

# ON THE CUSPIDALITY OF PULLBACKS OF SIEGEL EISENSTEIN SERIES AND APPLICATIONS TO THE BLOCH-KATO CONJECTURE

JIM BROWN

ABSTRACT. Let  $k > 3$  be an integer and  $p$  a prime with  $p > 2k - 2$ . Let  $f$  be a newform of weight  $2k - 2$  and level 1 so that  $f$  is ordinary at  $p$  and  $\bar{\rho}_f$  is irreducible. Under some additional hypotheses we prove that  $\text{ord}_p(L_{\text{alg}}(k, f)) \leq \text{ord}_p(\#S)$  where  $S$  is the Pontryagin dual of the Selmer group associated to  $\rho_f \otimes \varepsilon^{1-k}$  with  $\varepsilon$  the  $p$ -adic cyclotomic character. We accomplish this by first constructing a congruence between the Saito-Kurokawa lift of  $f$  and a non-CAP Siegel cusp form. Once this congruence is established, we use Galois representations to obtain the lower bound on the Selmer group.

## 1. INTRODUCTION

The conjecture of Bloch and Kato, also known as the Tamagawa number conjecture, is one of the central outstanding conjectures in number theory. Let  $f$  be a newform of weight  $2k - 2$  and level 1. The Bloch-Kato conjecture for modular forms roughly states that the special values of the  $L$ -function associated to  $f$  should measure the size of the Selmer group associated to twists of the Galois representation associated to  $f$ . In previous work we showed that under suitable hypotheses that one has that if  $\text{ord}_p(L_{\text{alg}}(k, f)) \geq 1$ , then  $\text{ord}_p(\# \text{Sel}(W)) \geq 1$  ([Br07]). Unfortunately, due to limitations of the method used one was unable to gain any more information than this. In this paper we improve upon these results yielding the much stronger result that under the same hypotheses needed before roughly speaking one has

$$\text{ord}_p(L_{\text{alg}}(k, f)) \leq \text{ord}_p(\# \text{Sel}(W)).$$

The method of proof is in the same spirit as used in [Br07] with significant improvements at a couple of steps. Nevertheless, we briefly recount the method here.

The general outline of the method goes back to work of Ribet on the proof of the converse of Herbrand's theorem ([R76]). This method has been generalized and applied in other contexts by several authors ([KK07], [SU06], [Wi90], etc.) The method employed by Ribet (in a slightly more general

---

2000 *Mathematics Subject Classification*. Primary 11F33, 11F67; Secondary 11F46, 11F80.

*Key words and phrases*. Saito-Kurokawa, modular forms, pullbacks of Eisenstein series, Selmer groups.

form) is as follows. Given a positive integer  $k$  and a primitive Dirichlet character  $\chi$  of conductor  $N$  so that  $\chi(-1) = (-1)^k$ , one has an associated Eisenstein series  $E_{k,\chi}$  with constant term  $\frac{L(1-k,\chi)}{2}$ . For an odd prime  $p$  with  $p \mid L(1-k,\chi)$  and  $p \nmid N$ , one can show that there is a cuspidal eigenform  $g$  of weight  $k$  and level  $M$  with  $N \mid M$  so that  $g \equiv E_{k,\chi} \pmod{\mathfrak{p}}$  for some prime  $\mathfrak{p} \mid p$ . This congruence is used to study the residual Galois representation of  $g$ . It is shown that  $\bar{\rho}_{g,\mathfrak{p}} \simeq \begin{pmatrix} 1 & * \\ 0 & \chi\omega^{k-1} \end{pmatrix}$  is non-split where  $\omega$  is the reduction of the  $p$ -adic cyclotomic character. This allows one to show that  $*$  gives a non-zero cohomology class in  $H_{\text{ur}}^1(\mathbb{Q}, \chi^{-1}\omega^{1-k})$ .

For our purposes, the character in Ribet's method will be replaced with a newform  $f$  of weight  $2k - 2$  and level 1. Associated to  $f$  we have its Saito-Kurokawa lift  $F_f$ , our replacement for the Eisenstein series  $E_{k,\chi}$ . Our goal is to find a Siegel modular form  $G$  that is not a Saito-Kurokawa lift so that the Fourier coefficients of  $G$  are congruent modulo  $\varpi^m$  to those of  $F_f$  for some integer  $m \geq 1$ . We are able to produce such a  $G$  by exploiting the explicit nature of the Saito-Kurokawa correspondence, using the pullback of a Siegel Eisenstein series and an inner product relation of Shimura ([Sh95]) as key ingredients. It is at this step a significant improvement over the results of [Br07] is made. We use results of Garrett to show that in fact the Siegel Eisenstein series used pulls back to something cuspidal in each variable. This allows us to avoid some of the ad hoc methods needed in [Br07] that "lost the powers of  $p$ ". Once we have the congruence desired, we generalize results of Urban ([U01]) to our situation to allow us to give the lower bound on the Selmer group. This generalization is another significant improvement over our work in [Br07] and allows us to get the lower bound desired.

The author would like to thank Jim Cogdell for many helpful conversations.

## 2. NOTATION

In this section we set the notation and definitions to be used throughout this paper.

Let  $\mathbb{A}$  be the ring of adeles over  $\mathbb{Q}$ . For a prime  $p$ , we fix once and for all compatible embeddings  $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ ,  $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ , and  $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ . We write  $\text{ord}_p(n)$  to denote  $p^m$  for  $p^m \parallel n$ . We denote by  $\varepsilon_p$  the  $p$ -adic cyclotomic character  $\varepsilon_p : G_{\mathbb{Q}} \rightarrow \text{GL}_1(\mathbb{Z}_p)$ . We drop the  $p$  when it is clear from context. We denote the residual representation of  $\varepsilon_p$  by  $\omega_p$ , again dropping the  $p$  when it is clear from context.

For a ring  $R$ , we let  $M_{m,n}(R)$  denote the set of  $m$  by  $n$  matrices with entries in  $R$ . If  $m = n$  we write  $M_m(R)$  for  $M_{m,m}(R)$ . For a matrix  $x \in M_{2n}(R)$ , we write

$$x = \begin{pmatrix} a_x & b_x \\ c_x & d_x \end{pmatrix}$$

where  $a_x, b_x, c_x,$  and  $d_x$  are all in  $M_n(R)$ . We drop the subscript  $x$  when it is clear from the context. The transpose of a matrix  $x$  is denoted by  ${}^t x$ .

Let  $\mathrm{SL}_2$  and  $\mathrm{GL}_n$  have their standard definitions. We denote the complex upper half-plane by  $\mathfrak{h}^1$ . We have the usual action of  $\mathrm{GL}_2^+(\mathbb{R})$  on  $\mathfrak{h}^1 \cup \mathbb{P}^1(\mathbb{Q})$  given by linear fractional transformations. Define

$$\mathrm{Sp}_{2n} = \{g \in \mathrm{GL}_{2n} : {}^t \gamma \iota_{2n} \gamma = \iota_{2n}\}, \quad \iota_{2n} = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix}.$$

Siegel upper half-space is defined by

$$\mathfrak{h}^n = \{Z \in M_n(\mathbb{C}) : {}^t Z = Z, \mathrm{Im}(Z) > 0\}.$$

The group  $\mathrm{Sp}_{2n}(\mathbb{R})$  acts on  $\mathfrak{h}^n$  via

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} Z = (AZ + B)(CZ + D)^{-1}.$$

We let  $\Gamma_1^J = \mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2$  be the Jacobi modular group ([EZ85]).

Given an  $L$ -function  $L(s) = \prod_p L_p(s)$  and a finite set of places  $\Sigma$ , we write

$$L^\Sigma(s) = \prod_{p \notin \Sigma} L_p(s)$$

when we restrict to places away from  $\Sigma$  and

$$L_\Sigma(s) = \prod_{p \in \Sigma} L_p(s)$$

when we restrict to the places in  $\Sigma$ .

Let  $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$  be a congruence subgroup. We write  $M_k(\Gamma)$  to denote the space of modular forms of weight  $k$  and level  $\Gamma$ . We let  $S_k(\Gamma)$  denote the subspace of cusp forms. The  $n$ th Fourier coefficient of  $f \in M_k(\Gamma)$  is denoted by  $a_f(n)$ . Given a ring  $R \subset \mathbb{C}$ , we write  $M_k(\Gamma, R)$  for the space of modular forms with Fourier coefficients in  $R$  and similarly for  $S_k(\Gamma, R)$ . Let  $f_1, f_2 \in M_k(\Gamma)$  with at least one of the  $f_i$  a cusp form. The Petersson product is given by

$$\langle f_1, f_2 \rangle = \frac{1}{[\overline{\mathrm{SL}_2(\mathbb{Z})} : \overline{\Gamma}]} \int_{\Gamma \backslash \mathfrak{h}^1} f_1(z) \overline{f_2(z)} y^{k-2} dx dy$$

where  $\overline{\mathrm{SL}_2(\mathbb{Z})} = \mathrm{SL}_2(\mathbb{Z}) / \{\pm 1_2\}$  and  $\overline{\Gamma}$  is the image of  $\Gamma$  in  $\overline{\mathrm{SL}_2(\mathbb{Z})}$ . The  $n$ th Hecke operator  $T(n)$  has its usual meaning. Let  $A$  be a  $\mathbb{Z}$ -algebra. Let  $\mathbb{T}_{\mathbb{Z}}$  be the  $\mathbb{Z}$ -subalgebra of  $\mathrm{End}_{\mathbb{C}}(S_k(\mathrm{SL}_2(\mathbb{Z})))$  generated by  $T(n)$  for  $n = 1, 2, 3, \dots$ . Note that we do not include the weight in the notation as it will always be clear from context. We set  $\mathbb{T}_A = \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} A$ . We say  $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$  is a newform if it is an eigenform for all  $T(n)$  and  $a_f(1) = 1$ . The  $L$ -function associated to a newform  $f$  of weight  $k$  is given by

$$L(s, f) = \sum_{n \geq 1} a_f(n) n^{-s}.$$

The  $L$ -function  $L(s, f)$  can be factored as

$$L(s, f) = \prod_p [(1 - \alpha_f(p)p^{-s})(1 - \beta_f(p)p^{-s})]^{-1}$$

where  $\alpha_f(p) + \beta_f(p) = a_f(p)$  and  $\alpha_f(p)\beta_f(p) = p^{k-1}$ . The terms  $\alpha_f(p)$  and  $\beta_f(p)$  are referred to as the  $p$ th Satake parameters of  $f$ .

Kohnen's  $+$ -space of half-integral weight modular forms is given by

$$S_{k-1/2}^+(\Gamma_0(4)) = \{g \in S_{k-1/2}(\Gamma_0(4)) : a_g(n) = 0 \text{ if } (-1)^{k-1}n \equiv 2, 3 \pmod{4}\}.$$

The Petersson product on  $S_{k-1/2}^+(\Gamma_0(4))$  is given by

$$\langle g_1, g_2 \rangle = \int_{\Gamma_0(4)\backslash\mathfrak{h}^1} g_1(z)\overline{g_2(z)}y^{k-5/2}dx dy.$$

We denote the space of Jacobi cusp forms on  $\Gamma_1^J$  by  $J_{k,1}^{\text{cusp}}(\Gamma_1^J)$ . The inner product is given by

$$\langle \phi_1, \phi_2 \rangle = \int_{\Gamma_1^J\backslash\mathfrak{h}^1 \times \mathbb{C}} \phi_1(\tau, z)\overline{\phi_2(\tau, z)}v^{k-3}e^{-4\pi y^2/v}dx dy du dv$$

for  $\phi_1, \phi_2 \in J_{k,1}^{\text{cusp}}(\Gamma_1^J)$  and  $\tau = u + iv$ ,  $z = x + iy$ .

We denote the space of Siegel modular forms of weight  $k$  and level  $\Gamma \subset \text{Sp}_{2n}(\mathbb{Z})$  by  $\mathcal{M}_k(\Gamma)$ . The subspace of cusp forms is denoted by  $\mathcal{S}_k(\Gamma)$ . For  $F, G \in \mathcal{M}_k(\text{Sp}_{2n}(\Gamma))$  with at least one a cusp form, the Petersson product is given by

$$\langle F, G \rangle = \frac{1}{[\text{Sp}_{2n}(\mathbb{Z}) : \Gamma]} \int_{\Gamma\backslash\mathfrak{h}^n} F(Z)\overline{G(Z)}\det(\text{Im}(Z))^k d\mu(Z).$$

We will be particularly interested in the decomposition

$$\mathcal{S}_k(\text{Sp}_4(\mathbb{Z})) = \mathcal{S}_k^{\text{M}}(\text{Sp}_4(\mathbb{Z})) \oplus \mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$$

where  $\mathcal{S}_k^{\text{M}}(\text{Sp}_4(\mathbb{Z}))$  is the space of Maass spezialchars and  $\mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$  is the orthogonal complement. A form  $F \in \mathcal{S}_k(\text{Sp}_4(\mathbb{Z}))$  is in  $\mathcal{S}_k^{\text{M}}(\text{Sp}_4(\mathbb{Z}))$  if the Fourier coefficients of  $F$  satisfy the relation

$$A_F(n, r, m) = \sum_{d|\text{gcd}(n,r,m)} d^{k-1} A_F\left(\frac{nm}{d^2}, \frac{r}{d}, 1\right).$$

We let  $T^S(n)$  denote the  $n$ th Siegel Hecke operator. As above, we set  $\mathbb{T}_{\mathbb{Z}}^S$  to be the  $\mathbb{Z}$ -subalgebra of  $\text{End}_{\mathbb{C}}(\mathcal{S}_k(\text{Sp}_{2n}(\mathbb{Z})))$  generated by the  $T(n)$ . For a  $\mathbb{Z}$ -algebra  $A$  we write  $\mathbb{T}_A^S = \mathbb{T}_{\mathbb{Z}}^S \otimes_{\mathbb{Z}} A$ . The Hecke algebra  $\mathbb{T}_{\mathbb{C}}^S$  respects the decomposition of  $\mathcal{S}_k(\text{Sp}_4(\mathbb{Z}))$  into the space of Maass and non-Maass forms ([A80]).

Let  $F \in \mathcal{S}_k(\Gamma_2)$  be a Hecke eigenform with eigenvalues  $\lambda_F(m)$ . Associated to  $F$  is an  $L$ -function called the spinor  $L$ -function. It is defined by

$$L_{\text{spin}}(s, F) = \zeta(2s - 2k + 4) \sum_{m \geq 1} \lambda_F(m) m^{-s}.$$

One can also define the spinor  $L$ -function in terms of the Satake parameters  $\alpha_0, \alpha_1$ , and  $\alpha_2$  of  $F$ . One has

$$L_{\text{spin}}(s, F) = \prod_p Q_p(p^{-s})^{-1}$$

where

$$Q_p(X) = (1 - \alpha_0 X)(1 - \alpha_0 \alpha_1 X)(1 - \alpha_0 \alpha_2 X)(1 - \alpha_0 \alpha_2 \alpha_2 X).$$

The standard  $L$ -function associated to  $F$  is given by

$$(1) \quad L_{\text{st}}(s, F) = \prod_{\ell} W_{\ell}(\ell^{-s})^{-1}$$

where

$$W_{\ell}(t) = (1 - \ell^2 t) \prod_{i=1}^2 (1 - \ell^2 \alpha_i t)(1 - \ell^2 \alpha_i^{-1} t).$$

Given a Hecke character  $\phi$ , the twisted standard zeta function is given by

$$L_{\text{st}}(s, F, \phi) = \prod_{\ell} W_{\ell}(\phi(\ell)\ell^{-s})^{-1}.$$

### 3. SIEGEL EISENSTEIN SERIES

In this section we study pullbacks of Siegel Eisenstein series and show that the pullback of the Siegel Eisenstein series from  $\text{Sp}_{4n}$  to  $\text{Sp}_{2n} \times \text{Sp}_{2n}$  is cuspidal in each variable. We use the methods developed by Garrett ([G92]) along with standard facts about Siegel Eisenstein series to establish this result. We also recall facts that can be found in [Br07] about the Fourier coefficients of the Siegel Eisenstein series as well as a formula for the inner product of the pullback of the Siegel Eisenstein series with a cuspidal Siegel eigenform due to Shimura ([Sh95]).

**3.1. Basic definitions and results.** We begin by recalling the definition of some subgroups of  $\text{Sp}_{2m}(\mathbb{A})$  and  $\text{Sp}_{2m}(\mathbb{Q})$ . Let  $N > 1$  be an integer let  $\Sigma$  be the set of primes dividing  $N$ . For a prime  $\ell$  define

$$K_{0,\ell}(N) = \{g \in \text{Sp}_{2m}(\mathbb{Q}_{\ell}) : a_g, b_g, d_g \in \text{M}_m(\mathbb{Z}_{\ell}), c_g \in \text{M}_m(N\mathbb{Z}_{\ell})\}$$

and set

$$K_{0,f}(N) = \prod_{\ell \nmid \infty} K_{0,\ell}(N).$$

Set

$$K_{\infty} = \{g \in \text{Sp}_{2m}(\mathbb{R}) : g\mathbf{i}_{2m} = \mathbf{i}_{2m}\}$$

where  $\mathbf{i}_{2m} = i1_{2m}$ . and

$$K_0(N) = K_{\infty} K_{0,f}(N).$$

Set

$$\mathbb{S}_m = \{x \in \text{M}_m : {}^t x = x\}.$$

Let  $P_{2m} = U_{2m}Q_{2m}$  be the Siegel parabolic of  $\mathrm{Sp}_{2m}$  defined by

$$P_{2m} = \{g \in \mathrm{Sp}_{2m} : c_g = 0\}$$

with unipotent radical

$$U_{2m} = \left\{ u(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{S}_m \right\}$$

and Levi subgroup

$$Q_{2m} = \left\{ Q(A) = \begin{pmatrix} A & 0 \\ 0 & {}_tA^{-1} \end{pmatrix} : A \in \mathrm{GL}_m \right\}.$$

We drop the subscript  $2m$  from the notation when it is clear from context.

Let  $k$  be a positive integer such that  $k > \max\{3, m+1\}$ . Let  $\chi$  be a Hecke character of  $\mathbb{A}^\times$  satisfying

$$(2) \quad \begin{aligned} \chi_\infty(x) &= \mathrm{sgn}(x)^k, \\ \chi_\ell(a) &= 1 \quad \text{if } \ell \nmid \infty, a \in \mathbb{Z}_\ell^\times, \text{ and } N \mid (a-1). \end{aligned}$$

Define  $\varepsilon(g, s; k, N, \chi)$  on  $\mathrm{Sp}_{2m}(\mathbb{A}) \times \mathbb{C}$  by

$$\varepsilon(g, s; k, N, \chi) = 0$$

if  $g \notin P(\mathbb{A})K_0(N)$  and for  $g = u(x)Q(A)\theta$  with  $u(x)Q(A) \in P(\mathbb{A})$  and  $\theta \in K_0(N)$

$$\varepsilon(g, s; k, N, \chi) = \varepsilon_\infty(g, s; k, \chi) \prod_{\ell \nmid N} \varepsilon_\ell(g, s; k, \chi) \prod_{\ell \mid N} \varepsilon_\ell(g, s; k, N, \chi)$$

where we define the components by

$$\begin{aligned} \varepsilon_\infty(g, s; k, \chi) &= \chi_\infty(\det A_\infty) |\det A_\infty|^{2s} j^k(\theta_\infty, \mathbf{i})^{-1}, \\ \varepsilon_\ell(g, s; k, \chi) &= \chi_\ell(\det A_\ell) |\det A_\ell|^{2s} \quad (\ell \nmid N) \\ \varepsilon_\ell(g, s; k, N, \chi) &= \chi_\ell(\det A_\ell) \chi_\ell(\det d_\theta)^{-1} |\det A_\ell|^{2s} \quad (\ell \mid N). \end{aligned}$$

The Siegel Eisenstein series is defined by

$$E(g, s) = E(g, s; k, N, \chi) = \sum_{\gamma \in P(\mathbb{Q}) \backslash \mathrm{Sp}_{2m}(\mathbb{Q})} \varepsilon(\gamma g, s; k, N, \chi).$$

The series  $E(g, s)$  converges locally uniformly for  $\mathrm{Re}(s) > (m+1)/2$  and can be continued to a meromorphic function on all of  $\mathbb{C}$ . It has a functional equation relating  $E(g, s)$  to  $E(g, (m+1)/2 - s)$ .

Associated to the Siegel Eisenstein series  $E(g, s)$  is a complex version  $E(Z, s)$  defined on  $\mathfrak{h}^m \times \mathbb{C}$  by

$$E(Z, s) = j^k(g_\infty, \mathbf{i}_{2m}) E(g, s)$$

where  $Z = g_\infty \mathbf{i}_{2m}$  and  $g = g_\mathbb{Q} g_\infty \theta_f \in \mathrm{Sp}_{2m}(\mathbb{Q}) \mathrm{Sp}_{2m}(\mathbb{R}) K_{0,f}(N)$ . It will be important for us that  $E(Z, (m+1)/2 - k/2)$  and  $E(Z, k/2)$  are both holomorphic modular forms of weight  $k$  and level  $N$  ([Sh87]). We will use whichever of these Siegel Eisenstein series is most convenient for the current application, keeping in mind the above relation between them.

Finally, we recall a result on the Fourier coefficients of  $E(Z, (m+1)/2 - k/2)$  demonstrated in [Br07]. Let  $E^*(g, s) = E(g\varsigma_f^{-1}, s)$  where we recall  $\varsigma = \begin{pmatrix} 0_m & -1_m \\ 1_m & 0_m \end{pmatrix}$ . It is convenient to look at this translation when calculating the Fourier coefficients of  $E(g, s)$ . We let  $E^*(Z, s)$  be the corresponding complex version. Write elements  $Z \in \mathfrak{h}^m$  as  $Z = X + iY$  with  $X, Y \in \mathbb{S}^m(\mathbb{R})$  and  $Y > 0$ .  $L = \mathbb{S}^m(\mathbb{Q}) \cap M_m(\mathbb{Z})$ ,  $L' = \{\mathfrak{s} \in \mathbb{S}^m(\mathbb{Q}) : \text{Tr}(\mathfrak{s}L) \subseteq \mathbb{Z}\}$  and  $M = N^{-1}L'$ . The Eisenstein series  $E^*(Z, s)$  has a Fourier expansion

$$E^*(Z, s) = \sum_{h \in M} a(h, Y, s) e(\text{Tr}(hX))$$

for  $Z = X + iY \in \mathfrak{h}^m$ . Set

$$\Lambda^\Sigma(s, \chi) = L^\Sigma(2s, \chi) \prod_{j=1}^{[m/2]} L^\Sigma(4s - 2j, \psi^2).$$

We normalize  $E^*(Z, s)$  by multiplying it by  $\pi^{-\frac{m(m+2)}{4}} \Lambda^\Sigma(s, \chi)$ . We have the following result.

**Theorem 3.1.** ([Br07] *Theorem 2.4*) *Let  $p$  be an odd prime such that  $p > m$  and  $\gcd(p, N) = 1$ . Set*

(3)

$$D_{E^*}(Z, (m+1)/2 - k/2) = (\pi^{-\frac{m(m+2)}{4}} \Lambda^\Sigma((m+1)/2 - k/2, \chi)) E^*(Z, (m+1)/2 - k/2).$$

Then

$$D_{E^*}(Z, (m+1)/2 - k/2) \in \mathcal{M}_k(\Gamma_0^{2m}(N), \mathbb{Z}_p[\chi, i^{mk}]).$$

**3.2. Pullbacks of Siegel Eisenstein series.** We begin by reviewing the notion of the pullback of an automorphic form on  $\text{Sp}_{4n}(\mathbb{A})$  to  $\text{Sp}_{2n}(\mathbb{A}) \times \text{Sp}_{2n}(\mathbb{A})$ . This theory has been well established and the interested reader is advised to consult any of the following references for more details: ([B85], [G92], [G84], [Sh95], [Sh97]).

Let  $\text{Sp}_{2n} \times \text{Sp}_{2n}$  be imbedded in  $\text{Sp}_{4n}$  via

$$\iota \left( \left( \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right) \right) = \begin{pmatrix} a_1 & 0 & b_1 & 0 \\ 0 & a_2 & 0 & b_2 \\ c_1 & 0 & d_1 & 0 \\ 0 & c_2 & 0 & d_2 \end{pmatrix}.$$

One can show that given a holomorphic automorphic form  $F$  of weight  $k$  and level  $N$  on  $\text{Sp}_{4n}(\mathbb{A})$ , the function  $(g_1, g_2) \mapsto F(\iota(g_1, g_2))$  is a holomorphic automorphic form of weight  $k$  and level  $N$  in each variable, see [G92] for example. The form  $F(\iota(g_1, g_2))$  is referred to as the pullback of  $F$  from  $\text{Sp}_{4n}$  to  $\text{Sp}_{2n} \times \text{Sp}_{2n}$ , or just the pullback of  $F$ . We will often drop the  $\iota$  from the notation when it is clear from context. If we wish to work classically rather than adelically we make use of the embedding

$$\mathfrak{h}^n \times \mathfrak{h}^n \hookrightarrow \mathfrak{h}^{2n}$$

given by

$$Z \times W \mapsto \begin{pmatrix} Z & 0 \\ 0 & W \end{pmatrix} = \text{diag}[Z, W]$$

arising from the isomorphism  $\text{Sp}_{2n}(\mathbb{R})/K_{0,\infty} \cong \mathfrak{h}^n$ .

Our goal is to show that the Eisenstein series  $E(\iota(g_1, g_2), (n+1)/2 - k/2)$  is cuspidal in  $g_1$  and  $g_2$  where  $g_1, g_2 \in \text{Sp}_{2n}(\mathbb{A})$ . We begin by noting that using the functional equation, this is equivalent to showing that  $E(\iota(g_1, g_2), k/2)$  is cuspidal in  $g_1$  and  $g_2$ . We now wish to apply the methods used by Garrett in [G92]. To do this, we restrict our Eisenstein series from  $P_{4n}(\mathbb{A})K_0(N)$  to  $P_{4n}(\mathbb{A})K(N)$  where  $K(N) = K_\infty \prod_{\ell \mid \infty} K_\ell(N)$  with

$$K_\ell(N) = \{g \in \text{Sp}_{4n}(\mathbb{Q}_\ell) : g \equiv 1_{4n} \pmod{N}\}.$$

Classically we are taking  $E(\mathcal{Z}, k/2)$ , which is in  $\mathcal{M}_k(\Gamma_0^{4n}(N))$ , and thinking of it as a modular form in  $\mathcal{M}_k(\Gamma^{4n}(N))$ . From this it is clear that if the pullback of the restricted Eisenstein series is cuspidal, so is the original. We denote the Eisenstein series restricted to  $P_{4n}(\mathbb{A})K(N)$  as  $E'$ . Observe that if we write

$$E'(g, k/2) = \sum_{\gamma \in P_{4n}(\mathbb{Q}) \backslash \text{Sp}_{4n}(\mathbb{Q})} \epsilon(\gamma g, k/2)$$

with  $\epsilon(g, k/2)$  factored into local components as in the previous section, then we have  $\epsilon_\infty(g, k/2) = \varepsilon_\infty(g, k/2)$ ,  $\epsilon_\ell(g, k/2) = \varepsilon_\ell(g, k/2)$  for  $\ell \nmid N$ , and  $\epsilon_\ell(g, k/2) = \chi_\ell(\det A_\ell) |\det A_\ell|^k$  for  $\ell \mid N$ . Note the  $\chi_\ell(\det d_\theta)^{-1}$  drops out because of the restriction to  $K(N)$ . We are now in a position to apply Garrett's argument to  $E'(\iota(g_1, g_2), k/2)$  to show that it is cuspidal in  $g_1$  and  $g_2$  ([G92]).

Let  $\theta \in \text{Sp}_{4n}(\mathbb{A}_f)$  be an element so that

$$(0_{2n} 1_{2n})\theta = \begin{pmatrix} 1_n & 1_n & 0_n & 0_n \\ 0_n & 0_n & -1_n & 1_n \end{pmatrix}.$$

We will consider the Eisenstein series translated by this  $\theta$ , namely, we will show that  $E'(\iota(g_1, g_2)\theta^{-1}, k/2)$  is cuspidal in  $g_1$  and  $g_2$ . Classically this just amounts to translating to a different cusp, so it is sufficient to show this translated Eisenstein series is cuspidal in  $g_1$  and  $g_2$ .

The space

$$X = P_{4n}(\mathbb{Q}) \backslash \text{Sp}_{4n}(\mathbb{Q}) / \iota(\text{Sp}_{2n}(\mathbb{Q}) \times \text{Sp}_{2n}(\mathbb{Q}))$$

has representatives  $\tau_0, \tau_1, \dots, \tau_n$  so that

$$(0_{2n} 1_{2n})\tau_i = \begin{pmatrix} 1_{n-i} & 0_i & 0_{n-i} & 0_i & 0_{n-i} & 0_i & 0_{n-i} & 0_i \\ 0_{n-i} & 1_i & 0_{n-i} & 1_i & 0_{n-i} & 0_i & 0_{n-i} & 0_i \\ 0_{n-i} & 0_i & 0_{n-i} & 0_i & 0_{n-i} & 0_i & 1_{n-i} & 0_i \\ 0_{n-i} & 0_i & 0_{n-i} & 0_i & 0_{n-i} & -1_i & 0_{n-i} & 1_i \end{pmatrix}.$$

This is essentially a result in geometric algebra, see [G92] for a proof. Let  $I_i$  be the isotropy group of  $P_{4n}(\mathbb{Q})\tau_i$  in  $P_{4n}(\mathbb{Q}) \backslash \text{Sp}_{4n}(\mathbb{Q})$  under  $\text{Sp}_{2n}(\mathbb{Q}) \times$

$\mathrm{Sp}_{2n}(\mathbb{Q})$  acting on the right, i.e.,

$$I_i = \{(g_1, g_2) \in \mathrm{Sp}_{2n}(\mathbb{Q}) \times \mathrm{Sp}_{2n}(\mathbb{Q}) : P_{4n}(\mathbb{Q})\tau_i\iota(g_1, g_2) = P_{4n}(\mathbb{Q})\tau_i\}.$$

This allows us to write our Eisenstein series as

$$E'(\iota(g_1, g_2)\theta^{-1}, k/2) = \sum_{0 \leq i \leq n} \vartheta_i(g_1, g_2)$$

where

$$\vartheta_i(g_1, g_2) = \sum_{\gamma \in I_i \backslash \iota(\mathrm{Sp}_{2n}(\mathbb{Q}) \times \mathrm{Sp}_{2n}(\mathbb{Q}))} \epsilon(\tau_i \gamma \iota(g_1, g_2)\theta^{-1}, k/2).$$

Our goal now is to show that  $\vartheta_i(g_1, g_2) = 0$  for all  $g_1, g_2 \in \mathrm{Sp}_{2n}(\mathbb{Q})$  unless  $i = n$ . Observe that it is enough to show that for any prime  $p \mid N$ , we have  $\epsilon_p(\tau_i \gamma \iota(g_1, g_2)\theta^{-1}, k/2) = 0$  for all  $g_1, g_2 \in \mathrm{Sp}_{2n}(\mathbb{Q}_p)$ . In order to show this, we give an integral representation of the Eisenstein series components  $\epsilon_p$ .

Let  $\mathrm{GL}_n(\mathbb{Q}_p)$  have Haar measure normalized so that  $\mathrm{GL}_n(\mathbb{Z}_p)$  has Haar measure 1. For  $p \mid N$ , let  $\phi_p$  be the characteristic function of the set

$$\{(m_1 m_2) \in \mathrm{M}_{n \times 2n}(\mathbb{Q}_p) : (m_1 m_2) \equiv (0_n 1_n) \pmod{N}\}.$$

A change of variables shows that for  $g \in \mathrm{Sp}_n(\mathbb{Q}_p)$  we have

$$\epsilon_p(g; k/2) = \mathcal{I}_p(g) / \mathcal{I}_p(1_{2n})$$

where

$$\mathcal{I}_p(g) = \int_{\mathrm{GL}_n(\mathbb{Q}_p)} |\det h|^k \chi(\det h) \phi_p(h(0_n 1_n)g) dh.$$

In order to show that  $\vartheta_i(g_1, g_2) = 0$  for all  $g_1, g_2 \in \mathrm{Sp}_{2n}(\mathbb{Q})$  unless  $i = n$ , we will show that

$$\mathcal{I}_p(\tau_i \iota(g_1, g_2)\theta^{-1}) = 0$$

for  $p \mid N$  and every  $g_1, g_2 \in \mathrm{Sp}_{2n}(\mathbb{Q}_p)$  if  $i \neq n$ . In particular, the definition of  $\mathcal{I}_p$  allows us to reduce this to showing that

$$\phi_p(g(0_{2n} 1_{2n})\tau_i \iota(g_1, g_2)\theta^{-1}) = 0$$

for every  $p \mid N$ ,  $g_1, g_2 \in \mathrm{Sp}_{2n}(\mathbb{Q}_p)$ , and  $g \in \mathrm{GL}_{2n}(\mathbb{Q}_p)$  unless  $i = n$ . We have that  $\phi_p(g(0_{2n} 1_{2n})\tau_i \iota(g_1, g_2)\theta^{-1}) \neq 0$  if and only if  $g(0_{2n} 1_{2n})\tau_i \iota(g_1, g_2)\theta^{-1} \equiv (0_{2n} 1_{2n}) \pmod{N}$ , i.e.,

$$g(0_{2n} 1_{2n})\tau_i \iota(g_1, g_2) \equiv (0_{2n} 1_{2n})\theta \pmod{N}.$$

Define  $\psi : M_{2n, 4n} \rightarrow M_{2n}$  by

$$\begin{pmatrix} a_{11} & a_{12} & b_{11} & b_{12} \\ c_{11} & c_{12} & d_{11} & d_{12} \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & b_{11} \\ c_{11} & d_{11} \end{pmatrix}.$$

The definition of  $\theta$  yields

$$\psi((0_{2n} 1_{2n})\theta) = \begin{pmatrix} 1_n & 0_n \\ 0_n & -1_n \end{pmatrix}.$$

Thus, we have that  $\psi((0_{2n}1_{2n})\theta)$  is a matrix of rank  $2n$  in  $M_{2n}(\mathbb{Q}_p)$ . However, a short calculation yields that

$$\psi(g(0_{2n}1_{2n})\tau_i\iota(g_1, g_2)) = g\psi((0_{2n}1_{2n})\tau_i)g_1$$

and

$$\psi((0_{2n}1_{2n})\tau_i) = \begin{pmatrix} 1_{n-i} & 0_i & 0_i & 0_i \\ 0_{n-i} & 1_i & 0_i & 0_i \\ 0_{n-i} & 0_i & 0_i & 0_i \\ 0_{n-i} & 0_i & 0_i & -1_i \end{pmatrix}.$$

Thus, the rank of  $\psi(g(0_{2n}1_{2n})\tau_i\iota(g_1, g_2))$  is at most  $n + i$ . Hence, for  $\psi(g(0_{2n}1_{2n})\tau_i\iota(g_1, g_2))$  to be congruent modulo  $N$  to  $(0_{2n}1_{2n})\theta$  we must have a matrix of rank at most  $n + i$  congruent modulo a proper ideal to a matrix of rank  $2n$ . This can only happen if  $i = n$ . Thus, we have shown that

$$\phi_p(g(0_{2n}1_{2n})\tau_i\iota(g_1, g_2)\theta^{-1}) = 0$$

unless  $i = n$ . This shows that  $\vartheta_i(g_1, g_2) = 0$  for all  $g_1, g_2 \in \mathrm{Sp}_{2n}(\mathbb{Q})$  unless  $i = n$ . Thus we have

$$E'(\iota(g_1, g_2)\theta^{-1}, k/2) = \sum_{\gamma \in I_n \setminus \iota(\mathrm{Sp}_{2n}(\mathbb{Q}) \times \mathrm{Sp}_{2n}(\mathbb{Q}))} \epsilon(\tau_n \gamma \iota(g_1, g_2)\theta^{-1}, k/2).$$

We are now in a position to show that  $E'(\iota(g_1, g_2)\theta^{-1}, k/2)$  is a cuspform in  $g_1$  ( $g_2$  respectively). We show here that  $E'(\iota(g_1, g_2)\theta^{-1}, k/2)$  is a cusp form in  $g_1$ . The argument to establish the result for  $g_2$  is the same argument and is omitted. Observe that we have

$$(4) \quad I_n = \{\iota(g_1, g_2) : g_2 = \hat{g}_1\} \cong \mathrm{Sp}_{2n}(\mathbb{Q})$$

where  $\hat{g} = \beta g \beta$  with  $\beta = \begin{pmatrix} -1_n & 0_n \\ 0_n & 1_n \end{pmatrix}$ . Thus, we can take  $\iota(\mathrm{Sp}_{2n}(\mathbb{Q}) \times \{1\})$  as a collection of representatives for  $I_n \setminus \iota(\mathrm{Sp}_{2n}(\mathbb{Q}) \times \mathrm{Sp}_{2n}(\mathbb{Q}))$ . This allows us to write

$$E'(\iota(g_1, g_2)\theta^{-1}, k/2) = \sum_{\gamma \in \mathrm{Sp}_{2n}(\mathbb{Q})} \epsilon(\tau_n \iota(\gamma g_1, g_2)\theta^{-1}, k/2).$$

We can unfold this sum along the unipotent radical as follows:

$$\begin{aligned} E'(\iota(g_1, g_2)\theta^{-1}, k/2) &= \sum_{\gamma \in \mathrm{Sp}_{2n}(\mathbb{Q})} \epsilon(\tau_n \iota(\gamma g_1, g_2)\theta^{-1}, k/2) \\ &= \sum_{\gamma \in \mathrm{Sp}_{2n}(\mathbb{Q})/U_{2n}(\mathbb{Q})} \sum_{u \in U_{2n}(\mathbb{Q})} \epsilon(\tau_n \iota(\gamma u g_1, g_2)\theta^{-1}, k/2) \\ &= \sum_{\gamma \in \mathrm{Sp}_{2n}(\mathbb{Q})/U_{2n}(\mathbb{Q})} \sum_{u \in U_{2n}(\mathbb{Q})} \epsilon(\tau_n \iota(u g_1, \hat{\gamma}^{-1} g_2)\theta^{-1}, k/2) \end{aligned}$$

where the last equality follows from the isomorphism in equation (4). We can expand the sum

$$\sum_{u \in U_{2n}(\mathbb{Q})} \epsilon(\tau \iota(u g_1, \hat{\gamma}^{-1} g_2)\theta^{-1}, k/2)$$

in its Fourier expansion in  $g_1$  along the unipotent radical. Since we are only interested here in showing cuspidality, it is enough to show that the  $\sigma$ -th Fourier coefficient is zero for all  $g_1, g_2 \in \mathrm{Sp}_{2n}(\mathbb{A})$  unless  $\sigma$  is totally positive definite. Recall the Fourier coefficient is given by

$$\int_{U_{2n}(\mathbb{Q}) \backslash U_{2n}(\mathbb{A})} \bar{\psi}(\mathrm{Tr}(\sigma g)) \sum_{u \in U_{2n}(\mathbb{Q})} \epsilon(\tau_n \iota(uu(g)g_1, g_2) \theta^{-1}, k/2) dg$$

where we recall that  $\psi$  is the standard additive character on  $\mathbb{A}/\mathbb{Q}$  given by  $x \mapsto e^{2\pi i x}$  on  $\mathbb{R}$  and is trivial on  $\mathbb{Z}_p$  for all  $p$ . We can fold this integral to obtain the collapsed integral given by

$$\int_{U_{2n}(\mathbb{A})} \bar{\psi}(\mathrm{Tr}(\sigma g)) \epsilon(\tau_n \iota(u(g)g_1, g_2) \theta^{-1}, k/2) dg.$$

We restrict ourselves now to looking at the infinite place as this is the place that forces the vanishing of the integral for  $\sigma$  not totally positive definite. Recall that  $\theta \in \mathrm{Sp}_{4n}(\mathbb{A}_f)$ , so when we look at the infinite place our integral becomes

$$(5) \quad \int_{U_{2n}(\mathbb{R})} \bar{\psi}(\mathrm{Tr}(\sigma g)) \epsilon_\infty(\tau_n \iota(u(g)g_1, g_2), k/2) dg.$$

It is enough to consider  $g_1$  and  $g_2$  of the form  $g_1 = Q(A_1)$ ,  $g_2 = u(x)Q(A_2)$ . This follows from the Iwasawa decomposition and the right  $(K(N), j^{-k})$ -equivariance of  $\epsilon_\infty$ . One can use the fact that  $\tau_n$  is of the form

$$\begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 1_n & 1_n & 0_n & 0_n \\ 0_n & 0_n & -1_n & 1_n \end{pmatrix}$$

to calculate

$$\tau_n \iota(u(g)g_1, g_2) = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ A_1 & A_2 & g {}^t A_1^{-1} & x {}^t A_2^{-1} \\ 0 & 0 & -{}^t A_1^{-1} & {}^t A_2^{-1} \end{pmatrix}$$

where we use a  $*$  to indicate that we are not interested in this entry of the matrix. We now make the observation that for any  $g \in \mathrm{Sp}_{4n}(\mathbb{R})$ , one has  $\epsilon_\infty(g, k/2) = \chi(\det A_g) j(g, i)^{-k}$  where  $g = u(x_g)Q(A_g)k_g$ . This follows immediately from the definition of  $\epsilon_\infty$  and the fact that  $j(g, i)^{-k} = |\det A_g|^k j(k_g, i)^{-k}$ . Applying this to our current situation we have

$$\epsilon_\infty(\tau_n \iota(u(g)g_1, g_2), k/2) = \chi(\det \tilde{A}) \det \left( i \begin{pmatrix} A_1 & A_2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} g {}^t A_1^{-1} & x {}^t A_2^{-1} \\ -{}^t A_1^{-1} & {}^t A_2^{-1} \end{pmatrix} \right)^{-k}$$

where we write  $\tilde{A} = A_{\tau_n \iota(u(g)g_1, g_2)}$  to ease the notation. Observe that we have

$$i \begin{pmatrix} A_1 & A_2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} g {}^t A_1^{-1} & x {}^t A_2^{-1} \\ -{}^t A_1^{-1} & {}^t A_2^{-1} \end{pmatrix} = \begin{pmatrix} iA_1 {}^t A_1 + g & iA_2 {}^t A_2 + x \\ -1 & 1 \end{pmatrix} \begin{pmatrix} {}^t A_1^{-1} & 0 \\ 0 & {}^t A_2^{-1} \end{pmatrix}.$$

We now recall the formula that if  $D^{-1}$  exists then we have

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det D \det(A - BD^{-1}C).$$

This follows immediately from the identity

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 1 & BD^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A - BD^{-1}C & 0 \\ C & D \end{pmatrix}.$$

Thus, we have

$$\begin{aligned} \epsilon_\infty(\tau_n \iota(u(g)g_1, g_2), k/2) &= \chi(\det \tilde{A})(\det A_1 \det A_2)^{-1} \det(g + x + iA_1 {}^t A_1 + iA_2 {}^t A_2)^{-k} \\ &= \chi(\det \tilde{A})(\det A_1 \det A_2)^{-1} \det(g + z)^{-k} \end{aligned}$$

where  $z \in \mathfrak{h}^n$ . Thus, the integral in equation (5) is equal to

$$\chi(\det \tilde{A})(\det A_1 \det A_2)^{-1} \int_{U_{2n}(\mathbb{R})} \bar{\psi}(\mathrm{Tr}(\sigma g)) \det(g + z)^{-k} dg = 0$$

unless  $\sigma$  is totally positive definite. This last equality is a result due to Siegel. Thus, we have that  $E'(\iota(g_1, g_2)\theta^{-1}, k/2)$  is a holomorphic cuspform in  $g_1$ . Similarly, we have it is a holomorphic cuspform in  $g_2$  as well. Combining this with our previous discussion relating  $E(\iota(g_1, g_2), (n+1)/2 - k/2)$  to  $E'(\iota(g_1, g_2)\theta^{-1}, k/2)$ , we see that  $E(\iota(g_1, g_2), (n+1)/2 - k/2)$  is a holomorphic cuspform in  $g_1$  (respectively,  $g_2$ .)

**3.3. Pullbacks and an inner product relation.** In this section we summarize a result of Shimura giving the inner product between a cuspidal Siegel eigenform and the pullback of the Siegel Eisenstein series. See [Sh95] for a detailed treatment of this material. We specialize to the case of  $\mathrm{Sp}_4 \times \mathrm{Sp}_4$  embedded in  $\mathrm{Sp}_8$  as this will be the case for which we apply the result.

Let  $\sigma \in \mathrm{Sp}_8(\mathbb{A}_f)$  be defined by

$$\sigma_\ell = \begin{cases} I_8 & \text{if } \ell \nmid N \\ \begin{pmatrix} I_4 & 0_4 \\ \begin{pmatrix} 0_2 & I_2 \\ I_2 & 0_2 \end{pmatrix} & I_4 \end{pmatrix} & \text{if } \ell \mid N. \end{cases}$$

Strong approximation gives an element  $\rho \in \mathrm{Sp}_8(\mathbb{Q})$  so that  $E|_\rho(Z, s)$  corresponds to  $E(g\sigma^{-1}, s)$ .

Let  $F \in \mathcal{S}_k(\Gamma_0^4(N))$  be a Siegel eigenform. Applying ([Sh95], equation (6.17)) to our situation we obtain

$$(6) \quad \langle D_{E|_\rho}(\mathrm{diag}[Z, W], (5-k)/2), (F|_\varsigma)^c(W) \rangle = \pi^{-3} \mathcal{A}_{k,N} L_{\mathrm{st}}^\Sigma(5-k, F, \chi) F(Z)$$

where  $D_{E|_\rho}$  is the normalized Eisenstein series as defined in equation (3),  $\mathcal{A}_{k,N} = \frac{(-1)^k 2^{2k-3} v_N}{3 [\mathrm{Sp}_4(\mathbb{Z}) : \Gamma_0^4(N)]}$ ,  $v_N = \pm 1$ ,  $L_{\mathrm{st}}^\Sigma(5-k, F, \chi)$  is the standard zeta function as defined in equation (1), and  $(F|_\varsigma)^c$  denotes taking the complex conjugates of the Fourier coefficients of  $F|_\varsigma$ .

## 4. THE SAITO-KUROKAWA CORRESPONDENCE

The Saito-Kurokawa correspondence is a well known result with several excellent references for the basic facts ([EZ85], [Geer], [Z80]). For the facts we will be interested in, the reader is advised to consult the section on Saito-Kurokawa lifts in [Br07]. Here we will briefly recall the Saito-Kurokawa correspondence and state some necessary facts, but omit a lengthy discussion preferring to point unfamiliar readers to the appropriate references.

Let  $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}), \mathcal{O})$  be a newform with Fourier coefficients in a ring  $\mathcal{O}$ . The Saito-Kurokawa correspondence associates to  $f$  a cuspidal Siegel eigenform  $F_f$  in the Maass specialchars  $\mathcal{S}_k^{\mathrm{M}}(\mathrm{Sp}_4(\mathbb{Z}))$ . This correspondence is achieved via a set of isomorphisms, the first being between  $S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$  and  $S_{k-1/2}^+(\Gamma_0(4))$ . The isomorphism from Kohnen's +-space of half-integral weight modular forms to  $S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$  is given by sending

$$g(z) = \sum_{\substack{n \geq 1 \\ (-1)^{k-1} n \equiv 0, 1 \pmod{4}}} c_g(n) q^n \in S_{k-1/2}^+(\Gamma_0(4))$$

to

$$\zeta_D g(z) = \sum_{n=1}^{\infty} \left( \sum_{d|n} \left( \frac{D}{d} \right) d^{k-2} c_g(|D|n^2/d^2) \right) q^n$$

where  $D$  is a fundamental discriminant with  $(-1)^{k-1}D > 0$ . The second isomorphism is between  $J_{k,1}^{\mathrm{cusp}}(\mathrm{SL}_2(\mathbb{Z}) \times \mathbb{Z}^2)$  and  $S_{k-1/2}^+(\Gamma_0(4))$  via the map

$$\sum_{\substack{D < 0, r \in \mathbb{Z} \\ D \equiv r^2 \pmod{4}}} c(D, r) e\left(\frac{r^2 - D}{4}\tau + rz\right) \mapsto \sum_{\substack{D < 0 \\ D \equiv 0, 1 \pmod{4}}} c(D) e(|D|\tau).$$

Finally, we obtain an isomorphism between  $J_{k,1}^{\mathrm{cusp}}(\mathrm{SL}_2(\mathbb{Z}) \times \mathbb{Z}^2)$  and the space of Maass specialchars  $\mathcal{S}_k^{\mathrm{M}}(\mathrm{Sp}_4(\mathbb{Z}))$  given by

$$\phi(\tau, z) \mapsto F(\tau, z, \tau') = \sum_{m \geq 0} V_m \phi(\tau, z) e(m\tau')$$

where  $V_m$  is the index shifting operator as defined in ([EZ85], Section 4). We will need that the Fourier coefficients of the form  $F$  arising from  $\phi(\tau, z)$  are related to the Fourier coefficients of  $\phi$  by

$$A_F(n, r, m) = \sum_{d|\mathrm{gcd}(m, m, r)} d^{k-1} c_\phi\left(\frac{4nm - r^2}{d^2}, \frac{r}{d}\right).$$

We recall that we write  $\mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z}))$  for the orthogonal complement to  $\mathcal{S}_k^{\mathrm{M}}(\mathrm{Sp}_4(\mathbb{Z}))$  in  $\mathcal{S}_k(\mathrm{Sp}_4(\mathbb{Z}))$  and refer to this as the space of non-Maass forms. The Saito-Kurokawa correspondence is stated in the following theorem.

**Theorem 4.1.** ([Z80]) *There is a Hecke-equivariant isomorphism between  $S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$  and  $\mathcal{S}_k^{\mathrm{M}}(\mathrm{Sp}_4(\mathbb{Z}))$  such that if  $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$  is a newform, then one has*

$$(7) \quad L_{\mathrm{spin}}(s, F_f) = \zeta(s-k+1)\zeta(s-k+2)L(s, f).$$

As our applications of the Saito-Kurokawa correspondence will be in terms of arithmetic data, we also need the follow two results.

**Corollary 4.2.** ([Br07], Corollary 3.8) *Given  $f \in S_k(\mathrm{SL}_2(\mathbb{Z}), \mathcal{O})$  a newform, then  $F_f$  also has Fourier coefficients in  $\mathcal{O}$ . In particular, if  $\mathcal{O}$  is a discrete valuation ring,  $F_f$  has a Fourier coefficient in  $\mathcal{O}^\times$ .*

**Corollary 4.3.** *Let  $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$  and  $F_f$  the Saito-Kurokawa lift of  $f$ . One has that  $F_f^c = F_{f^c}$ . In other words, the Saito-Kurokawa correspondence respects complex conjugation of Fourier coefficients.*

*Proof.* This is straightforward by viewing the lift through the isomorphisms described above. For example, if we let  $g_f$  denote the half-integral weight modular form corresponding to  $f$ , then just observe that  $g_f^c$  maps to  $f^c$  under the given isomorphism, as does  $g_{f^c}$ . Thus, we must have  $g_{f^c} = g_f^c$ . The others are even more obvious.  $\square$

We will also make use of the following three results.

**Theorem 4.4.** ([KS89], [KZ81]) *Let  $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$  be a newform,  $F_f \in \mathcal{S}_k^{\mathrm{M}}(\mathrm{Sp}_4(\mathbb{Z}))$  the corresponding Saito-Kurokawa lift, and  $g(z) = \sum c_g(n)q^n$  the weight  $k-1/2$  cusp form corresponding to  $f$ . We have the following inner product relation*

$$\langle F_f, F_f \rangle = \frac{(k-1)}{2^5 3^2 \pi} \cdot \frac{c_g(|D|)^2}{|D|^{k-3/2}} \cdot \frac{L(k, f)}{L(k-1, f, \chi_D)} \langle f, f \rangle$$

where  $D$  is a fundamental discriminant so that  $(-1)^{k-1}D > 0$  and  $\chi_D$  is the character associated to the field  $\mathbb{Q}(\sqrt{D})$ .

**Theorem 4.5.** ([Br07], Theorem 3.10) *Let  $N$  be a positive integer,  $\Sigma$  the set of primes dividing  $N$ , and  $\chi$  a Dirichlet character of conductor  $N$ . Let  $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$  be a newform and  $F_f$  the corresponding Saito-Kurokawa lift of  $f$ . The standard zeta function of  $F_f$  factors as*

$$L_{\mathrm{st}}^\Sigma(2s, F_f, \chi) = L^\Sigma(2s-2, \chi)L^\Sigma(2s+k-3, f, \chi)L^\Sigma(2s+k-4, f, \chi).$$

**Proposition 4.6.** *Let  $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$  be a newform,  $\rho_f$  the associated  $\ell$ -adic Galois representation,  $F_f$  the Saito-Kurokawa lift, and  $\rho_{F_f}$  the associated 4-dimensional  $\ell$ -adic Galois representation. Then one has*

$$\rho_{F_f} = \begin{pmatrix} \varepsilon^{k-2} & & & \\ & \rho_f & & \\ & & \varepsilon^{k-1} & \\ & & & \end{pmatrix}$$

where  $\varepsilon$  is the  $\ell$ -adic cyclotomic character and blank spaces in the matrix are assumed to be 0's of the appropriate size.

*Proof.* This fact is used in [Br07], though not formally stated as a proposition there. It follows directly from the decomposition of the Spinor  $L$ -function of  $F_f$ , the fact that  $\rho_{F_f}$  is necessarily semi-simple, and the Brauer-Nesbitt theorem.  $\square$

## 5. CONGRUENCES BETWEEN SAITO-KUROKAWA LIFTS AND NON-MAASS FORMS

In this section we will use the results obtained in § 3 as well as arguments originally used in [Br07] to produce a congruence between a Saito-Kurokawa lift  $F_f$  and a form  $G \in \mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$ . This congruence will provide the foundation for providing the lower bound on the size of the appropriate Selmer group in § 8.

Let  $k > 3$  be an integer and  $p$  a prime so that  $p > 2k - 2$  and  $\gcd(p, N) = 1$ . Let  $E$  be a finite extension of  $\mathbb{Q}_p$  with ring of integers  $\mathcal{O}$  and uniformizer  $\varpi$ . We fix an embedding of  $E$  into  $\mathbb{C}$  that is compatible with the embeddings fixed in section 2. Let  $\mathfrak{p}$  be the prime of  $\mathcal{O}$  lying over  $p$ .

Given two Siegel modular forms  $F$  and  $G$ , we write  $F \equiv G \pmod{\varpi^m}$  to mean that  $\text{ord}_{\varpi}(A_F(T) - A_G(T)) \geq m$  for all  $T$ . If  $F$  and  $G$  are Hecke eigenforms, we denote a congruence between the eigenvalues as  $F \equiv_{\text{ev}} G \pmod{\varpi^m}$ .

Let  $f \in S_{2k-2}(\text{SL}_2(\mathbb{Z}))$  be a newform and  $F_f$  the Saito-Kurokawa lift of  $f$ . As in [Br07], we begin by replacing the normalized Eisenstein series  $D_{E|\rho}(\text{diag}[Z, W], (5-k)/2)$  by its trace so as to work with level 1. Write

$$\mathcal{E}(Z, W) = \sum_{\gamma \times \delta \in (\text{Sp}_4(\mathbb{Z}) \times \text{Sp}_4(\mathbb{Z})) / (\Gamma_0^4(N) \times \Gamma_0^4(N))} (D_{E|\rho})|_{\gamma \times \delta}(\text{diag}[Z, W], (5-k)/2).$$

We then have that  $\mathcal{E}(Z, W)$  is a Siegel cusp form of weight  $k$  and level 1 in each variable separately. In addition, one sees that the coefficients of  $\mathcal{E}(Z, W)$  remain in  $\mathbb{Z}_p[\chi]$  by an application of the  $q$ -expansion principle for Siegel modular forms ([CF80], Proposition 1.5).

Let  $f_0 = f, f_1, \dots, f_m$  be an orthogonal basis of newforms for  $S_{2k-2}(\text{SL}_2(\mathbb{Z}))$  and let  $F_0 = F_f, F_1 = F_{f_1}, \dots, F_m = F_{f_m}, F_{m+1}, \dots, F_r$  be an orthogonal basis of eigenforms of  $\mathcal{S}_k(\text{Sp}_4(\mathbb{Z}))$ . Note we are implicitly using Corollary 4.3 and Theorem 4.4 here. We enlarge  $E$  here if necessary so that both of the bases are defined over  $\mathcal{O}$  and  $\mathcal{O}$  contains the values of  $\chi$ . We write

$$\mathcal{E}(Z, W) = \sum_{i,j} c_{i,j} F_i(Z) F_j^c(W)$$

for some  $c_{i,j} \in \mathbb{C}$ . The reader is urged to see ([Sh83], Lemma 1.1) or [G84] for the general principles of such expansions. In [Br07] the assumption was made that  $f$  have real Fourier coefficients to remove the complex conjugation from the formulas. Though this assumption will eventually be necessary, we do not immediately make it. This adds some minor complexity to the argument, but provides a much better picture of why the assumption is necessary for the method and is not just one made out of convenience.

**Proposition 5.1.** *With the notation as above, we have*

$$(8) \quad \mathcal{E}(Z, W) = \sum_{0 \leq i \leq r} c_{i,i} F_i(Z) F_i^c(W),$$

*i.e.,  $c_{i,j} = 0$  unless  $i = j$ . In particular, one has*

$$c_{i,i} = \frac{\mathcal{A}_{k,N} L_{\text{st}}^{\Sigma}(5-k, F_i, \chi)}{\pi^3 \langle F_i^c, F_i^c \rangle}.$$

*Proof.* Fix  $j_0$  with  $0 \leq j_0 \leq r$  and consider the inner product  $\langle \mathcal{E}(Z, W), F_{j_0}^c(W) \rangle$ . Using the orthogonality of the basis we have

$$(9) \quad \langle \mathcal{E}(Z, W), F_{j_0}^c(W) \rangle = \sum_{0 \leq i \leq r} c_{i,j_0} \langle F_{j_0}^c, F_{j_0}^c \rangle F_i(Z).$$

On the other hand, combining the facts that

$$\langle \mathcal{E}(Z, W), F_f^c(W) \rangle_{\text{Sp}_4(\mathbb{Z})} = \langle D_{E|\rho}(\text{diag}[Z, W], (5-k)/2), F_f^c(W) \rangle_{\Gamma_0^4(N)}$$

and  $F_f|_{\varsigma} = F_f$  since  $F_f$  is of full level with equation (6) gives

$$\langle \mathcal{E}(Z, W), F_{j_0}^c(W) \rangle = \pi^{-3} \mathcal{A}_{k,N} L_{\text{st}}^{\Sigma}(5-k, F_{j_0}, \chi) F_{j_0}(Z).$$

Combining this with equation (9) and using that the  $F_i$  form a basis allows us to conclude that  $c_{i,j_0} = 0$  unless  $i = j_0$  and if  $i = j_0$  we have

$$c_{j_0,j_0} = \frac{\mathcal{A}_{k,N} L_{\text{st}}^{\Sigma}(5-k, F_{j_0}, \chi)}{\pi^3 \langle F_{j_0}^c, F_{j_0}^c \rangle}.$$

Since  $j_0$  was arbitrary, we have

$$\mathcal{E}(Z, W) = \sum_{0 \leq i \leq r} c_{i,i} F_i(Z) F_i^c(W)$$

with the  $c_{i,i}$  as desired.  $\square$

As our goal is to produce a congruence between  $F_f$  and a Siegel cusp form that is not a CAP form, the first step is a theorem which allows us to kill all of  $F_i$  with  $1 \leq i \leq m$ . First we need the following result giving the existence of complex periods.

**Theorem 5.2.** ([Sh77], *Theorem 1*) *Let  $f \in S_{2k-2}(\text{SL}_2(\mathbb{Z}), \mathcal{O})$  be a newform. There exist complex periods  $\Omega_f^{\pm}$  such that for each integer  $m$  with  $0 < m < 2k-2$  and every Dirichlet character  $\chi$  one has*

$$\frac{L(m, f, \chi)}{\tau(\chi)(2\pi i)^m} \in \begin{cases} \Omega_f^- \mathcal{O}_{\chi} & \text{if } \chi(-1) = (-1)^m, \\ \Omega_f^+ \mathcal{O}_{\chi} & \text{if } \chi(-1) = (-1)^{m-1}, \end{cases}$$

where  $\tau(\chi)$  is the Gauss sum of  $\chi$  and  $\mathcal{O}_{\chi}$  is the extension of  $\mathcal{O}$  generated by the values of  $\chi$ . We write  $L_{\text{alg}}(m, f, \chi)$  to denote the value  $\frac{L(m, f, \chi)}{\tau(\chi)(2\pi i)^m}$ .

The theorem we will use to kill the  $F_i$  for  $1 \leq i \leq m$  is as follows.

**Theorem 5.3.** ([Br07], *Theorem 5.4*) *Let  $f = f_0, f_1, \dots, f_m$  be a basis of newforms of  $S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}), \mathcal{O})$  with  $k > 2$ . Suppose that the residual Galois representation  $\bar{\rho}_f$  is irreducible and  $f$  is ordinary at  $\mathfrak{p}$ . There exists a Hecke operator  $t \in \mathbb{T}_{\mathcal{O}}$  such that*

$$tf_i = \begin{cases} \alpha f & \text{if } i = 0, \\ 0 & \text{if } 1 \leq i \leq m, \end{cases}$$

where  $\alpha = \frac{u\langle f, f \rangle}{\Omega_f^+ \Omega_f^-}$ ,  $u$  is a unit in  $\mathcal{O}$ .

From this point on we assume that  $f$  is ordinary at  $\mathfrak{p}$  and  $\bar{\rho}_f$  is irreducible so we are able to apply this theorem. We write  $F \equiv G \pmod{\varpi^n}$  to indicate that  $\mathrm{ord}_{\varpi}(A_F(T) - A_G(T)) \geq n$  for all  $T$ , i.e., the congruence is a congruence of Fourier coefficients.

Applying the fact that the Saito-Kurokawa correspondence is Hecke-equivariant we are able to conclude there exists  $t^S \in \mathbb{T}_{\mathcal{O}}^S$  so that

$$t^S F_i = \begin{cases} \alpha F_0 & \text{if } i = 0, \\ 0 & \text{if } 1 \leq i \leq m. \end{cases}$$

Applying  $t^S$  to equation (8) we obtain

$$(10) \quad t^S \mathcal{E}(Z, W) = \alpha c_{0,0} F_0(Z) F_0^c(W) + \sum_{m < j \leq r} c_{j,j} t^S F_j(Z) F_j^c(W).$$

Before we study  $\mathrm{ord}_{\varpi}(\alpha c_{0,0})$ , we show how it ‘‘controls’’ a congruence between  $F_0 = F_f$  and a non-CAP eigenform.

Suppose we can have  $\mathrm{ord}_{\varpi}(\alpha c_{0,0}) = M < 0$ , i.e., there exists a  $\varpi$ -unit  $\beta$  so that  $\alpha c_{0,0} = \varpi^M \beta$ . Corollary 4.2 gives that there exists a  $T_0$  so that  $\varpi \nmid A_{F_0^c}(T_0)$ . We claim that this implies that  $c_{i,i} \neq 0$  for at least one  $i$  with  $i > 0$ . If not, we would have

$$t^S \mathcal{E}(Z, W) = \varpi^M \beta F_0(Z) F_0^c(W).$$

However, since  $\mathcal{E}(Z, W)$  has  $\varpi$ -integral Fourier coefficients,  $t^S \mathcal{E}(Z, W)$  does as well. Thus, upon multiplying both sides of the equation by  $\varpi^{-M}$  we obtain that  $F_0(Z) F_0^c(W) \equiv 0 \pmod{\varpi}$ , clearly a contradiction.

We now expand each side of equation (10) in terms of  $W$ , reduce modulo  $\varpi$ , and equate  $T_0^{\mathrm{th}}$  Fourier coefficients. The  $\mathcal{O}$ -integrality of the Fourier coefficients of  $t^S \mathcal{E}(Z, W)$  combined with the fact that  $M < 0$  gives

$$F_0(Z) \equiv -\frac{\varpi^{-M}}{A_{F_0^c}(T_0)\beta} \sum_{m < j \leq r} c_{j,j} A_{F_j^c}(T_0) t^S F_j(Z) \pmod{\varpi^{-M}}.$$

Set

$$G = -\frac{\varpi^{-M}}{A_{F_0^c}(T_0)\beta} \sum_{m < j \leq r} c_{j,j} A_{F_j^c}(T_0) t^S F_j(Z).$$

First, we note that if  $G \equiv 0 \pmod{\varpi^{-M}}$  we obtain a contradiction to Corollary 4.2, so we must have a nontrivial congruence. Secondly, since all of the

$F_j$ 's with  $m < j \leq r$  lie in  $\mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$  and as we noted earlier this space is stable under Hecke operators, we have that  $t^S F_j$  is in  $\mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$  for  $m < j \leq r$ . As  $G$  is a linear combination of forms in  $\mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$ , we must have  $G \in \mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$ . Thus, if we show that  $\text{ord}_\varpi(\alpha c_{0,0})$  is less than 0, we have a nontrivial congruence between  $F_f$  and a form in  $\mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$ , in particular, between a Saito-Kurokawa lift and a non-Saito-Kurokawa lift.

Our discussion of  $\alpha c_{0,0}$  will be brief as most of the work done in [Br07] applies verbatim to this situation. Corollary 4.3 allows us to apply Theorem 4.4 to  $\langle F_0^c, F_0^c \rangle$  as this is  $\langle F_{f^c}, F_{f^c} \rangle$ . Following the same argument as in [Br07] we are able to conclude that

$$\alpha c_{0,0} = \mathcal{B}_{k,N,D,\chi} \mathcal{L}(k, f, D, \chi) \frac{\langle f, f \rangle}{\langle f^c, f^c \rangle}$$

where

$$\mathcal{L}(k, f, D, \chi) = \frac{L^\Sigma(3-k, \chi) L_{\text{alg}}(k-1, f^c, \chi_D) L_{\text{alg}}(1, f, \chi) L_{\text{alg}}(2, f, \chi)}{L_{\text{alg}}(k, f^c)}$$

and

$$\mathcal{B}_{k,N,D,\chi} = \frac{(-1)^{k+1} 2^{2k+4} 3u |D|^k \tau(\chi_D) \tau(\chi)^2}{(k-1) [\text{Sp}_2(\mathbb{Z}) : \Gamma_0^2(N)] |D|^{3/2} |c_{g_{f^c}}(|D|)|^2 L_\Sigma(1, f, \chi) L_\Sigma(2, f, \chi)}$$

where  $D$  is a fundamental discriminant so that  $\chi_D(-1) = -1$ . It was shown in [Br07] that as long as  $\gcd(p, D[\text{Sp}_4(\mathbb{Z}) : \Gamma_0^4(N)]) = 1$  one has  $\text{ord}_\varpi(\mathcal{B}_{k,N,D,\chi}) \leq 0$ . Thus, we would be able to get a divisibility condition on  $L$ -functions associated to  $f$  guaranteeing the existence of the congruence if not for the factor  $\frac{\langle f, f \rangle}{\langle f^c, f^c \rangle} = \frac{\langle f, f \rangle}{\langle f, f \rangle^c}$  ([Sh76], Lemma 4). Unfortunately, we do not even know in general if this quantity is algebraic! However, if we assume that  $f$  has Fourier coefficients lying in  $\mathbb{R}$ , then this term is 1 and so does not cause any further issues. In that case, we have the following theorem.

**Theorem 5.4.** *Let  $k > 3$  be an integer and  $p$  a prime so that  $p > 2k - 2$ . Let  $f \in S_{2k-2}(\text{SL}_2(\mathbb{Z}), \mathcal{O})$  be a newform with real Fourier coefficients and  $F_f$  the Saito-Kurokawa lift of  $f$ . Let  $f$  be ordinary at  $p$  and  $\bar{\rho}_f$  be irreducible. If there exists  $N > 1$ , a fundamental discriminant  $D$  so that  $(-1)^{k-1} D > 0$ ,  $\chi_D(-1) = -1$ ,  $p \nmid ND[\text{Sp}_4(\mathbb{Z}) : \Gamma_0^4(N)]$ , and a Dirichlet character  $\chi$  of conductor  $N$  so that*

$$-M = \text{ord}_\varpi(\mathcal{L}(k, f, D, \chi)) < 0$$

*then there exists  $G \in \mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$  so that*

$$F_f \equiv G \pmod{\varpi^M}.$$

We repeat Lemma 6.4 of [Br07] here for completeness, though it will not be needed.

**Lemma 5.5.** *With the set-up as in Theorem 5.4, there exists an eigenform  $F \in \mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$  so that  $F_f \equiv_{\text{ev}} F \pmod{\varpi}$ .*

*Proof.* Let  $G$  be as in Theorem 5.4. The Hecke algebra  $\mathbb{T}_{\mathcal{O}}^S$  decomposes as

$$\mathbb{T}_{\mathcal{O}}^S \cong \prod \mathbb{T}_{\mathcal{O},\mathfrak{m}}^S$$

where the product is over the maximal ideals of  $\mathbb{T}_{\mathcal{O}}^S$  containing  $\varpi$ . Write  $\mathfrak{m}_{F_f}$  for the maximal ideal corresponding to  $F_f$ , i.e.,  $\mathfrak{m}_{F_f}$  is the kernel of the  $\mathcal{O}$ -algebra homomorphism  $\lambda_{F_f} : \mathbb{T}_{\mathcal{O}}^S \rightarrow \mathcal{O}$  sending  $t$  to the eigenvalue of  $t$  acting on  $F_f$ . The decomposition gives that there exists a Hecke operator  $t \in \mathbb{T}_{\mathcal{O}}^S$  so that  $tF_f = F_f$  and  $tF = 0$  if  $F$  does not correspond to the ideal  $\mathfrak{m}_{F_f}$ , i.e., if  $F \not\equiv_{\text{ev}} F_f \pmod{\varpi}$ .

Write  $G = \sum c_i F_i$ . By construction, the only  $F_i$  that appear are in  $\mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$ . Applying the Hecke operator  $t$  to  $G$  we see that  $F_f \equiv tG \pmod{\varpi}$  and so  $tG \not\equiv 0 \pmod{\varpi}$ . Thus, there is an eigenform  $F \in \mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$  so that  $F_f \equiv_{\text{ev}} F \pmod{\varpi}$  as claimed.  $\square$

We close this section by phrasing our results in terms of the CAP ideal ([KK07]). This ideal can be thought of as a generalization of the Eisenstein ideal to our situation. As the Eisenstein ideal measures congruences between Eisenstein series, the CAP ideal measures congruences between  $F_f$  and non-CAP modular forms.

Let  $\mathbb{T}_{\mathcal{O}}^{\text{NM}}$  denote the image of  $\mathbb{T}_{\mathcal{O}}^S$  inside of  $\text{End}_{\mathbb{C}}(\mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z})))$ . Let  $\phi : \mathbb{T}_{\mathcal{O}}^S \rightarrow \mathbb{T}_{\mathcal{O}}^{\text{NM}}$  denote the canonical  $\mathcal{O}$ -algebra surjection. Denote the annihilator of  $F_f$  in  $\mathbb{T}_{\mathcal{O}}^S$  by  $\text{Ann}(F_f)$ . The annihilator of  $F_f$  in  $\mathbb{T}_{\mathcal{O}}^S$  is a prime ideal and one has that the map  $\lambda_{F_f}$  induces an  $\mathcal{O}$ -algebra isomorphism

$$\mathbb{T}_{\mathcal{O}}^S / \text{Ann}(F_f) \cong \mathcal{O}.$$

As the map  $\phi$  is surjective, one has that  $\phi(\text{Ann}(F_f))$  is an ideal in  $\mathbb{T}_{\mathcal{O}}^{\text{NM}}$ . We call this ideal the *CAP ideal associated to  $F_f$* .

One has that there exists an  $r \in \mathbb{Z}_{\geq 0}$  so that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{T}_{\mathcal{O}}^S & \xrightarrow{\phi} & \mathbb{T}_{\mathcal{O}}^{\text{NM}} \\ \downarrow & & \downarrow \\ \mathbb{T}_{\mathcal{O}}^S / \text{Ann}(F_f) & \xrightarrow{\phi} & \mathbb{T}_{\mathcal{O}}^{\text{NM}} / \phi(\text{Ann}(F_f)) \\ \downarrow \lambda_{F_f} & & \downarrow \simeq \\ \mathcal{O} & \longrightarrow & \mathcal{O} / \varpi^r \mathcal{O}. \end{array}$$

Note that all of the maps in the above diagram are  $\mathcal{O}$ -algebra surjections.

**Corollary 5.6.** *With  $r$  as in the diagram above and  $M$  as in Theorem 5.4 we have  $r \geq M$ .*

*Proof.* Let  $G$  be as in Theorem 5.4. Choose a  $t \in \phi^{-1}(\varpi^r) \subset \mathbb{T}_{\mathcal{O}}^S$ . Note that this means that  $tG = \varpi^r G$ . We also have by the commutativity of

the diagram that  $t \in \text{Ann}(F_f)$  and so the congruence in Theorem 5.4 gives  $\varpi^r G \equiv 0 \pmod{\varpi^M}$ , i.e.,

$$G \equiv 0 \pmod{\varpi^{M-r}}.$$

Now assume that  $r < M$ . The fact that  $F_f \equiv G \pmod{\varpi^M}$  and  $G \equiv 0 \pmod{\varpi}$  imply that

$$F_f \equiv 0 \pmod{\varpi}.$$

However, this is impossible and so we must have  $r \geq M$  as claimed.  $\square$

## 6. RESIDUALLY REDUCIBLE REPRESENTATIONS AND LATTICES

In this section we construct the lattice we will use in section 8 to give a lower bound on the appropriate Selmer group. Our main result here is a generalization of Theorem 1.1 of [U01]. Where his result deals with the case of  $\bar{\rho}^{\text{ss}}$  splitting into two irreducible representations, our results are for when  $\bar{\rho}^{\text{ss}}$  splits into three irreducible representations. The proofs given here are adapted from those in [U01] to our situation. As Theorem 1.1 of [U01] is a variant of the main result of [U99], our result here is very much a variant of the main result of [Br08]. The results contained in this section or some alternative version of them will also appear in [SU].

Let  $\mathcal{O}$  be a discrete valuation ring and  $\mathcal{R}$  a reduced local commutative algebra that is finite over  $\mathcal{O}$  and is Henselian. Let  $\mathfrak{m}_{\mathcal{R}}$  be the maximal ideal of  $\mathcal{R}$  and  $\kappa_{\mathcal{R}}$  the residue field. We use the fact that  $\mathcal{R}$  is reduced to embed it into a product of its irreducible components

$$\mathcal{R} \subset \tilde{\mathcal{R}} = \prod_{\wp} \mathcal{O}_{\wp} \subset \prod_{\wp} F_{\wp} = F_{\mathcal{R}}$$

where  $F_{\wp}$  is the field of fractions of  $\mathcal{O}_{\wp}$ . Let  $\mathfrak{m}_{\wp}$  be the maximal ideal of  $\mathcal{O}_{\wp}$  and  $\kappa_{\wp}$  the residue field.

Let  $M_{F_{\mathcal{R}}}$  be a finite free  $F_{\mathcal{R}}$ -module and let  $\mathcal{L}$  be a  $\mathcal{R}$ -submodule of  $M_{F_{\mathcal{R}}}$ . We say  $\mathcal{L}$  is a  $\mathcal{R}$ -lattice if  $\mathcal{L}$  is finite over  $\mathcal{R}$  and  $\mathcal{L} \otimes_{\mathcal{R}} F_{\mathcal{R}} = M_{F_{\mathcal{R}}}$ .

**Theorem 6.1.** *Let  $\mathcal{A}$  be a  $\mathcal{R}$ -algebra and let  $\rho$  be an absolutely irreducible representation of  $\mathcal{A}$  on  $F_{\mathcal{R}}^n$ . Suppose there are at least  $n$  distinct elements in  $\kappa_{\mathcal{R}}^{\times}$  and suppose that there exist three representations  $\rho_i$  for  $1 \leq i \leq 3$  in  $M_{n_i}(\mathcal{R})$  and  $I \subset \mathcal{R}$  a proper ideal of  $\mathcal{R}$  such that*

- (1) *the coefficients of the characteristic polynomial of  $\rho$  belong to  $\mathcal{R}$ ;*
- (2) *the characteristic polynomials of  $\rho$  and  $\rho_1 \oplus \rho_2 \oplus \rho_3$  are congruent modulo  $I$ ;*
- (3) *the residual representations  $\bar{\rho}_i$  are absolutely irreducible for  $1 \leq i \leq 3$ ;*
- (4)  *$\bar{\rho}_i \neq \bar{\rho}_j$  if  $i \neq j$ .*

*Then there exists an  $\mathcal{A}$ -stable  $\mathcal{R}$ -lattice  $\mathcal{L}$  in  $F_{\mathcal{R}}^n$  and  $\mathcal{R}$ -lattices  $\mathcal{T}_1, \mathcal{T}_2$  of  $F_{\mathcal{R}}$  such that we have the following exact sequence of  $\mathcal{A}$ -modules:*

$$0 \longrightarrow \mathcal{N}_1 \oplus \mathcal{N}_2 \longrightarrow \mathcal{L} \otimes \mathcal{R}/I \xrightarrow{\quad s \quad} \rho_3 \otimes \mathcal{R}/I \longrightarrow 0,$$

where  $\mathcal{N}_i = \rho_i \otimes \mathcal{T}_i/I\mathcal{T}_i$  for  $i = 1, 2$  and  $s$  is a section (though only of  $\mathcal{R}/I$ -modules.) Moreover,  $\mathcal{L}$  has no quotient isomorphic to a representation  $\bar{\rho}'$  with  $\bar{\rho}'^{\text{ss}} = \bar{\rho}_1 \oplus \bar{\rho}_2$ .

Let  $\rho_\varphi : \mathcal{A} \rightarrow M_n(F_\varphi)$  be the representation arising from  $\rho$  via the projection  $F_{\mathcal{R}} \rightarrow F_\varphi$ . Since the trace of  $\rho_\varphi$  takes values in  $\mathcal{O}_\varphi$ , we can find an  $\mathcal{A}$ -stable  $\mathcal{O}_\varphi$ -lattice  $\mathcal{L}_\varphi$  in  $F_\varphi^n$ . Write  $\bar{\rho}_\varphi$  for the residual representation  $\bar{\rho}_\varphi : \mathcal{A} \rightarrow M_n(\kappa_\varphi)$ . We abuse notation and write  $\bar{\rho}_i$  for the residual representation  $\bar{\rho}_i : \mathcal{A} \rightarrow M_{n_i}(\kappa_{\mathcal{R}})$  as well as the residual representation arising from the natural projection from  $\kappa_{\mathcal{R}} \rightarrow \kappa_\varphi$ . The fact that  $\bar{\rho}_\varphi^{\text{ss}} = \bar{\rho}_1 \oplus \bar{\rho}_2 \oplus \bar{\rho}_3$  allows us to conclude that there is an  $\mathcal{O}_\varphi$ -basis of  $\mathcal{L}_\varphi$  so that

$$(11) \quad \rho_\varphi : \mathcal{A} \rightarrow M_n(\mathcal{O}_\varphi)$$

with

$$(12) \quad \bar{\rho}_\varphi(a) = \begin{pmatrix} \bar{\rho}_1(a) & \star_1 & \star_2 \\ \star_3 & \bar{\rho}_2(a) & \star_4 \\ 0 & 0 & \bar{\rho}_3(a) \end{pmatrix}$$

and  $\star_1 = 0$  or  $\star_3 = 0$ . In other words, there is an  $\mathcal{O}_\varphi$ -basis of  $\mathcal{L}_\varphi$  and a permutation  $\sigma$  of  $\{1, 2\}$  so that

$$(13) \quad \bar{\rho}_\varphi(a) = \begin{pmatrix} \bar{\rho}_{\sigma(1)}(a) & \star_1 & \star_2 \\ 0 & \bar{\rho}_{\sigma(2)}(a) & \star_4 \\ 0 & 0 & \bar{\rho}_3(a) \end{pmatrix}.$$

We adopt the convention that  $\sigma(3) = 3$ . Write  $n'_i = \sum_{j=1}^i n_j$ ,  $\varrho_i = \rho_{\sigma(i)}$ ,  $m_i = n_{\sigma(i)}$ , and  $m'_i = \sum_{j=1}^i m_j$ . Set  $\rho_{\tilde{\mathcal{R}}} = (\rho_\varphi)_\varphi : \mathcal{A} \rightarrow M_n(\tilde{R})$ .

The fact that each  $\bar{\rho}_i$  is absolutely irreducible implies that  $\text{im } \bar{\rho}_i = M_{n_i}(\kappa_{\mathcal{R}})$ . Combining this with  $\bar{\rho}_i \not\cong \bar{\rho}_j$  if  $i \neq j$  allows us to conclude that there exists  $a_0 \in \mathcal{A}$  so that  $\det(X - \bar{\rho}_{\tilde{\mathcal{R}}}(a_0))$  has  $n$  distinct roots  $\bar{\alpha}_1, \dots, \bar{\alpha}_n$  where  $\bar{\rho}_{\tilde{\mathcal{R}}}(a) \in M_n\left(\frac{\tilde{R}}{\text{Rad}(\tilde{\mathcal{R}})}\right)$ . Hensel's lemma guarantees that there exists  $n$  distinct elements  $\alpha_1, \dots, \alpha_n \in \mathcal{R}$  that are roots of  $\det(X - \rho_{\tilde{\mathcal{R}}}(a_0))$  so that  $\alpha_i \equiv \bar{\alpha}_i \pmod{\mathfrak{m}_{\mathcal{R}}}$ . After a change of basis we may assume that

$$\rho_{\tilde{\mathcal{R}}}(a_0) = \text{diag}(\alpha_1, \dots, \alpha_n).$$

Lemma 2.1 of [Br08] gives that the  $\mathcal{R}$ -submodule of  $M_n(\tilde{\mathcal{R}})$  generated by the powers of  $\rho_{\tilde{\mathcal{R}}}(a_0)$  is exactly the set of diagonal matrices with entries in  $\mathcal{R}$ . So for all  $i$  with  $1 \leq i \leq n$  there exists  $f_i \in \mathcal{A}$  so that

$$\rho_{\tilde{\mathcal{R}}}(f_i) = E(\alpha_i) = \text{diag}(0, \dots, 0, 1, 0, \dots, 0)$$

with 1 in the  $i$ th place. We also set  $a_1, a_2$ , and  $a_3$  to be the elements in  $\mathcal{A}$  so that

$$\begin{aligned}\rho_{\tilde{\mathcal{R}}}(a_1) = E_1 &= \begin{pmatrix} 1_{n_1} & 0 & 0 \\ 0 & 0_{n_2} & 0 \\ 0 & 0 & 0_{n_3} \end{pmatrix}, \\ \rho_{\tilde{\mathcal{R}}}(a_2) = E_2 &= \begin{pmatrix} 0_{n_1} & 0 & 0 \\ 0 & 1_{n_2} & 0 \\ 0 & 0 & 0_{n_3} \end{pmatrix},\end{aligned}$$

and

$$\rho_{\tilde{\mathcal{R}}}(a_3) = E_3 = \begin{pmatrix} 0_{n_1} & 0 & 0 \\ 0 & 0_{n_2} & 0 \\ 0 & 0 & 1_{n_3} \end{pmatrix}.$$

Similarly, we define  $a'_1, a'_2$ , and  $a'_3$  to be the elements in  $\mathcal{A}$  so that

$$\begin{aligned}\rho_{\tilde{\mathcal{R}}}(a'_1) = E'_1 &= \begin{pmatrix} 1_{m_1} & 0 & 0 \\ 0 & 0_{m_2} & 0 \\ 0 & 0 & 0_{m_3} \end{pmatrix}, \\ \rho_{\tilde{\mathcal{R}}}(a'_2) = E'_2 &= \begin{pmatrix} 0_{m_1} & 0 & 0 \\ 0 & 1_{m_2} & 0 \\ 0 & 0 & 0_{m_3} \end{pmatrix},\end{aligned}$$

and

$$\rho_{\tilde{\mathcal{R}}}(a'_3) = E'_3 = \begin{pmatrix} 0_{m_1} & 0 & 0 \\ 0 & 0_{m_2} & 0 \\ 0 & 0 & 1_{m_3} \end{pmatrix}.$$

We now consider  $\tilde{\mathcal{H}}^n$  with an action of  $\mathcal{A}$  given by  $\rho_{\tilde{\mathcal{R}}}$ . Let  $(e_1, \dots, e_n)$  be the canonical basis and set  $\mathcal{L}$  as the  $\mathcal{R}$ -sublattice of  $\tilde{\mathcal{H}}^n$  generated by  $\rho_{\tilde{\mathcal{R}}}(a)e_n$  as  $a$  runs through  $\mathcal{A}$ . It is clear that  $\mathcal{L}$  is  $\mathcal{A}$ -stable by construction. Set  $\mathcal{L}_i = E_i(\mathcal{L})$  for  $i = 1, 2, 3$ . Trivially we have  $\mathcal{L} = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3$ .

**Lemma 6.2.** *The lattice  $\mathcal{L}_i$  is free of rank  $n_i$  over  $\mathcal{R}$  for  $1 \leq i \leq 3$ .*

*Proof.* This is Lemma 1.1 of [U01]. We give the proof here for  $i = 3$  as the other two cases are identical. The definition of  $\mathcal{L}_3$  gives that  $\mathcal{L}_3 \otimes_{\mathcal{R}} \kappa_{\mathcal{R}}$  is generated by

$$\begin{pmatrix} 0_{n_1} & 0 & 0 \\ 0 & 0_{n_2} & 0 \\ 0 & 0 & \bar{\rho}_3(a) \end{pmatrix} \bar{e}_n$$

as  $a$  runs through  $\mathcal{A}$ . The fact that  $\text{im } \bar{\rho}_3 = M_{n_3}(\kappa_{\mathcal{R}})$  gives that  $\mathcal{L}_3 \otimes_{\mathcal{R}} \kappa_{\mathcal{R}} = \kappa_{\mathcal{R}} \bar{e}'_{n'_2+1} \oplus \dots \oplus \kappa_{\mathcal{R}} \bar{e}_n$ . For  $n'_2 + 1 \leq i \leq n$  let  $e'_i \in \mathcal{L}_3$  be a lifting of  $\bar{e}_i$ . Theorem 2.3 in [M94] (essentially Nakayama's lemma) gives that  $\mathcal{L}_3 = \mathcal{R}e'_{n'_2+1} + \dots + \mathcal{R}e'_n$ . We can now use the fact that  $\mathcal{L}_3 \otimes_{\mathcal{R}} F_{\mathcal{R}}$  is of rank  $n_3 = n - n'_2$  over  $F_{\mathcal{R}}$  to conclude the sum must be direct.  $\square$

Write  $\rho_{\mathcal{L}} = \rho_{\tilde{\mathcal{R}}} |_{\mathcal{L}}$ . We can write the decomposition  $\mathcal{L} = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3$  as  $\mathcal{L} = \mathcal{L}_{\sigma(1)} \oplus \mathcal{L}_{\sigma(2)} \oplus \mathcal{L}_3$ , which allows us to write  $\rho_{\mathcal{L}}$  in blocks

$$\rho_{\mathcal{L}}(a) = \begin{pmatrix} A^{1,1}(a) & A^{1,2}(a) & A^{1,3}(a) \\ A^{2,1}(a) & A^{2,2}(a) & A^{2,3}(a) \\ A^{3,1}(a) & A^{3,2}(a) & A^{3,3}(a) \end{pmatrix}$$

where

$$A^{i,j}(a) = \text{Res}_{\mathcal{L}_{\sigma(j)}}(E'_i \circ \rho_{\tilde{\mathcal{R}}}(a)) \in \text{Hom}_{\mathcal{R}}(\mathcal{L}_{\sigma(j)}, \mathcal{L}_{\sigma(i)}).$$

**Lemma 6.3.** *The map*

$$\begin{aligned} \mathcal{A} &\rightarrow \text{Hom}_{\mathcal{R}}(\mathcal{L}_3, \mathcal{L}_{\sigma(1)}) \oplus \text{Hom}_{\mathcal{R}}(\mathcal{L}_3, \mathcal{L}_{\sigma(2)}) \cong \text{Hom}_{\mathcal{R}}(\mathcal{L}_3, \mathcal{L}_{\sigma(1)} \oplus \mathcal{L}_{\sigma(2)}) \\ a &\mapsto (A^{1,3}(a), A^{2,3}(a)) \end{aligned}$$

is surjective as a map of  $\mathcal{R}$ -modules. Moreover, if there exists an  $a \in \mathcal{A}$  so that  $A^{1,2}(a) \neq 0$ , then the map

$$\begin{aligned} \mathcal{A} &\rightarrow \text{Hom}_{\mathcal{R}}(\mathcal{L}_{\sigma(2)}, \mathcal{L}_{\sigma(1)}) \oplus \text{Hom}_{\mathcal{R}}(\mathcal{L}_3, \mathcal{L}_{\sigma(1)}) \oplus \text{Hom}_{\mathcal{R}}(\mathcal{L}_3, \mathcal{L}_{\sigma(2)}) \\ a &\mapsto (A^{1,2}(a), A^{3,1}(a), A^{2,3}(a)) \end{aligned}$$

is surjective as a map of  $\mathcal{R}$ -modules.

*Proof.* This is a generalization of Lemma 1.2 of [U01]. The necessary work was done in Lemma 2.3 of [Br08], so here we merely reduce to what was shown there.

We prove the first statement. If we can show that the map

$$\begin{aligned} \mathcal{A} \otimes_{\mathcal{R}} \kappa_{\mathcal{R}} &\xrightarrow{\vartheta} \text{Hom}_{\kappa_{\mathcal{R}}}(\mathcal{L}_3 \otimes_{\mathcal{R}} \kappa_{\mathcal{R}}, \mathcal{L}_{\sigma(1)} \otimes_{\mathcal{R}} \kappa_{\mathcal{R}}) \oplus \text{Hom}_{\kappa_{\mathcal{R}}}(\mathcal{L}_3 \otimes_{\mathcal{R}} \kappa_{\mathcal{R}}, \mathcal{L}_{\sigma(2)} \otimes_{\mathcal{R}} \kappa_{\mathcal{R}}) \\ &\cong \bigoplus_{i=m'_2+1}^n \text{Hom}_{\kappa_{\mathcal{R}}}(\kappa_{\mathcal{R}} \bar{e}_i, \mathcal{L}_{\sigma(1)} \otimes_{\mathcal{R}} \kappa_{\mathcal{R}}) \oplus \bigoplus_{k=m'_2+1}^n \text{Hom}_{\kappa_{\mathcal{R}}}(\kappa_{\mathcal{R}} \bar{e}_k, \mathcal{L}_{\sigma(2)} \otimes_{\mathcal{R}} \kappa_{\mathcal{R}}) \\ &\cong \bigoplus_{i=m'_2+1}^n \bigoplus_{j=1}^{m'_1} \text{Hom}_{\kappa_{\mathcal{R}}}(\kappa_{\mathcal{R}} \bar{e}_i, \kappa_{\mathcal{R}} \bar{e}_j) \oplus \bigoplus_{k=m'_2+1}^n \bigoplus_{l=m'_1+1}^{m'_2} \text{Hom}_{\kappa_{\mathcal{R}}}(\kappa_{\mathcal{R}} \bar{e}_k, \kappa_{\mathcal{R}} \bar{e}_l) \end{aligned}$$

is surjective, then Nakayama's lemma will give the result. However, to see surjectivity here it is enough to see that the image contains each  $(i, j) \times (k, l)$ -factor. In terms of the block decomposition into matrices as above, this amounts to showing that  $e_{u,v}$  is in the image for all  $1 \leq u \leq m'_2$ ,  $m'_2 + 1 \leq v \leq n$  for  $e_{u,v}$  the matrix with a 1 in the  $uv$ th entry and 0's elsewhere. That this is true is shown in Lemma 2.3 of [Br08].

The second statement follows from the same method.  $\square$

As we are viewing these morphisms of  $\mathcal{R}$ -modules as matrices with entries in  $F_{\mathcal{R}}$ , we can compute their traces. We now rehash the work in [Br08] in our current setting.

**Lemma 6.4.** *For all  $a \in \mathcal{A}$  and  $1 \leq i \leq 3$  we have  $\text{Tr}(A^{i,i}(a)) \in \mathcal{R}$  and*

$$\text{Tr}(A^{i,i}(a)) \equiv \text{Tr}(\varrho_i(a)) \pmod{I}.$$

*Proof.* Observe that one has  $\text{Tr}(A^{i,i}(a)) = \text{Tr}(E'_i \rho_{\tilde{\mathcal{R}}}(a) E'_i) = \text{Tr}(\rho_{\tilde{\mathcal{R}}}(a_i a a_i)) \in \mathcal{R}$ , and so the first statement holds.

By assumption (2) we have that for all  $a \in \mathcal{A}$

$$\text{Tr}(\varrho_1(a_i a a_i)) + \text{Tr}(\varrho_2(a_i a a_i)) + \text{Tr}(\varrho_3(a_i a a_i)) \equiv \text{Tr}(\rho_{\tilde{\mathcal{R}}}(a_i a a_i)) = \text{Tr}(A^{i,i}(a)) \pmod{I}.$$

We have that  $\varrho_i(a_j) \equiv 0 \pmod{I}$  unless  $i = j$ . Thus, we obtain

$$\text{Tr}(A^{i,i}(a)) \equiv \text{Tr}(\varrho_i(a)) \pmod{I}$$

for  $1 \leq i \leq 3$ . □

**Lemma 6.5.** *For all  $a, b \in \mathcal{A}$  and  $1 \leq j \leq 3$  we have*

$$\text{Tr} \left( \sum_{\substack{1 \leq i \leq 3 \\ i \neq j}} A^{j,i}(a) A^{i,j}(b) \right) \in \mathcal{R}$$

and

$$\text{Tr} \left( \sum_{\substack{1 \leq i \leq 3 \\ i \neq j}} A^{j,i}(a) A^{i,j}(b) \right) \equiv \text{Tr} \left( \sum_{\substack{1 \leq i \leq 3 \\ i \neq j}} A^{j,i}(b) A^{i,j}(a) \right) \pmod{I}.$$

*Proof.* We prove the case with  $j = 3$  as the others are completely analogous. Let  $a, b \in \mathcal{A}$ . Observe that

$$\begin{aligned} \text{Tr} \left( \sum_{i=1}^2 A^{3,i}(a) A^{i,3}(b) \right) &= \text{Tr}(E'_3 \rho_{\tilde{\mathcal{R}}}(ab) E'_3) \\ &= \text{Tr}(\rho_{\tilde{\mathcal{R}}}(a_3 a b a_3)) \in \mathcal{R}. \end{aligned}$$

This proves the first claim.

Using the previous lemma we have that

$$\begin{aligned} \text{Tr}(A^{3,3}(ab)) &\equiv \text{Tr}(\varrho_3(ab)) \pmod{I} \\ &= \text{Tr}(\varrho_3(a) \rho_3(b)) \\ &= \text{Tr}(\varrho_3(b) \rho_3(a)) \\ &= \text{Tr}(\varrho_3(ba)) \\ &\equiv \text{Tr}(A^{3,3}(ba)) \pmod{I}. \end{aligned}$$

Thus,  $\text{Tr}(A^{3,3}(ab)) \equiv \text{Tr}(A^{3,3}(ba)) \pmod{I}$  for all  $a, b \in \mathcal{A}$ . We combine this with the fact that  $\rho_{\tilde{\mathcal{R}}}(ab) = \rho_{\tilde{\mathcal{R}}}(a) \rho_{\tilde{\mathcal{R}}}(b)$  to reach the desired congruence modulo  $I$ . □

**Lemma 6.6.** *For all  $a \in \mathcal{A}$  we have  $A^{i,j}(a) \in \text{Hom}_{\mathcal{R}}(\mathcal{L}_{\sigma(j)}, \mathfrak{m}_{\mathcal{R}} \mathcal{L}_{\sigma(i)})$  for  $i > j$ .*

*Proof.* Suppose there exists  $a \in \mathcal{A}$  so that  $A^{i,j}(a) \notin \text{Hom}_{\mathcal{R}}(\mathcal{L}_{\sigma(j)}, \mathfrak{m}_{\mathcal{R}} \mathcal{L}_{\sigma(i)})$ . Then there exists  $\wp$  so that after localization at  $\wp$  one has  $\rho_{\wp}(r)(\mathcal{L}_{\sigma(j),\wp})$  is not contained in  $\mathfrak{m}_{\wp} \mathcal{L}_{\sigma(i),\wp}$ . However, this contradicts equation (13).  $\square$

We use this lemma as our base case in an induction argument as used in [Br08] and [U01]. We prove that for  $i > j$  we have

$$(14) \quad A^{i,j}(a) \in \text{Hom}_{\mathcal{R}}(\mathcal{L}_{\sigma(j)}, (\mathfrak{m}_{\mathcal{R}}^k + I) \mathcal{L}_{\sigma(i)})$$

for all  $a \in \mathcal{A}$ . Assume inductively that the statement is true for some  $k$ . We break the proof into two steps. First we prove that the statement is true for  $a \in \ker(\rho \otimes_{\mathcal{R}} \kappa_{\mathcal{R}})$ .

**Lemma 6.7.** *Let  $a \in \ker(\rho \otimes_{\mathcal{R}} \kappa_{\mathcal{R}})$ . Then under our induction hypothesis we have*

$$A^{i,j}(a) \in \text{Hom}_{\mathcal{R}}(\mathcal{L}_j, (\mathfrak{m}_{\mathcal{R}}^{k+1} + I) \mathcal{L}_i)$$

for  $i > j$ .

*Proof.* The fact that  $a \in \ker(\rho \times_{\mathcal{R}} \kappa_{\mathcal{R}})$  implies that  $A^{j,i}(a)(\mathcal{L}_{\sigma(i)}) \subset \mathfrak{m}_{\mathcal{R}} \mathcal{L}_{\sigma(j)}$ . Thus, our induction hypothesis gives that for any  $b \in \mathcal{A}$  we have

$$A^{i,j}(b) A^{j,i}(a)(\mathcal{L}_{\sigma(i)}) \subset A^{i,j}(b) \mathfrak{m}_{\mathcal{R}}(\mathcal{L}_{\sigma(j)}) = \mathfrak{m}_{\mathcal{R}} A^{i,j}(b)(\mathcal{L}_{\sigma(j)}) \subset (\mathfrak{m}_{\mathcal{R}}^{k+1} + I) \mathcal{L}_{\sigma(i)}.$$

Thus, by Lemma 6.5 we have

$$\text{Tr} \left( \sum_{\substack{j \\ j \neq i}} A^{i,j}(a) A^{j,i}(b) \right) \in \mathfrak{m}_{\mathcal{R}}^{k+1} + I.$$

Consider now a fixed  $i_0, j_0$  with  $i_0 > j_0$ . Let  $\ell \in \mathcal{L}_{\sigma(j_0)}$ . We wish to show that  $A^{i_0, j_0}(a) \ell \in (\mathfrak{m}_{\mathcal{R}}^{k+1} + I) \mathcal{L}_{\sigma(i_0)}$ . Write

$$A^{i_0, j_0}(a) \ell = \sum_{s=m'_{i_0-1}+1}^{m'_{i_0}} \alpha_s e'_s$$

for some  $\alpha_s \in \mathcal{R}$ . Lemma 6.3 guarantees that for each  $m'_{i_0-1} + 1 \leq s \leq m'_{i_0}$  there exists a  $t_s \in \mathcal{A}$  so that  $A^{j_0, i_0}(t_s)(e'_s) = \ell$ ,  $A^{j_0, i_0}(t_s)(e'_r) = 0$  for  $r \neq s$  and  $A^{j, i_0}(t_s)(e'_r) = 0$  for all  $j \neq j_0$ ,  $m'_{j-1} + 1 \leq r \leq m'_j$ . Thus, we have  $\alpha_{i_0} = \text{Tr}(A^{i_0, j_0}(a) A^{j_0, i_0}(t_s)) \in \mathfrak{m}_{\mathcal{R}}^{k+1} + I$  for each  $m'_{i_0-1} + 1 \leq s \leq m'_{i_0}$ , which gives the first result.  $\square$

**Lemma 6.8.** *Under our induction hypothesis we have*

$$A^{i,j}(a) \in \text{Hom}_{\mathcal{R}}(\mathcal{L}_{\sigma(j)}, (\mathfrak{m}_{\mathcal{R}}^{k+1} + I) \mathcal{L}_{\sigma(i)})$$

for all  $a \in \mathcal{A}$  and  $i > j$ .

*Proof.* Consider  $\text{Im } \rho \otimes \kappa_{\mathcal{R}} \subset \text{Hom}(\mathcal{L} \otimes \kappa_{\mathcal{R}}, \mathcal{L} \otimes \kappa_{\mathcal{R}})$ . We denote the projection of  $\bar{\rho}(a)$  onto  $\text{Hom}(\mathcal{L}_{\sigma(t)} \otimes \kappa_{\mathcal{R}}, \mathcal{L}_{\sigma(s)} \otimes \kappa_{\mathcal{R}})$  by  $\bar{A}^{s,t}$ . Applying Lemma 6.6 we have a decomposition

$$\text{Im } \rho \otimes \kappa_{\mathcal{R}} = \sum_{1 \leq s \leq t \leq 3} (\text{Im } \rho \otimes \kappa_{\mathcal{R}})_{s,t}$$

and so we can denote any element of  $\text{Im } \rho \otimes \kappa_{\mathcal{R}}$  by a matrix

$$\begin{pmatrix} \bar{A}^{1,1} & \bar{A}^{1,2} & \bar{A}^{1,3} \\ 0 & \bar{A}^{2,2} & \bar{A}^{2,3} \\ 0 & 0 & \bar{A}^{3,3} \end{pmatrix}$$

with  $\bar{A}^{s,t} \in (\text{Im } \rho \otimes \kappa_{\mathcal{R}})_{s,t}$ .

Lemma 6.7 gives well-defined linear maps

$$\Phi_{i,j} : \text{Im } \rho \otimes \kappa_{\mathcal{R}} \rightarrow \text{Hom}_{\mathcal{R}}(\mathcal{L}_{\sigma(j)}, (\mathfrak{m}_{\mathcal{R}}^k + I)\mathcal{L}_{\sigma(i)} / (\mathfrak{m}_{\mathcal{R}}^{k+1} + I)\mathcal{L}_{\sigma(i)})$$

for  $i > j$  induced by the map  $a \mapsto A^{i,j}(a)$ . To finish the induction it is enough to show that  $\Phi_{i,j}$  is 0 for  $i > j$ . Observe that by definition  $\Phi_{i,j}$  is zero on diagonal matrices for  $i > j$ . The relation

$$A^{i,j}(ab) = \sum_{s=1}^3 A^{i,s}(a)A^{s,j}(b)$$

gives the equations

$$\Phi_{i,j}(\bar{B}\bar{C}) = \sum_{s=1}^j \Phi_{i,s}(\bar{B})\bar{C}^{s,j} + \sum_{s=j+1}^i \Phi_{i,s}(\bar{B})\Phi_{s,j}(\bar{C}) + \sum_{s=i+1}^3 \bar{B}^{i,s}\Phi_{s,j}(\bar{C}).$$

It is enough to show that for each  $1 \leq u \leq v \leq 3$ ,  $\Phi_{i,j}(\bar{D}) = 0$  for  $\bar{D}$  defined by  $\bar{D}^{i,j} = 0$  unless  $i = u, j = v$ . We have

$$\begin{aligned} \Phi_{i,j}(\bar{D}) &= \Phi_{i,j}(\bar{D}\bar{\rho}(a'_v)) \\ &= \sum_{s=1}^j \Phi_{i,s}(\bar{D})\bar{\rho}(a'_v)^{s,j} + \sum_{s=j+1}^i \Phi_{i,s}(\bar{D})\Phi_{s,j}(\bar{\rho}(a'_v)) + \sum_{s=i+1}^3 \bar{D}^{i,s}\Phi_{s,j}(\bar{\rho}(a'_v)) \end{aligned}$$

(15)

$$= \sum_{s=1}^j \Phi_{i,s}(\bar{D})\bar{\rho}(a'_v)^{s,j}$$

(16)

$$= \Phi_{i,j}(\bar{D})$$

(17)

$$= 0.$$

Note that equation (15) follows from the fact that  $\bar{\rho}(a'_v) = E'_v$ ,  $j < s$  and  $\Phi_{s,j}$  of a diagonal matrix is 0 for  $s \neq j$ . Equation (16) follows from noting  $\bar{\rho}(a'_v)^{s,j} = 0$  unless  $s = j = v$ , in which case  $\bar{\rho}(a'_v)^{v,v} = I_v$ . Finally, we see

that  $\Phi_{i,j}(\overline{D}) = 0$  unless  $(i, j) = (u, v)$ , but this is impossible since  $i > j$  and  $u \leq v$ . This completes the proof and hence the induction.  $\square$

We summarize what we have proven thus far (in terms of  $\rho_i$ 's and  $\mathcal{L}_i$ 's) in the following proposition. The only point that needs mentioning is the statement about the action on the quotient also requires Theorem 1 in [C94].

**Proposition 6.9.** *The lattice  $(\mathcal{L}_1 \otimes \mathcal{R}/I) \oplus (\mathcal{L}_2 \otimes \mathcal{R}/I)$  is stable under the action of  $\mathcal{A}$  and the action of  $\mathcal{A}$  on the quotient  $(\mathcal{L} \otimes \mathcal{R}/I)/((\mathcal{L}_1 \otimes \mathcal{R}/I) \oplus (\mathcal{L}_2 \otimes \mathcal{R}/I))$  is isomorphic to  $\rho_3 \otimes \mathcal{R}/I$ . Moreover, either  $\text{Hom}_{\mathcal{R}/I}(\mathcal{L}_1 \otimes \mathcal{R}/I, \mathcal{L}_2 \otimes \mathcal{R}/I) = 0$  or  $\text{Hom}_{\mathcal{R}/I}(\mathcal{L}_2 \otimes \mathcal{R}/I, \mathcal{L}_1 \otimes \mathcal{R}/I) = 0$ .*

It now remains to consider the action of  $\mathcal{A}$  on  $(\mathcal{L}_1 \otimes \mathcal{R}/I) \oplus (\mathcal{L}_2 \otimes \mathcal{R}/I)$ .

**Lemma 6.10.** (1) *The  $\mathcal{R}$ -modules*

$$\mathcal{L}_1(\alpha_i) = E(\alpha_i)\mathcal{L}_1 = \ker(\rho_{\overline{\mathcal{R}}}(a_0) - \alpha_i \text{Id}) \cap \mathcal{L}_1$$

*are mutually isomorphic to some module  $\mathcal{T}_1$  for  $1 \leq i \leq n_2$  and similarly the  $\mathcal{R}$ -modules*

$$\mathcal{L}_2(\alpha_i) = E(\alpha_i)\mathcal{L}_2 = \ker(\rho_{\overline{\mathcal{R}}}(a_0) - \alpha_i \text{Id}) \cap \mathcal{L}_2$$

*are mutually isomorphic to some module  $\mathcal{T}_2$  for  $n_1 + 1 \leq i \leq n_2$ .*

(2) *As an  $\mathcal{A}$ -module,  $\mathcal{L}_j \otimes \mathcal{R}/I \cong \rho_j \otimes \mathcal{T}_j/I\mathcal{T}_j$  for  $j = 1, 2$ .*

*Proof.* We prove this theorem for  $\mathcal{L}_1$  as the argument for  $\mathcal{L}_2$  is exactly the same. Recall that we let  $f_i \in \mathcal{A}$  denote the element so that  $\rho_{\overline{\mathcal{R}}}(f_i) = \text{diag}(0, \dots, 0, 1, 0, \dots, 0)$  with a 1 in the  $i$ th place. Given any  $i, j \in \{1, \dots, n_1\}$ , the irreducibility of  $\overline{\rho}_1$  gives an element  $\sigma_{i,j} \in \mathcal{A}$  so that  $\rho_{\overline{\mathcal{R}}}(\sigma_{i,j})\overline{e}_i = \overline{e}_j$ . Thus,  $\rho_{\overline{\mathcal{R}}}(f_j\sigma_{i,j}f_i)$  gives a morphism  $\phi_{i,j}$  from  $\mathcal{L}_1(\alpha_i)$  to  $\mathcal{L}_1(\alpha_j)$ . Our choice of  $f_i$ 's and  $\sigma_{i,j}$  give that  $\phi_{i,j} \circ \phi_{j,i}$  gives an automorphism of  $\mathcal{L}_1(\alpha_i)$  and so  $\phi_{i,j}$  is an isomorphism. This gives the first result where we set  $\mathcal{T}_1 = \mathcal{L}_1(\alpha_1)$  and  $\mathcal{T}_2 = \mathcal{L}_2(\alpha_{n_1+1})$ .

Fix an isomorphism  $\mathcal{L}_1 \otimes \mathcal{R}/I \cong (\mathcal{T}_1/I\mathcal{T}_1)^{n_1}$ . Set  $\mathcal{E} = \text{End}_{\mathcal{R}/I}(\mathcal{T}_1/I\mathcal{T}_1)$  (a noncommutative Artinian algebra) and  $\theta : \mathcal{R}/I \rightarrow \mathcal{E}$  the canonical algebra homomorphism. The action of  $\mathcal{A}$  on  $\mathcal{L}_1 \otimes \mathcal{R}/I$  gives a representation  $\rho'_1$  in  $M_{n_1}(\mathcal{E})$  so that  $\text{Tr}(\rho'_1(a)) \in \theta(\mathcal{R}/I)$  is defined for all  $a \in \mathcal{A}$  and we have  $\text{Tr}(\rho'_1(a)) = \theta(\text{Tr}(\rho_1(a)))$  for all  $a \in \mathcal{A}$ . A generalization of Theorem 1.1.2 in [C94] then gives the result. See the proof of Lemma 1.5 in [U01] for the proof of this generalization.  $\square$

*Proof.* (of Theorem 6.1) In light of Proposition 6.9 and Lemma 6.10, it only remains to prove the last statement of the theorem. Suppose some quotient of  $\mathcal{L}$  is isomorphic to  $\overline{\rho}'$  with  $\overline{\rho}'^{\text{ss}} = \overline{\rho}_1 \oplus \overline{\rho}_2$ . Let  $\mathcal{L}'$  be the sublattice of  $\mathcal{L}$  that is stable under the action of  $\mathcal{A}$  so that  $\mathcal{L}/\mathcal{L}' \cong \overline{\rho}'$ . From our decomposition of  $\mathcal{L}$  we inherit a decomposition of  $\mathcal{L}'$  as  $\mathcal{L}' = \mathcal{L}'_1 \oplus \mathcal{L}'_2 \oplus \mathcal{L}'_3$ . Thus, we have

$$\mathcal{L}/\mathcal{L}' = \mathcal{L}_1/\mathcal{L}'_1 \oplus \mathcal{L}_2/\mathcal{L}'_2 \oplus \mathcal{L}_3/\mathcal{L}'_3 \cong \overline{\rho}'.$$

However, our assumption on  $\bar{\rho}'^{\text{ss}}$  gives that  $\mathcal{L}_3 = \mathcal{L}'_3$ . This, combined with the fact that  $\mathcal{L}$  is generated by  $\mathcal{L}_3$  over  $\mathcal{A}$  gives  $\mathcal{L} = \mathcal{L}'$ , a contradiction. Thus, no such quotient can exist. It is useful to observe that what this is saying in terms of the matrices is that  $A^{1,3}$  and  $A^{2,3}$  cannot both be 0.  $\square$

## 7. SELMER GROUPS

Let  $K$  be a field and write  $G_K$  for  $\text{Gal}(\bar{K}/K)$ . Let  $M$  be a topological  $G_K$ -module. We write the cohomology group  $H_{\text{cont}}^1(G_K, M)$  as  $H^1(K, M)$  where “cont” refers to continuous cocycles. For a prime  $\ell$ , we write  $D_\ell$  for the decomposition group at  $\ell$  and identify it with  $G_{\mathbb{Q}_\ell}$ .

Let  $E/\mathbb{Q}_p$  be a finite extension. Let  $\mathcal{O}$  be the ring of integers of  $E$  and  $\varpi$  a uniformizer. Let  $V$  be a finite dimensional Galois representation over  $E$ . We will also find it convenient to write  $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_n(E)$  to denote the Galois representation  $V$  when  $\dim_E(V) = n$ . We switch interchangeably between these notations depending upon context. Let  $T \subseteq V$  be a Galois-stable  $\mathcal{O}$ -lattice, i.e.,  $T$  is stable under the action of  $G_{\mathbb{Q}}$  and  $T \otimes_{\mathcal{O}} E \cong V$ . Set  $W = V/T$ .

We write  $\mathbb{B}_{\text{cris}}$  for the ring of  $p$ -adic periods ([Fo82]). Set

$$D = (V \otimes_{\mathbb{Q}_p} \mathbb{B}_{\text{cris}})^{D_p}$$

and

$$\text{Cris}(V) = H^0(\mathbb{Q}_p, V \otimes_{\mathbb{Q}_p} \mathbb{B}_{\text{cris}}).$$

We say the representation  $V$  is *crystalline* if  $\dim_{\mathbb{Q}_p} V = \dim_{\mathbb{Q}_p} \text{Cris}(V)$ . Let  $\text{Fil}^i D$  be a decreasing filtration of  $D$ . If  $V$  is crystalline, we say  $V$  is *short* if  $\text{Fil}^0 D = D$ ,  $\text{Fil}^p D = 0$ , and if whenever  $V'$  is a nonzero quotient of  $V$ , then  $V' \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(p-1)$  is ramified. Note that  $\mathbb{Q}_p(n)$  is the 1-dimensional space over  $\mathbb{Q}_p$  on which  $G_{\mathbb{Q}}$  acts via the  $n$ th power of the  $p$ -adic cyclotomic character.

The local Selmer groups are defined as follows. Set

$$H_f^1(\mathbb{Q}_\ell, V) = \begin{cases} H_{\text{ur}}^1(\mathbb{Q}_\ell, V) & \ell \neq p \\ \ker(H^1(\mathbb{Q}_p, V) \rightarrow H^1(\mathbb{Q}_p, V \otimes_{\mathbb{Q}_p} \mathbb{B}_{\text{cris}})) & \ell = p \end{cases}$$

where

$$H_{\text{ur}}^1(\mathbb{Q}_\ell, M) = \ker(H^1(\mathbb{Q}_\ell, M) \rightarrow H^1(I_\ell, M))$$

for any  $D_\ell$ -module  $M$  where  $I_\ell$  is the inertia group at  $\ell$ . With  $W$  as above we define  $H_f^1(\mathbb{Q}_\ell, W)$  to be the image of  $H_f^1(\mathbb{Q}_\ell, V)$  under the natural map  $H^1(\mathbb{Q}_\ell, V) \rightarrow H^1(\mathbb{Q}_\ell, W)$ .

**Definition 7.1.** The Selmer group of  $W$  is given by

$$\text{Sel}(W) = \ker \left( H^1(\mathbb{Q}, W) \rightarrow \bigoplus_{\ell} \frac{H^1(\mathbb{Q}_\ell, W)}{H_f^1(\mathbb{Q}_\ell, W)} \right),$$

i.e., it is the cocycles  $\mathfrak{c} \in H^1(\mathbb{Q}, W)$  that lie in  $H_f^1(\mathbb{Q}_\ell, W)$  when restricted to  $D_\ell$ .

Before we can define the degree  $n$  Selmer groups of interest we must recall the notion of extensions of modules and the relationship between these extensions and the first cohomology group. An extension of  $M$  by  $N$  is a short exact sequence

$$0 \longrightarrow N \xrightarrow{\alpha} X \xrightarrow{\beta} M \longrightarrow 0$$

where  $X$  is a  $R[G]$ -module and  $\alpha$  and  $\beta$  are  $R[G]$ -homomorphisms. We sometimes refer to such an extension as the extension  $X$ . We say two extensions  $X$  and  $Y$  are equivalent if there is a  $R[G]$ -isomorphism  $\gamma$  making the following diagram commute

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\alpha_X} & X & \xrightarrow{\beta_X} & M & \longrightarrow & 0 \\ & & \text{id}_N \downarrow & & \gamma \downarrow & & \text{id}_M \downarrow & & \\ 0 & \longrightarrow & N & \xrightarrow{\alpha_Y} & Y & \xrightarrow{\beta_Y} & M & \longrightarrow & 0. \end{array}$$

Let  $\text{Ext}_{R[G]}^1(M, N)$  denote the set of equivalence classes of  $R[G]$ -extensions of  $M$  by  $N$  which split as extensions of  $R$ -modules, i.e., if  $X$  is the extension of  $M$  by  $N$ , then  $X \cong M \oplus N$  as  $R$ -modules.

The following result will allow us to appropriately define the degree  $n$  Selmer group. The case where  $M = N$  is given as Proposition 4 in [Wa95].

**Theorem 7.2.** (*Theorem 9.2, [Br]*) *Let  $M$  and  $N$  be  $R[G]$ -modules. There is a one-one correspondence between the sets  $H^1(G, \text{Hom}_R(M, N))$  and  $\text{Ext}_{R[G]}^1(M, N)$ .*

The map from  $\text{Ext}_{R[G]}^1(M, N)$  to  $H^1(G, \text{Hom}_R(M, N))$  is given as follows. Let

$$0 \longrightarrow N \xrightarrow{\alpha} X \xrightarrow{\beta} M \longrightarrow 0$$

$\xleftarrow{s_X}$

be an extension with  $s_X$  a  $R$ -section of  $X$ . This extension is mapped to the cohomology class  $g \mapsto \mathbf{c}_g$  where  $\mathbf{c}_g : M \rightarrow N$  is defined by

$$\mathbf{c}_g(m) = \alpha^{-1}(\rho(g)s_X(\rho_M(g^{-1})m) - s_X(m))$$

where  $\rho$  denotes the  $G$ -action on  $X$  and  $\rho_M$  the  $G$ -action on  $M$ .

As it will be useful later, we briefly consider the case where  $N = N_1 \oplus N_2$ . In this case we have that

$$\text{Ext}_{R[G]}^1(M, N) \cong \prod_{i=1}^2 \text{Ext}(M, N_i)$$

and

$$\begin{aligned} \mathrm{H}^1(G, \mathrm{Hom}_R(M, N)) &\cong \mathrm{H}^1(G, \mathrm{Hom}_R(M, N_1) \oplus \mathrm{Hom}_R(M, N_2)) \\ &\cong \mathrm{H}^1(G, \mathrm{Hom}_R(M, N_1)) \oplus \mathrm{H}^1(G, \mathrm{Hom}_R(M, N_2)). \end{aligned}$$

Thus, in this case given an extension  $X \in \mathrm{Ext}_{R[G]}^1(M, N)$ , we obtain cohomology classes  $\mathfrak{c}_1 \in \mathrm{H}^1(G, \mathrm{Hom}_R(M, N_1))$  and  $\mathfrak{c}_2 \in \mathrm{H}^1(G, \mathrm{Hom}_R(M, N_2))$ .

Let  $W[n]$  be the  $\mathcal{O}$ -submodule of  $W$  consisting of elements killed by  $\varpi^n$ . The previous theorem gives a bijection between  $\mathrm{Ext}_{(\mathcal{O}/\varpi^n)[D_p]}^1(\mathcal{O}/\varpi^n, W[n])$  and  $\mathrm{H}^1(D_p, W[n])$ . For  $\ell \neq p$ , we define the local degree  $n$  Selmer groups by  $\mathrm{H}_f^1(\mathbb{Q}_\ell, W[n]) = \mathrm{H}_{\mathrm{ur}}^1(\mathbb{Q}, W[n])$ . At the prime  $p$  we define the local degree  $n$  Selmer group to be the subset of classes of extensions of  $D_p$ -modules

$$0 \longrightarrow W[n] \longrightarrow X \longrightarrow \mathcal{O}/\varpi^n \longrightarrow 0$$

where  $X$  lies in the essential image of the functor  $\mathbb{V}$  defined in § 1.1 of [DFG04]. The precise definition of  $\mathbb{V}$  is technical and is not needed here. We content ourselves with stating that this essential image is stable under direct sums, subobjects, and quotients ([DFG04], § 2.1). For our purposes the following two propositions are what is needed.

**Proposition 7.3.** ([DFG04], p. 670) *If  $V$  is a short crystalline representation at  $p$ ,  $T$  a  $D_p$ -stable lattice, and  $X$  a subquotient of  $T/\varpi^n$  that gives an extension of  $D_p$ -modules as above, then the class of this extension is in  $\mathrm{H}_f^1(\mathbb{Q}_p, W[n])$ .*

**Proposition 7.4.** ([DFG04], Proposition 2.2) *The natural isomorphism*

$$\varinjlim_n \mathrm{H}^1(\mathbb{Q}_\ell, W[n]) \cong \mathrm{H}^1(\mathbb{Q}_\ell, W)$$

*induces isomorphisms*

$$\varinjlim_n \mathrm{H}_{\mathrm{ur}}^1(\mathbb{Q}_\ell, W[n]) \cong \mathrm{H}_{\mathrm{ur}}^1(\mathbb{Q}_\ell, W)$$

*and*

$$\varinjlim_n \mathrm{H}_f^1(\mathbb{Q}_p, W[n]) \cong \mathrm{H}_f^1(\mathbb{Q}_p, W).$$

Let  $M$  be a  $\mathbb{Z}_p$ -module. We denote the Pontryagin dual  $\mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$  of  $M$  by  $M^\vee$ . In particular, we denote the dual of the Selmer group  $\mathrm{Sel}(W)$  by  $S(W)$  to ease the notation.

We close this section with the following results on  $S(W)$ .

**Lemma 7.5.** ([KK07] Lemma 9.4)  *$S(W)$  is a finitely generated  $\mathcal{O}$ -module.*

**Lemma 7.6.** ([KK07] Lemma 9.5) *If the modulo  $\varpi$  reduction  $\bar{\rho}$  of  $\rho$  is absolutely irreducible, then the length of  $S(W)$  as an  $\mathcal{O}$ -module is independent of the choice of the lattice  $T$ .*

## 8. A LOWER BOUND ON THE SELMER GROUP

Let  $E/\mathbb{Q}_p$  be a finite extension as before large enough so that our results from § 5 are defined over  $E$ . We enlarge  $E$  when necessary so that the appropriate Galois representations in this section are defined over  $E$  as well. Let  $\mathcal{O}$  be the ring of integers of  $E$ ,  $\varpi$  the uniformizer,  $\mathfrak{p} = (\varpi)$  the prime ideal over  $p$ , and  $\mathbb{F}$  the residue field.

Let  $\rho_f : \mathbb{G}_{\mathbb{Q}} \rightarrow \mathrm{GL}(V_{f,\mathfrak{p}})$  be the  $p$ -adic Galois representation associated to an eigenform  $f$ ,  $T_{f,\mathfrak{p}}$  a  $\mathbb{G}_{\mathbb{Q}}$ -stable  $\mathcal{O}$ -lattice, and  $W_{f,\mathfrak{p}} = V_{f,\mathfrak{p}}/T_{f,\mathfrak{p}}$ . We denote twists by the  $m$ th power of the cyclotomic character by writing  $V_{f,\mathfrak{p}}(m)$  and similarly for  $W_{f,\mathfrak{p}}(m)$ . We drop the subscript  $f$  and  $\mathfrak{p}$  except for in the statement of theorems as they are fixed throughout the section, i.e., we set  $W = W_{f,\mathfrak{p}}$ ,  $T = T_{f,\mathfrak{p}}$  and  $V = V_{f,\mathfrak{p}}$ .

We have the following result giving the existence of 4-dimensional Galois representations attached to Siegel eigenforms.

**Theorem 8.1.** ([SU06], *Theorem 3.1.3*) *Let  $F \in \mathcal{S}_k(\mathrm{Sp}_4(\mathbb{Z}))$  be an eigenform,  $K_F$  the number field generated by the Hecke eigenvalues of  $F$ , and  $\varphi$  a prime of  $K_F$  over  $p$ . There exists a finite extension  $E$  of the completion of  $K_{F,\varphi}$  of  $K_F$  at  $\varphi$  and a continuous semi-simple Galois representation*

$$\rho_{F,\varphi} : \mathbb{G}_{\mathbb{Q}} \rightarrow \mathrm{GL}_4(E)$$

*unramified away from  $p$  so that for all  $\ell \neq p$  we have*

$$\det(X \cdot 1_4 - \rho_{F,\varphi}(\mathrm{Frob}_{\ell})) = L_{\mathrm{spin},(\ell)}(X).$$

The following result is crucial in producing elements in the Selmer group.

**Theorem 8.2.** ([F89], [U00]) *Let  $F$  be as in Theorem 8.1. The restriction of  $\rho_{F,\varphi}$  to the decomposition group  $D_p$  is crystalline at  $p$ . In addition, if  $p > 2k - 2$  then  $\rho_{F,\varphi}$  is short.*

Recall that we denoted the image of  $\mathbb{T}_{\mathcal{O}}^S$  in  $\mathrm{End}_{\mathbb{C}}(\mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z})))$  by  $\mathbb{T}_{\mathcal{O}}^{\mathrm{NM}}$ . Let  $\mathcal{M}^S$  denote the set of maximal ideals of  $\mathbb{T}_{\mathcal{O}}^S$  and  $\mathcal{M}^{\mathrm{NM}}$  denote the set of maximal ideals of  $\mathbb{T}_{\mathcal{O}}^{\mathrm{NM}}$ . Write  $\mathbb{T}_{\mathcal{O}}^{\mathrm{NM}} = \prod_{\mathfrak{m} \in \mathcal{M}^{\mathrm{NM}}} \mathbb{T}_{\mathcal{O},\mathfrak{m}}^{\mathrm{NM}}$  where the subscript  $\mathfrak{m}$  denotes localization at  $\mathfrak{m}$ . Again we let  $\phi$  denote the natural projection from  $\mathbb{T}_{\mathcal{O}}^S$  to  $\mathbb{T}_{\mathcal{O}}^{\mathrm{NM}}$ . Let  $\mathcal{M}^c$  denote the set of primes in  $\mathcal{M}^S$  that are preimages of elements of  $\mathcal{M}^{\mathrm{NM}}$  under  $\phi$  and  $\mathcal{M}^{nc} = \mathcal{M}^S - \mathcal{M}^c$ . Our factorization of  $\mathbb{T}_{\mathcal{O}}^S$  and  $\mathbb{T}_{\mathcal{O}}^{\mathrm{NM}}$  allows us to factor the map  $\phi$  as

$$\phi = \prod_{\mathfrak{m} \in \mathcal{M}^c} \phi_{\mathfrak{m}} \times \prod_{\mathfrak{m} \in \mathcal{M}^{nc}} 0_{\mathfrak{m}}$$

where  $0_{\mathfrak{m}}$  is the zero map and  $\phi_{\mathfrak{m}} : \mathbb{T}_{\mathcal{O},\mathfrak{m}}^S \rightarrow \mathbb{T}_{\mathcal{O},\mathfrak{m}'}^S$  is the projection with  $\mathfrak{m}' \in \mathcal{M}^{\mathrm{NM}}$  the unique maximal ideal so that  $\phi^{-1}(\mathfrak{m}') = \mathfrak{m}$ .

**Theorem 8.3.** *We have*

$$\mathrm{ord}_p(\#S(\mathbb{Q}, W_{f,\mathfrak{p}}(1-k))) \geq \mathrm{ord}_p(\#\mathbb{T}_{\mathfrak{m}_{F_f}}^{\mathrm{NM}} / \phi_{\mathfrak{m}_{F_f}}(\mathrm{Ann}(F_f)))$$

*where for an  $\mathcal{O}$ -module  $M$ ,  $\mathrm{ord}_p(\#M) = [\mathcal{O}/\varpi : \mathbb{F}_p] \mathrm{length}_{\mathcal{O}}(M)$ .*

**Corollary 8.4.** *Let  $k > 3$  be an integer and  $p$  a prime so that  $p > 2k - 2$ . Let  $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}), \mathcal{O})$  be a newform with real Fourier coefficients and  $F_f$  the Saito-Kurokawa lift of  $f$ . Let  $f$  be ordinary at  $p$  and  $\bar{\rho}_f$  be irreducible. If there exists  $N > 1$ , a fundamental discriminant  $D$  so that  $(-1)^{k-1}D > 0$ ,  $\chi_D(-1) = -1$ ,  $p \nmid ND[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma_0^4(N)]$ , and a Dirichlet character  $\chi$  of conductor  $N$  so that*

$$-M = \mathrm{ord}_{\varpi}(\mathcal{L}(k, f, D, \chi)) < 0$$

then

$$\mathrm{ord}_p(\#S(\mathbb{Q}, W_{f,p}(1-k))) \geq M$$

where we recall

$$\mathcal{L}(k, f, D, \chi) = \frac{L^{\Sigma}(3-k, \chi)L_{\mathrm{alg}}(k-1, f, \chi_D)L_{\mathrm{alg}}(1, f, \chi)L_{\mathrm{alg}}(2, f, \chi)}{L_{\mathrm{alg}}(k, f)}.$$

*Proof.* This corollary is an immediate consequence of Theorem 8.3 and Corollary 5.6.  $\square$

The work in § 6 and in particular Theorem 6.1 is the main input into the proof of Theorem 8.3. We begin by adapting Theorem 6.1 to our current situation. First we set up some notation following [KK07].

Let  $n = n_1 + n_2 + n_3$  with  $n_i \geq 1$ . Let  $V_i$  be  $E$  vector spaces of dimension  $n_i$  affording continuous absolutely irreducible representations  $\rho_i : \mathrm{G}_{\mathbb{Q}} \rightarrow \mathrm{Aut}_E(V_i)$  for  $1 \leq i \leq 3$ . Assume the residual representations  $\bar{\rho}_i$  are irreducible and nonisomorphic for  $1 \leq i \leq 3$ . Let  $\mathcal{V}_1, \dots, \mathcal{V}_m$  be  $n$ -dimensional  $E$  vector spaces affording absolutely irreducible continuous representations  $\varrho_i : \mathrm{G}_{\mathbb{Q}} \rightarrow \mathrm{Aut}_E(\mathcal{V}_i)$  for  $1 \leq i \leq m$ . Further assume that the modulo  $\varpi$  reductions of  $\varrho_i$  satisfy

$$\bar{\varrho}_i^{\mathrm{ss}} \cong \bar{\rho}_1 \oplus \bar{\rho}_2 \oplus \bar{\rho}_3$$

for some  $\mathrm{G}_{\mathbb{Q}}$ -stable lattice in  $\mathcal{V}_i$  (and hence for all such lattices.)

For each  $\sigma \in \mathrm{G}_{\mathbb{Q}}$ , let

$$\sum_{j=0}^n a_j(\sigma)X^j \in \mathcal{O}[X]$$

be the characteristic polynomial of  $(\rho_1 \oplus \rho_2 \oplus \rho_3)(\sigma)$  and

$$\sum_{j=0}^n c_j(i, \sigma)X^j \in \mathcal{O}[X]$$

be the characteristic polynomial of  $\varrho_i(\sigma)$ . Set

$$c_j(\sigma) = \begin{pmatrix} c_j(1, \sigma) \\ \vdots \\ c_j(m, \sigma) \end{pmatrix} \in \mathcal{O}^m$$

for  $0 \leq j \leq n-1$ . Let  $\mathbb{T} \subset \mathcal{O}^m$  be the  $\mathcal{O}$ -subalgebra generated by the set  $\{c_j(\sigma) : \sigma \in \mathbb{G}_{\mathbb{Q}}, 0 \leq j \leq n-1\}$ . We can use the continuity of the  $\varrho_i$  along with the Chebotarev density theorem to conclude that

$$\mathbb{T} = \{c_j(\text{Frob}_{\ell}) : 0 \leq j \leq n-1, \ell \neq p\}.$$

Observe that  $\mathbb{T}$  is a finite  $\mathcal{O}$ -algebra. Let  $I \subset \mathbb{T}$  be the ideal generated by the set  $\{c_j(\text{Frob}_{\ell}) - a_j(\text{Frob}_{\ell}) : 0 \leq j \leq n-1, \ell \neq p\}$ . The definition of  $I$  gives that the map  $\mathcal{O} \rightarrow \mathbb{T}/I$  giving the  $\mathcal{O}$ -algebra structure is surjective. Let  $J$  be the kernel of this map so that we have  $\mathcal{O}/J \cong \mathbb{T}/I$ .

**Corollary 8.5.** *Suppose  $\mathbb{F}^{\times}$  contains at least  $n$  distinct elements. Then there exists a  $\mathbb{G}_{\mathbb{Q}}$ -stable  $\mathbb{T}$ -submodule  $\mathcal{L} \subset \bigoplus_{i=1}^m \mathcal{V}_i$ ,  $\mathbb{T}$ -submodules  $\mathcal{L}_1, \mathcal{L}_2$  and  $\mathcal{L}_3$  contained in  $\mathcal{L}$  and finitely generated  $\mathbb{T}$ -modules  $\mathcal{T}_1, \mathcal{T}_2$  such that*

- (1) *as  $\mathbb{T}$ -modules we have  $\mathcal{L} = \mathcal{L}_1 \oplus \mathcal{L}_2 \oplus \mathcal{L}_3$  and  $\mathcal{L}_i \cong \mathbb{T}^{n_i}$  for  $1 \leq i \leq 3$ ;*
- (2)  *$\mathcal{L}$  has no  $\mathbb{T}[\mathbb{G}_{\mathbb{Q}}]$ -quotient isomorphic to  $\bar{\rho}'$  where  $\bar{\rho}'^{\text{ss}} = \bar{\rho}_1 \oplus \bar{\rho}_2$ ;*
- (3)  *$(\mathcal{L}_1 \oplus \mathcal{L}_2)/I(\mathcal{L}_1 \oplus \mathcal{L}_2)$  is  $\mathbb{G}_{\mathbb{Q}}$ -stable and there exists a  $\mathbb{T}[\mathbb{G}_{\mathbb{Q}}]$ -isomorphism*

$$\mathcal{L}/(\mathcal{L} + I(\mathcal{L}_1 \oplus \mathcal{L}_2)) \cong M_3 \otimes_{\mathcal{O}} \mathbb{T}/I$$

*for any  $\mathbb{G}_{\mathbb{Q}}$ -stable  $\mathcal{O}$ -lattice  $M_3 \subset V_3$ ;*

- (4) *one has either  $\text{Hom}_{\mathbb{T}/I}(M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1, M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) = 0$  or  $\text{Hom}_{\mathbb{T}/I}(M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2, M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1) = 0$  for any  $\mathbb{G}_{\mathbb{Q}}$ -stable  $\mathcal{O}$ -lattices  $M_i \subset V_i$  for  $i = 1, 2$ ;*
- (5)  *$\text{Fitt}_{\mathbb{T}}(\mathcal{T}_i) = 0$  for  $i = 1, 2$  and there exists a  $\mathbb{T}[\mathbb{G}_{\mathbb{Q}}]$ -isomorphism*

$$\mathcal{L}_i/I\mathcal{L}_i \cong M_i \otimes_{\mathcal{O}} \mathcal{T}_i/I\mathcal{T}_i$$

*for any  $\mathbb{G}_{\mathbb{Q}}$ -stable  $\mathcal{O}$ -lattice  $M_i \subset V_i$  for  $i = 1, 2$ .*

*Proof.* Everything in this corollary follows immediately from Theorem 6.1. Though Fitting ideals are not mentioned there, the proof that  $\text{Fitt}_{\mathbb{T}}(\mathcal{T}_i) = 0$  follows immediately from our work in § 6. See Lemma 9.13 of [KK07] for the details.  $\square$

We now specialize to our situation.

- $n_1 = n_3 = 1, n_2 = 2$ ;
- $\rho_1 = \varepsilon^{-1}, \rho_2 = \rho_f \otimes \varepsilon^{1-k}, \rho_3 = \text{id}$ . Note what we are doing here is looking at the components of the  $\rho_{F_f} \otimes \varepsilon^{1-k}$ .
- $\mathbb{T} = \mathbb{T}_{\mathfrak{m}_{F_f}}^{\text{NM}}$ ;
- $G_1, \dots, G_m$  for the elements in an orthogonal eigenbasis of  $\mathcal{S}_k^{\text{NM}}(\text{Sp}_4(\mathbb{Z}))$  such that  $\phi^{-1}(\mathfrak{m}_{G_i}^{\text{NM}}) = \mathfrak{m}_{F_f}$ .
- $I =$  the ideal of  $\mathbb{T}$  generated by  $\phi_{\mathfrak{m}_{F_f}}(\text{Ann } F_f)$ ;
- $(\mathcal{V}_i, \varrho_i) =$  the representation  $\rho_{G_i}$  for  $1 \leq i \leq m$ .

Let  $M_i$  be a  $\mathbb{G}_{\mathbb{Q}}$ -stable  $\mathcal{O}$ -lattice inside  $V_i$  for  $1 \leq i \leq 3$ . We will continue to use the matrix notation as was used in § 6 when it is convenient for our purposes. We now break into two cases depending on whether  $\text{Hom}_{\mathbb{T}/I}(M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1, M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) = 0$  or  $\text{Hom}_{\mathbb{T}/I}(M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2, M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1) = 0$ .

We begin with the case where  $\mathrm{Hom}_{\mathbb{T}/I}(M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1, M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) = 0$ . Consider the exact sequence

$$0 \longrightarrow \mathcal{N}_1 \oplus \mathcal{N}_2 \longrightarrow \mathcal{L} \otimes \mathbb{T}/I \xrightarrow{\quad s \quad} \rho_3 \otimes \mathbb{T}/I \longrightarrow 0,$$

where we have  $\mathcal{N}_i = M_i \otimes_{\mathcal{O}} \mathcal{T}_i/I\mathcal{T}_i$  for  $i = 1, 2$  (see Theorem 6.1 or Theorem 8.5 (3) and (5).) As we saw in § 7, this gives rise to a cocycle

$$\mathbf{c}_2 \in \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, \mathrm{Hom}_{\mathbb{T}/I}(M_3 \otimes_{\mathcal{O}} \mathbb{T}/I, M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2)).$$

Observe that we have

$$\mathrm{Hom}_{\mathbb{T}/I}(M_3 \otimes_{\mathcal{O}} \mathbb{T}/I, M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) \cong \mathrm{Hom}_{\mathcal{O}}(M_3, M_2) \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2$$

and so  $\mathbf{c}_2$  can be regarded as a cocycle in  $\mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, \mathrm{Hom}_{\mathcal{O}}(M_3, M_2) \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2)$ . Define a map

$$\begin{aligned} \iota_2 : \mathrm{Hom}_{\mathcal{O}}(\mathcal{T}_2/I\mathcal{T}_2, E/\mathcal{O}) &\rightarrow \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, \mathrm{Hom}_{\mathcal{O}}(M_3, M_2) \otimes_{\mathcal{O}} E/\mathcal{O}) \\ f &\mapsto (1 \otimes f)(\mathbf{c}_2). \end{aligned}$$

Our assumption that  $\mathrm{Hom}_{\mathbb{T}/I}(M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1, M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) = 0$  and the fact that modulo  $\varpi$  reduction of  $\rho_f \otimes \varepsilon^{1-k}$  is absolutely irreducible give that we can choose  $T = \mathrm{Hom}_{\mathcal{O}}(M_3, M_2)$  and we have  $W = \mathrm{Hom}_{\mathcal{O}}(M_3, M_2) \otimes_{\mathcal{O}} E/\mathcal{O}$ .

**Lemma 8.6.**  $\mathrm{Im}(\iota_2) \subseteq \mathrm{Sel}(W)$ .

*Proof.* As our representations are unramified away from  $p$ , the only thing remaining to prove is that the condition at  $p$  is satisfied. Observe that since  $\mathcal{T}_2/I\mathcal{T}_2$  is a finitely generated  $\mathbb{T}$ -module and  $\mathbb{T}/I \cong \mathcal{O}/J$ , it is also a finitely generated  $\mathcal{O}$ -module. Thus, there exists a positive integer  $n$  so that  $\mathrm{Hom}_{\mathcal{O}}(\mathcal{T}_2/I\mathcal{T}_2, E/\mathcal{O}) = \mathrm{Hom}_{\mathcal{O}}(\mathcal{T}_2/I\mathcal{T}_2, (E/\mathcal{O})[n])$ . Thus, we have

$$\mathrm{Im}(\iota_2) \subseteq \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, \mathrm{Hom}_{\mathcal{O}}(M_3, M_2) \otimes_{\mathcal{O}} (E/\mathcal{O})[n]) = \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, W[n]).$$

Proposition 7.4 gives that

$$\varinjlim_n \mathrm{H}_f^1(\mathbb{Q}_p, W[n]) \cong \mathrm{H}_f^1(\mathbb{Q}_p, W).$$

Thus, it is enough to show that  $\mathrm{Im}(\iota_2) \subseteq \mathrm{H}_f^1(\mathbb{Q}_p, W[n])$ . However, this follows from the fact that each  $(\rho_i, \mathcal{V}_i)$  is short and crystalline at  $p$ .  $\square$

**Lemma 8.7.**  $(\ker \iota_2)^\vee = 0$ .

*Proof.* Let  $f \in \ker \iota_2$ ,  $\mathcal{B}_f = (\mathcal{T}_2/I\mathcal{T}_2)/\ker f$ , and  $\mathcal{I}_f = (E/\mathcal{O})/\mathrm{Im} f$ . Consider the short exact sequence

$$0 \rightarrow \mathcal{B}_f \xrightarrow{f} E/\mathcal{O} \rightarrow \mathcal{I}_f \rightarrow 0.$$

We tensor this sequence with  $T$  and consider the long exact sequence of cohomology that results as well as the natural map  $\phi$ :

$$\begin{array}{ccc}
& \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) & \\
& \downarrow \phi & \searrow \mathrm{H}^1(1 \otimes f) \\
\mathrm{H}^0(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} \mathcal{I}_f) & \longrightarrow \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} \mathcal{B}_f) & \xrightarrow{\mathrm{H}^1(1 \otimes f)} \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} E/\mathcal{O}).
\end{array}$$

The fact that  $\mathrm{G}_{\mathbb{Q}}$  acts on  $M_3$  and  $M_2$  in such a way as to give rise to irreducible non-isomorphic representations gives that  $\mathrm{H}^0(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} \mathcal{I}_f) = 0$ . Thus, we must have  $\mathrm{H}^1(1 \otimes f)$  is an injective map. Since  $f \in \ker \iota_2$  by assumption, we have  $\mathrm{H}^1(1 \otimes f) \circ \phi(\mathfrak{c}_2) = 0$ . Thus, the fact that  $\mathrm{H}^1(1 \otimes f)$  is injective shows that  $\mathfrak{c}_2$  maps to 0 under the map  $\phi$ .

Given any  $g \in \mathrm{Hom}_{\mathcal{O}}(\mathcal{T}_2/I\mathcal{T}_2, E/\mathcal{O})$ , one has that  $\ker g$  has finite index in  $\mathcal{T}_2/I\mathcal{T}_2$ . So in particular, we have that there exists an  $\mathcal{O}$ -module  $A$  with  $\ker f \subseteq A \subset \mathcal{T}_2/I\mathcal{T}_2$  such that  $(\mathcal{T}_2/I\mathcal{T}_2)/A \cong \mathcal{O}/\varpi \cong \mathbb{F}$ . Thus we have that the image of  $\mathfrak{c}_2$  in  $\mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} \mathbb{F})$  is zero under the composite

$$\mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) \xrightarrow{\phi} \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} ((\mathcal{T}_2/I\mathcal{T}_2)/\ker f)) \rightarrow \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} \mathbb{F}).$$

We now consider  $\mathfrak{c}_1 \in \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, \mathrm{Hom}_{\mathbb{T}/I}(M_3 \otimes_{\mathcal{O}} \mathbb{T}/I, M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1))$ . Let  $T' = \mathrm{Hom}_{\mathcal{O}}(M_3, M_1)$ . Choose an  $\mathcal{O}$ -module  $B \subset \mathcal{T}_1/I\mathcal{T}_1$  so that  $(\mathcal{T}_1/I\mathcal{T}_1)/B \cong \mathbb{F}$ . The fact that  $\mathfrak{c}_2$  vanishes in  $\mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T \otimes_{\mathcal{O}} \mathbb{F})$  gives that  $T' \otimes_{\mathcal{O}} \mathbb{F} \cong \mathbb{F}(-1)$  where we write  $\mathbb{F}(-1)$  to indicate the finite field  $\mathbb{F}$  with a  $\mathrm{G}_{\mathbb{Q}}$ -action given by  $\omega^{-1}$ . Thus, if  $\mathfrak{c}_1$  is nonzero in  $\mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T' \otimes_{\mathcal{O}} \mathbb{F})$ , i.e., is nonzero in  $\mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, \mathbb{F}(-1))$ , we obtain, reasoning as above, an element in  $\mathrm{Sel}(\mathbb{F}(-1))$ . However, such an element gives a non-trivial finite unramified abelian  $p$ -extension  $K/\mathbb{Q}(\mu_p)$  with the action of  $\mathrm{Gal}(K/\mathbb{Q})$  on  $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$  given by  $\omega^{-1}$ . Thus, we obtain a non-trivial subgroup of the  $\omega^{-1}$ -isotypical piece of the  $p$ -part of the class group of  $\mathbb{Q}(\mu_p)$ . However, Herbrand's theorem says that this implies  $p \mid B_2 = \frac{1}{30}$ , clearly a contradiction. Thus, it must be that  $\mathfrak{c}_2$  is zero in  $\mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T' \otimes_{\mathcal{O}} \mathbb{F})$ . (See [Br07] pages 316-317 for the details of the argument showing  $\mathfrak{c}_2$  must be zero.) However, this gives that the exact sequence

$$0 \rightarrow (M_1 \otimes_{\mathcal{O}} \mathbb{F}) \oplus (M_2 \otimes_{\mathcal{O}} \mathbb{F}) \rightarrow (\mathcal{L}/I\mathcal{L})/\mathcal{L}' \rightarrow M_3 \otimes_{\mathcal{O}} \mathbb{F} \rightarrow 0$$

splits as a sequence of  $\mathbb{T}[\mathrm{G}_{\mathbb{Q}}]$ -modules where  $\mathcal{L}' = \varpi\mathcal{L} + (M_1 \otimes_{\mathcal{O}} B) + (M_2 \otimes_{\mathcal{O}} B)$ . This contradicts Corollary 8.5 (2). Thus, we have the result that  $(\ker \iota_2)^{\vee} = 0$ .  $\square$

We are now able to finish the proof of Theorem 8.3 in the case where  $\mathrm{Hom}_{\mathbb{T}/I}(M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1, M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) = 0$ .

*Proof.* (of Theorem 8.3) Lemma 8.6 immediately implies that we have the bound

$$\mathrm{ord}_p(\#S(W)) \geq \mathrm{ord}_p(\#(\mathrm{Im} \iota_2)^{\vee}).$$

Similarly, we use Lemma 8.7 to conclude that

$$\mathrm{ord}_p(\#(\mathrm{Im} \iota_2)^{\vee}) = \mathrm{ord}_p(\#\mathrm{Hom}_{\mathcal{O}}(\mathcal{T}_2/I\mathcal{T}_2, E/\mathcal{O})^{\vee}).$$

Applying ([H00], page 98) to our situation we obtain

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{T}_2/I\mathcal{T}_2, E/\mathcal{O})^\vee \cong (\mathcal{T}_2/I\mathcal{T}_2)^{\vee\vee} \cong \mathcal{T}_2/I\mathcal{T}_2.$$

This allows us to conclude that

$$\mathrm{ord}_p(\#(\mathrm{Im} \iota_2)^\vee) = \mathrm{ord}_p(\#\mathcal{T}_2/I\mathcal{T}_2).$$

Corollary 8.5 gives that  $\mathrm{Fitt}_{\mathbb{T}}(\mathcal{T}_2) = 0$  and so  $\mathrm{Fitt}_{\mathbb{T}}(\mathcal{T}_2 \otimes_{\mathbb{T}} \mathbb{T}/I) \subset I$ . Thus we have

$$\mathrm{ord}_p(\#(\mathcal{T}_2 \otimes_{\mathbb{T}} \mathbb{T}/I)) \geq \mathrm{ord}_p(\#\mathbb{T}/I).$$

However, as  $\mathrm{ord}_p(\#\mathcal{T}_2/I\mathcal{T}_2) = \mathrm{ord}_p(\#(\mathcal{T}_2 \otimes_{\mathbb{T}} \mathbb{T}/I))$ , we are able to combine these results to obtain

$$\mathrm{ord}_p(\#S(W)) \geq \mathrm{ord}_p(\#\mathbb{T}/I)$$

as desired.  $\square$

It now only remains to deal with the case where  $\mathrm{Hom}_{\mathbb{T}/I}(M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2, M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1) = 0$ . We will see this argument goes much as before so we will be able to reference the first case for most of the work. Again consider the cocycle

$$\mathbf{c}_1 \in H^1(G_{\mathbb{Q}}, \mathrm{Hom}_{\mathbb{T}/I}(M_3 \otimes_{\mathcal{O}} \mathbb{T}/I, M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1)).$$

As before, we have

$$\mathrm{Hom}_{\mathbb{T}/I}(M_3 \otimes_{\mathcal{O}} \mathbb{T}/I, M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1) \cong \mathrm{Hom}_{\mathcal{O}}(M_3, M_1) \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1$$

and so  $\mathbf{c}_1$  can be regarded as a cocycle in  $H^1(G_{\mathbb{Q}}, \mathrm{Hom}_{\mathcal{O}}(M_3, M_1) \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1)$ .

Define a map

$$\begin{aligned} \iota_1 : \mathrm{Hom}_{\mathcal{O}}(\mathcal{T}_1/I\mathcal{T}_1, E/\mathcal{O}) &\rightarrow H^1(G_{\mathbb{Q}}, \mathrm{Hom}_{\mathcal{O}}(M_3, M_1) \otimes_{\mathcal{O}} E/\mathcal{O}) \\ f &\mapsto (1 \otimes f)(\mathbf{c}_1). \end{aligned}$$

Our assumption that  $\mathrm{Hom}_{\mathbb{T}/I}(M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2, M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1) = 0$  give that we can choose  $T' = \mathrm{Hom}_{\mathcal{O}}(M_3, M_1) \cong \mathcal{O}(-1)$  and we have  $W' = \mathrm{Hom}_{\mathcal{O}}(M_3, M_1) \otimes_{\mathcal{O}} E/\mathcal{O} \cong (E/\mathcal{O})(-1)$ . As above in Lemma 8.6 we obtain that  $\mathrm{Im}(\iota_1) \subset \mathrm{Sel}((E/\mathcal{O})(-1))$ . However, as was used in the proof of Lemma 8.7,  $\mathrm{Sel}((E/\mathcal{O})(-1)) = 0$ . Thus, the image of  $\iota_1$  must be zero. This puts us back into the situation where  $T = \mathrm{Hom}_{\mathcal{O}}(M_3, M_2)$  and  $W = \mathrm{Hom}_{\mathcal{O}}(M_3, M_2) \otimes_{\mathcal{O}} E/\mathcal{O}$ . We now are exactly in the situation we were in before and so the same arguments apply and give us the proof of Theorem 8.3.

## REFERENCES

- [A80] A. Andrianov, *Modular descent and the Saito-Kurokawa conjecture*, Invent. Math. 53, 267-280 (1980).
- [B85] S. Böcherer, *Über die Funktionalgleichung automorpher L-Funktionen zur Siegelscher Modulgruppe*, J. reine angew. Math. 362 146-168 (1985).
- [Br] J. Brown, *Special values of L-functions on  $\mathrm{GSp}(4) \times \mathrm{GL}(2)$  and the non-vanishing of Selmer groups*, preprint.
- [Br08] J. Brown, *Residually reducible representations of algebras over local Artinian rings*, to appear PAMS.

- [Br07] J. Brown, *Saito-Kurokawa lifts and applications to the Bloch-Kato conjecture*, Compositio Math. 143 part 2, 290-322 (2007).
- [Bru99] J. Bruinier, *Nonvanishing modulo  $\ell$  of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. 98 no. 3, 595-611 (1999).
- [C94] H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, Contemp. Math. 165, 213-235 (1994).
- [CF80] C. Chai and G. Faltings, *Degeneration of Abelian Varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3.Folge Band 22, A Series of Modern Surveys in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, (1980).
- [DFG04] F. Diamond, M. Flach, and L. Guo, *The Tamagawa number conjecture of adjoint motives of modular forms*, Ann. Sc. École Norm. Sup. 37 (4) 663-727 (2004).
- [EZ85] M. Eichler and D. Zagier, *The theory of Jacobi forms*, Prog. in Math. 55, Birkhauser, Boston (1985).
- [F89] G. Faltings, *Crystalline cohomology and  $p$ -adic Galois representations*, Algebraic Analysis, Geometry and Number Theory, Proceedings of JAMI Inaugural Conference, John Hopkins Univ. Press, (1989).
- [Fo82] J. M. Fontaine, *Sur certains types de représentations  $p$ -adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*, Ann. Math. 115, 529-577 (1982).
- [G84] P. Garrett, *Pullbacks of Eisenstein series; applications*, Progress in Mathematics, Vol. 46, Birkhauser, Boston, (1984).
- [G92] P. Garrett, *Petersson inner products and Fourier coefficients*, Invent. Math., 107 no. 3, 453-481 (1992).
- [Geer] G. van der Geer, *Siegel modular forms*, arXiv:math/0605346v1.
- [H00] H. Hida, *Modular forms and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 69, Cambridge University Press, Cambridge, (2000).
- [KK07] K. Klosin, *Congruences among modular forms on  $U(2, 2)$  and the Bloch-Kato conjecture*, preprint (2007).
- [KS89] W. Kohnen and N.P. Skoruppa, *A certain Dirichlet series attached to Siegel modular forms of degree two*, Invent. Math. 95, 541-558 (1989).
- [KZ81] W. Kohnen and D. Zagier, *Values of  $L$ -Series of modular forms at the center of the critical strip*, Invent. Math., 64, 175-198 (1981).
- [M94] H. Matsumura, *Commutative ring theory*, Cambridge Advanced Studies in Mathematics, vol. 8, Cambridge University Press, Cambridge, (1994).
- [OS98] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo  $\ell$* , Ann. of Math. (2) 147, 453-470 (1998).
- [R76] K. Ribet, *A modular construction of unramified  $p$ -extensions of  $\mathbb{Q}(\mu_p)$* , Invent. Math. 34, 151-162 (1976).
- [Sh97] G. Shimura, *Euler products and Eisenstein series*, CBMS, Regional Conference Series in Mathematics, Vol. 93, AMS, Providence, (1997).
- [Sh95] G. Shimura, *Eisenstein series and zeta functions on symplectic groups*, Inv. Math. 119, 539-584 (1995).
- [Sh87] G. Shimura, *Nearly holomorphic functions on Hermitian symmetric space*, Math. Ann. 278, 1-28 (1987).
- [Sh83] G. Shimura, *Algebraic relations between critical values of zeta functions and inner products*, Am. J. Math. 104, 253-285 (1983).
- [Sh77] G. Shimura, *On the periods of modular forms*, Math. Ann. 229, 211-221 (1977).
- [Sh76] G. Shimura, *The special values of the zeta functions associated to cusp forms*, Comm. Pure and Applied Math., Vol. XXIX, 783-804 (1976).
- [SU] C. Skinner and E. Urban, *The Iwasawa main conjecture for  $GL(2)$* .
- [SU06] C. Skinner and E. Urban, *Sur les déformations  $p$ -adiques de certaines représentations automorphes*, JIMJ 5, 629-698, (2006).

- [U01] E. Urban, *Selmer groups and the Eisenstein-Klingen ideal*, Duke Math. J. 106 no. 3, 485-525 (2001).
- [U00] E. Urban, *Sur les représentations  $p$ -adiques associées aux représentations cuspidales de  $GS_{p,4/\mathbb{Q}}$* , à paraître aux actes du congrès “Formes Automorphes” du centre Emile Borel, Institute Henri Poincaré, (2000).
- [U99] E. Urban, *On residually reducible representations on local rings*, J. Algebra 212, 738-742 (1999).
- [V99] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. 98 no. 2, 397-419 (1999).
- [W81] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures. et Appl. 60, 375-484 (1981).
- [Wa95] L. Washington, *Galois cohomology*, Modular forms and Fermat’s last theorem (Boston, MA, 1995), Springer, New York, 101-120 (1997).
- [Wi90] A. Wiles, *The Iwasawa conjecture for totally real fields*, Annals of Math. (2) 131 no. 3, 493-540 (1990).
- [Z80] D. Zagier, *Sur la conjecture de Saito-Kurokawa*, Sé Delange-Pisot-Poitou 1979/80, Progress in Math. 12, Boston-Basel-Stuttgart, 371-394 (1980).

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA,  
CA 91125

*E-mail address:* jim1b@caltech.edu