main conjecture, Conjecture 3.1.3.

Theorem 3.2.7. \(\text{Sel}_E(W_i)^\vee\) is a torsion \(H_{tQ}^{\text{po}}\)-module and

\[(3.2.3) \quad \text{length}_p \text{Sel}_E(W_i)^\vee \leq \text{length}_p \text{Sel}^E(T_i^*) / \langle z(1)_i \rangle\]

for every height 1 prime \(p \subseteq H_{tQ}^{\text{po}}\) not containing \((p)\). \(\text{Sel}^E(T_i^*)\) is pseudo-torsion-free of generic rank 1 over \(H_{tQ}^{\text{po}}\). If the sign of \(\mathcal{F}\) is \(-1\), then \(\text{Sel}(W_i)^\vee\) has generic rank 1 over \(H_{tQ}^{\text{po}}\) and \(\text{Sel}(T_i^*) = \text{Sel}^E(T_i^*)\). Otherwise, \(\text{Sel}(W_{tQ}^{\text{po}})^\vee\) is a torsion \(H_{tQ}^{\text{po}}\)-module.
The proof of this theorem will follow from the work of Mazur-Rubin [9] on Euler systems and an analysis of the fundamental exact sequences in Proposition 3.2.5. The argument should follow formally along the same lines as the proof of Theorem 2.2.14; in particular, the needed input from the theory of Euler systems is limited to (3.2.3).

3.3. Descent from the nearly ordinary Hecke algebra

This section is devoted to proving the remaining divisibility in the main conjecture by making use of the 2-variable main conjecture, Conjecture 3.1.3, and a descent argument from $H^\text{no}$ to $H^\text{po}$.

3.3.1. Descent. Theorem 3.2.7 gives the inequality

$$\text{length}_p \text{Sel}_\Sigma(W_I) \leq \text{length}_p \text{Sel}^\Sigma(T^*_I)/\langle z(1)_I \rangle$$

for primes $p \subseteq H^\text{no}_I$ of height 1 not containing $(p)$. In order to deduce Theorem 3.1.4 from Theorem 3.2.7, it is necessary to prove the reverse inequality.

**Proposition 3.3.1.** For every height 1 prime $p \subseteq H^\text{no}_I$ not containing $(p)$, we have the inequality

$$\text{length}_p \text{Sel}_\Sigma(W_I) = \text{length}_p \text{Sel}^\Sigma(T^*_I)/\langle z(1)_I \rangle.$$ 

The proof of the proposition starts from Conjecture 3.1.3, the 2-variable main conjecture, to conclude a similar statement for the corresponding $H^\text{no}$-modules. It is then a (non-trivial) exercise in Galois cohomology to conclude that the desired inequality is preserved upon descending from $H^\text{no}$ to $H^\text{po}$.

3.3.2. Proof of Theorem 3.1.4. To complete the proof of Theorem 3.1.4, it remains to be proved that $\text{length}_p \text{Sel}(W_I) = \text{ord}_p \Xi(\text{loc}_a z(1))_I$ in case the sign of $\mathcal{F}$ is 1. Consider the exact sequence

$$0 \rightarrow \text{Sel}^\Sigma(T^*_I)/\langle z(1)_I \rangle \rightarrow H^1_b(Q_p, T^*_I)/\langle \text{loc}_a z(1)_I \rangle \rightarrow$$

$$\rightarrow \text{Sel}(W_I) \rightarrow \text{Sel}_\Sigma(W_I) \rightarrow 0$$

78
obtained from (3.2.1). Let \( p \subseteq H_f^{\text{irr}} \) be any height 1 prime not containing \( (p) \). After localizing the above exact sequence at \( p \), all terms in the sequence have finite length over \( (H_f^{\text{irr}})_p \). The length of the two outside terms is the same by Proposition 3.3.1 and Theorem 3.2.7, so the two middle terms must also have the same length. Ochiai’s Theorem 3.1.2 then completes the argument.

**3.3.3. The Selmer group of \( f \).** Corollary 3.1.5 can be deduced from from Theorem 3.1.4 and the proposition below, which can be considered as a “control theorem” for \( H_f^{\text{irr}} \).

**Proposition 3.3.2.** The natural restriction homomorphism

\[
\text{Sel}(W_f(k/2)) \otimes_{\mathbb{Z}_p} \mathcal{O} \longrightarrow \text{Sel}(W_f)[p_{(\lambda, \kappa)}]
\]

has finite kernel and cokernel, where \( \mathcal{O} \) denotes the image of the arithmetic character \( (\lambda, \kappa) : H^{\text{irr}} \rightarrow \overline{\mathbb{Q}}_p \) for which \( T_{(\lambda, \kappa)} \cong T_f(k/2) \otimes_{\mathbb{Z}_p} \mathcal{O} \).

When the sign of \( \mathcal{F} \) is \(-1\), \( \text{Sel}(W_f)^{\vee} \) has positive generic rank over \( H_f^{\text{irr}} \), so \( \text{Sel}(W_f) \otimes_{H_f^{\text{irr}}} \mathcal{O} \) is infinite. This implies that \( \text{rk}_{\mathbb{Z}_p} \text{Sel}(W_f(k/2)) > 0 \). Otherwise, if the sign of \( \mathcal{F} \) is 1, then the vanishing of \( L(f, k/2) \) is equivalent, by Theorem 3.1.4 and the interpolation property of \( \Xi(\text{loc}_f z(1)) \), to the infinitude of \( \text{Sel}(W_f)[p_{(\lambda, \kappa)}] \).
Bibliography


