Brown, J. (2011) "On the Cuspidality of Pullbacks of Siegel Eisenstein Series and Applications to the Bloch–Kato Conjecture,"
International Mathematics Research Notices, Vol. 2011, No. 7, pp. 1706–1756
Advance Access publication July 8, 2010
doi:10.1093/imrn/rnq135

On the Cuspidality of Pullbacks of Siegel Eisenstein Series and Applications to the Bloch–Kato Conjecture

Jim Brown

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634, USA

Correspondence to be sent to: jimlb@clemson.edu

Let $k > 9$ be an even integer and p a prime with $p > 2k-2$. Let f be a newform of weight $2k-2$ and level $\mathrm{SL}_2(\mathbb{Z})$ so that f is ordinary at p and $\overline{\rho}_{f,\mathfrak{p}}$ is irreducible. Under some additional hypotheses, we prove that $\mathrm{ord}_p(L_{\mathrm{alg}}(k, f)) \le \mathrm{ord}_p(\#S)$, where S is the Pontryagin dual of the Selmer group associated to $\rho_{f,\mathfrak{p}} \otimes \varepsilon^{1-k}$ with ε 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 $\mathrm{SL}_2(\mathbb{Z})$. 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 $\mathrm{ord}_p(L_{\mathrm{alg}}(k, f)) \ge 1$, then $\mathrm{ord}_p(\#\,\mathrm{Sel}(W)) \ge 1$ [4]. Unfortunately, due to limitations of the method used, one was unable to gain any more information than this. In this paper,

Received February 5, 2010; Revised May 2, 2010; Accepted June 16, 2010
Communicated by by Prof. Jim Cogdell

we improve upon these results yielding the much stronger result that under the same hypotheses needed before roughly speaking, one has

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

The method of proof is in the same spirit as was used in [4] with significant improvements at a couple of steps. Nevertheless, we briefly recount the method here.

The general outline of the method goes back to the work of Ribet on the proof of the converse of Herbrand's theorem [26]. This method has been generalized and applied in other contexts by several authors ([19], [35], [42], etc.) The method employed by Ribet (in a slightly more general form) is as follows. Given a positive integer k and a primitive Dirichlet character χ of conductor N so that $\chi(-1) = (-1)^k$, one has an associated Eisenstein series $E_{k,\chi}$ with constant term $(L(1-k, \chi))/2$. 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 $\overline{\rho}_{g,\mathfrak{p}} \simeq \begin{pmatrix} 1 & * \\ 0 & \chi\omega^{k-1} \end{pmatrix}$ is non-split where ω is the reduction of the p-adic cyclotomic character. This allows one to show that $*$ gives a nonzero cohomology class in $\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}, \chi^{-1}\omega^{1-k})$.

For our purposes, the character in Ribet's method will be replaced with a newform f of weight $2k-2$ and level $\mathrm{SL}_2(\mathbb{Z})$. 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 ϖ^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 [31] as key ingredients. It is at this step that a significant improvement over the results of [4] 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 [4] that "lost the powers of p." Once we have the congruence desired, we generalize results of Urban [38] 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 [4] and allows us to get the lower bound desired.

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 $\mathrm{ord}_p(n)$ to denote m for $p^m \parallel n$. We denote by ε_p the p-adic cyclotomic character $\varepsilon_p : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_1(\mathbb{Z}_p)$. We drop the p when it is clear from context. We denote the residual representation of ε_p by ω_p, again dropping the p when it is clear from context.

For a ring R, we let $\mathrm{M}_{m,n}(R)$ denote the set of m by n matrices with entries in R. If $m = n$, we write $\mathrm{M}_m(R)$ for $M_{m,m}(R)$. For a matrix $x \in \mathrm{M}_{2n}(R)$, 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 $\mathrm{M}_n(R)$. We drop the subscript x when it is clear from the context. The transpose of a matrix x is denoted by ${}^t x$.

Let SL_2 and 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

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

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 [12].

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

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

when we restrict to places away from Σ and

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

when we restrict to the places in Σ.

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 Γ. We let $S_k(\Gamma)$ denote the subspace of cusp forms. The nth 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

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

where $\overline{\mathrm{SL}_2(\mathbb{Z})} = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1_2\}$ and $\overline{\Gamma}$ is the image of Γ in $\overline{\mathrm{SL}_2(\mathbb{Z})}$. The nth 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 $n = 1, 2, 3, \ldots$. 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 pth Satake parameters of f.

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

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

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

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

We denote the space of Jacobi cusp forms on Γ_1^{J} by $J_{k,1}^{\mathrm{cusp}}(\Gamma_1^{\mathrm{J}})$. The inner product is given by

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

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

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

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

We will be particularly interested in the decomposition

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

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

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

We let $T^S(n)$ denote the nth Siegel Hecke operator. As above, we set $\mathbb{T}_{\mathbb{Z}}^S$ to be the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(\mathcal{S}_k(\mathrm{Sp}_{2n}(\mathbb{Z}))$ 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 $\mathcal{S}_k(\mathrm{Sp}_4(\mathbb{Z}))$ into the space of Maass and non-Maass forms [1].

Let $F \in \mathcal{S}_k(\mathrm{Sp}_4(\mathbb{Z}))$ 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

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

One can also define the spinor L-function in terms of the Satake parameters α_0, α_1, and α_2 of F. One has

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

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

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

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 ϕ, the twisted standard zeta function is given by

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

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 Sp_{4n} to $\mathrm{Sp}_{2n} \times \mathrm{Sp}_{2n}$ is cuspidal in each variable. We use the methods developed by Garrett [16] along with standard facts about Siegel Eisenstein series to establish this result. We also recall facts that can be found in [4] 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 [31]. One can also see [3], [15], or [25] for analogous results.

3.1 Basic definitions and results

We begin by recalling the definition of some subgroups of $\mathrm{Sp}_{2m}(\mathbb{A})$ and $\mathrm{Sp}_{2m}(\mathbb{Q})$. Let $N > 1$ be an integer, and let Σ be the set of primes dividing N. For a prime ℓ, define

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

and set

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

Set

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

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

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

Set

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

Let $P_{2m} = U_{2m}Q_{2m}$ be the Siegel parabolic of Sp_{2m} defined by

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

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 χ be a Hecke character of $\mathbb{A}^\times$ satisfying

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

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

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

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 $E(g, (m+1)/2 - s)$. One can work out the precise functional equation via the general theory contained in [22], but the exact functional equation will not be needed.

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 [22, 30]. We will use whichever of these Siegel Eisenstein series is most convenient for the current application, keeping in mind the functional equation relating them.

Finally, we recall a result on the Fourier coefficients of $E(Z, (m+1)/2 - k/2)$ demonstrated in [4]. 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 $Y > 0$. $L = \mathbb{S}^m(\mathbb{Q}) \cap \mathrm{M}_m(\mathbb{Z})$, $L' = \{\mathfrak{s} \in \mathbb{S}^m(\mathbb{Q}) : \mathrm{Tr}(\mathfrak{s}L) \subseteq \mathbb{Z}\}$, and $M = N^{-1}L'$. The Eisenstein series $E^*(Z, s)$ has a Fourier expansion

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

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

$$D_{E^*}(Z, (m+1)/2 - k/2) = \pi^{-\frac{m(m+2)}{4}} \Lambda^{\Sigma}((m+1)/2 - k/2, \chi) E^*(Z, (m+1)/2 - k/2). \tag{3}$$

Then

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

3.2 Pullbacks of Siegel Eisenstein series

We begin by reviewing the notion of the pullback of an automorphic form on $\mathrm{Sp}_{4n}(\mathbb{A})$ to $\mathrm{Sp}_{2n}(\mathbb{A}) \times \mathrm{Sp}_{2n}(\mathbb{A})$. This theory has been well established, and the interested reader is advised to consult any of the following references for more details: [3, 15, 16, 31, 32].

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

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

One can show that given a holomorphic automorphic form F of weight k and level $\Gamma_0^{(4n)}(N)$ on $\mathrm{Sp}_{4n}(\mathbb{A})$, the function $(g_1, g_2) \mapsto F(\iota(g_1, g_2))$ is a holomorphic automorphic form of weight k and level $\Gamma_0^{(2n)}(N)$ in each variable, see [16] for example. The form

$F(\iota(g_1, g_2))$ is referred to as the pullback of F from Sp_{4n} to $\mathrm{Sp}_{2n} \times \mathrm{Sp}_{2n}$, or just the pullback of F. We will often drop the ι 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

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

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

We now show that the pullback Eisenstein series $E(\iota(g_1, g_2), k/2)$ is cuspidal in g_1 and g_2. We restrict now to the case that $k > 4n+1$ to ensure that the series defining the Eisenstein series converges. We wish to apply the methods used by Garrett in [16]. To do this, we restrict our Eisenstein series from $P_{4n}(\mathbb{A})K_0(N)$ to $P_{4n}(\mathbb{A})K(N)$ where $K(N) = K_\infty \prod_{\ell \nmid \infty} K_\ell(N)$ with

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

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

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

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 [16].

Let $\theta \in \mathrm{Sp}_{4n}(\mathbb{A}_f)$ 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 θ, 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

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

has representatives $\tau_0, \tau_1, \ldots, \tau_n$ 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 [16] for a proof. Let I_i be the isotropy group of $P_{4n}(\mathbb{Q})\tau_i$ in $P_{4n}(\mathbb{Q})\backslash \operatorname{Sp}_{4n}(\mathbb{Q})$ under $\operatorname{Sp}_{2n}(\mathbb{Q}) \times \operatorname{Sp}_{2n}(\mathbb{Q})$ acting on the right, that is,

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

This allows us to write our Eisenstein series as

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

where

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

Our goal now is to show that $\vartheta_i(g_1, g_2) = 0$ for all $g_1, g_2 \in \operatorname{Sp}_{2n}(\mathbb{Q})$ 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 $g_1, g_2 \in \operatorname{Sp}_{2n}(\mathbb{Q}_p)$ In order to show this, we give an integral representation of the Eisenstein series components ϵ_p.

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

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

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

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

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 $g(0_{2n} 1_{2n})\tau_i \iota(g_1, g_2)\theta^{-1} \equiv (0_{2n} 1_{2n}) (\mathrm{mod}\, N)$, that is,

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

Define $\psi : M_{2n,4n} \to M_{2n}$ 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 θ 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

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

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

$$I_n = \{\iota(g_1, g_2) : g_2 = \hat{g}_1\} \tag{4}$$

where $\hat{g} = \beta g \beta$ with $\beta = \begin{pmatrix} -1_n & 0_n \\ 0_n & 1_n \end{pmatrix}$. From this, we see that for $\iota(g_1, g_2) \in \iota(\mathrm{Sp}_{2n}(\mathbb{Q}) \times \mathrm{Sp}_{2n}(\mathbb{Q}))$, we have

$$\iota(g_1, g_2) \equiv \iota(g_1\hat{g}_2^{-1}, 1) \pmod{I_n}.$$

It is straightforward to check that every element of $\mathrm{Sp}_{2n}(\mathbb{Q})$ can be written in the form $g_1\hat{g}_2^{-1}$, and so we can take $\iota(\mathrm{Sp}_{2n}(\mathbb{Q}) \times \{1\})$ as a collection of representatives for $I_n \backslash \iota(\mathrm{Sp}_{2n}(\mathbb{Q}) \times \mathrm{Sp}_{2n}(\mathbb{Q}))$. This allows us to write

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

Since we are interested in unfolding this along the unipotent radical in the first variable, we observe that we can choose the representatives of $I_n \backslash \iota(\mathrm{Sp}_{2n}(\mathbb{Q}) \times \mathrm{Sp}_{2n}(\mathbb{Q}))$ to be $\{\iota(u, \hat{\gamma}^{-1}) : u \in U_{2n}(\mathbb{Q}), \gamma \in \mathrm{Sp}_{2n}(\mathbb{Q})/U_{2n}(\mathbb{Q})\}$. Thus, we can write

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

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 σ-th Fourier coefficient is zero for all $g_1, g_2 \in \mathrm{Sp}_{2n}(\mathbb{A})$ unless σ is totally positive definite. Recall the Fourier coefficient given by

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

where we recall that ψ 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

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

We restrict ourselves now to looking at the infinite place as this is the place that forces the vanishing of the integral for σ 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

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

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 ϵ_∞. One can use the fact that τ_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

$$\tau_{n^\iota}(u(g)g_1, g_2) = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ A_1 & A_2 & g\,{}^tA_1^{-1} & x\,{}^tA_2^{-1} \\ 0 & 0 & -{}^tA_1^{-1} & {}^tA_2^{-1} \end{pmatrix},$$

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 ϵ_∞ 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

$$\epsilon_\infty(\tau_{n^\iota}(u(g)g_1, g_2), k/2) = \chi(\det \tilde{A}) \det\left(i\begin{pmatrix} A_1 & A_2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} g\,{}^tA_1^{-1} & x\,{}^tA_2^{-1} \\ -{}^tA_1^{-1} & {}^tA_2^{-1} \end{pmatrix}\right)^{-k}$$

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

$$i\begin{pmatrix} A_1 & A_2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} g\,{}^tA_1^{-1} & x\,{}^tA_2^{-1} \\ -{}^tA_1^{-1} & {}^tA_2^{-1} \end{pmatrix} = \begin{pmatrix} iA_1\,{}^tA_1 + g & iA_2\,{}^tA_2 + x \\ -1 & 1 \end{pmatrix}\begin{pmatrix} {}^tA_1^{-1} & 0 \\ 0 & {}^tA_2^{-1} \end{pmatrix}.$$

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

$$\begin{aligned}\epsilon_\infty(\tau_n\iota(u(g)g_1, g_2), k/2) &= \chi(\det\tilde{A})(\det A_1 \det A_2)^{-1}\det(g + x + iA_1\,{}^tA_1 + iA_2\,{}^tA_2)^{-k}\\ &= \chi(\det\tilde{A})(\det A_1 \det A_2)^{-1}\det(g+z)^{-k}\end{aligned}$$

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

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

unless σ is totally positive definite. This last equality is a classic result due to Siegel [33]. Alternatively, one can see [6] for an explicit proof of this result provided by Paul Garrett. Thus, we have that $E'(\iota(g_1, g_2)\theta^{-1}, k/2)$ is a holomorphic cuspform in g_1. Similarly, we have that it is a holomorphic cuspform in g_2 as well. Our previous comments allow us to conclude from this that $E(\iota(g_1, g_2), k/2)$ is a holomorphic cuspform in g_1 and g_2. In particular, the associated classical Eisenstein series $E(\mathrm{diag}[Z, W], k/2)$ is a holomorphic cuspform in Z and W.

As was mentioned before, there is a functional equation for the Eisenstein series relating s to $(2n+1)/2 - s$ in this case (our m from the previous subsection is $2n$ here). In particular, there is a function $h(s)$ so that

$$E(\mathrm{diag}[Z, W], (2n+1)/2 - s) = h(s)E(\mathrm{diag}[Z, W], s).$$

While $h(s)$ can be made explicit via [22], it is not necessary for our purposes. Observe that if we specialize to the case $s = k/2$, we know that $E(\mathrm{diag}[Z, W], (2n+1)/2 - k/2)$ and $E(\mathrm{diag}[Z, W], k/2)$ are both known to be holomorphic [22, 30]. In particular, since neither is exactly the zero function, we have that $h(s)$ cannot have a pole or zero at $s = k/2$.

We now recall the Siegel operator Φ_n. This is a linear operator taking modular forms on $\mathrm{Sp}_{2n}(\mathbb{Z})$ to $\mathrm{Sp}_{2n-2}(\mathbb{Z})$ for any $n \geq 2$. For $F \in \mathcal{M}_k(\Gamma)$ with $\Gamma \subset \mathrm{Sp}_{2n}(\mathbb{Z})$ a congruence subgroup, the Siegel operator is defined by

$$\Phi_n(F(\tau)) = \lim_{\lambda\to\infty} F\begin{pmatrix}\tau & 0\\ 0 & i\lambda\end{pmatrix}$$

where $\tau \in \mathfrak{h}^{n-1}$. Our interest in this operator is the following result.

Theorem 3.2. [2, Theorem 3.13] Let $F \in \mathcal{M}_k(\Gamma)$ for Γ a congruence subgroup of $\mathrm{Sp}_{2n}(\mathbb{Z})$. If $\Phi_n(F|_\gamma) = 0$ for every $\gamma \in \mathrm{Sp}_{2n}(\mathbb{Z})$, then F is a cuspform and conversely. □

We apply this theorem to our restricted Eisenstein series. In particular, viewing $E(\mathrm{diag}[Z, W], k/2)$ as a holomorphic modular form in Z, we have that $\Phi_{2n}(E(\mathrm{diag}[Z, W], k/2)) = 0$. Using the fact that the map is linear, we have that

$$\Phi_{2n}(E(\mathrm{diag}[Z, W], (2n+1)/2 - k/2)|_{\gamma\times 1}) = h(k/2)\Phi_{2n}(E(\mathrm{diag}[Z, W], k/2)|_{\gamma\times 1}) = 0$$

for each $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$. Thus, $E(\mathrm{diag}[Z, W], (2n+1)/2 - k/2)$ is a holomorphic cuspform in the variable Z. The variable W is handled in the same manner. Note that one could also show this by just expanding each side of the functional equation in its Fourier expansion. Thus, we obtain that $E(\mathrm{diag}[Z, W], (2n+1)/2 - k/2)$ is a holomorphic cuspform of weight k and level $\Gamma_0^{(2n)}(N)$ in Z and W independently.

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 [31] for a detailed treatment of this material. We specialize to the case of $\mathrm{Sp}_4 \times \mathrm{Sp}_4$ embedded in 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 [31, equation (6.17)] to our situation, we obtain

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

where $D_{E|_\rho}$ is the normalized Eisenstein series as defined in equation (3), $\mathcal{A}_{k,N} = ((-1)^k 2^{2k-3} v_N)/(3\,[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma_0^{(4)}(N)])$, $v_N = \pm 1$, $L_{\mathrm{st}}^{\Sigma}(5-k, F, \chi)$ is the standard zeta function as defined in equation (1), and $(F|_{\varsigma})^{c}$ denotes 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 [12, 17, 43]. For the facts we will be interested in, the reader is advised to consult the section on Saito–Kurokawa lifts in [4]. 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 $\mathcal{O}$ and $k \geq 2$ an even integer. The Saito–Kurokawa correspondence associates to f a cuspidal Siegel eigenform F_f in the Maass spezialschar $\mathcal{S}_k^{\mathrm{M}}(\mathrm{Sp}_4(\mathbb{Z}))$. 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 $D < 0$. The second isomorphism is between $J^{\mathrm{cusp}}_{k,1}(\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2)$ 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 $J^{\mathrm{cusp}}_{k,1}(\mathrm{SL}_2(\mathbb{Z}) \ltimes \mathbb{Z}^2)$ and the space of Maass spezialschar $\mathcal{S}_k^{\mathrm{M}}(\mathrm{Sp}_4(\mathbb{Z}))$ 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 [12, 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 ϕ by

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

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. [43] 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

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

□

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

Corollary 4.2. [4, 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 $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ be newform and F_f the Saito–Kurokawa lift of f. One has that $F_f^c = F_f$. □

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. Thus, we have that $F_f^c = F_{f^c}$. However, since f is a newform, we know that $f^c = f$. This follows immediately from the fact that the Hecke operators are self-adjoint with respect to the Petersson product. This gives the result. ■

We will also make use of the following three results.

Theorem 4.4. [20, 21] 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 $D < 0$ and χ_D is the character associated to the field $\mathbb{Q}(\sqrt{D})$. □

Theorem 4.5. [4, Theorem 3.10] Let N be a positive integer, Σ the set of primes dividing N, and χ 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, $\rho_{f,\lambda}$ the associated ℓ-adic Galois representation, F_f the Saito–Kurokawa lift, and $\rho_{F_f,\lambda}$ the associated 4-dimensional ℓ-adic Galois representation. Then one has

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

where ε is the ℓ-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 [4], 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 $\rho_{F_f,\lambda}$ is necessarily semi-simple, and the Brauer–Nesbitt theorem. ■

5 Congruences between Saito–Kurokawa Lifts and Non-Maass Forms

In this section we will use the results obtained in Section 3 as well as arguments originally used in [4] to produce a congruence between a Saito–Kurokawa lift F_f and a form

$G \in \mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z}))$. This congruence will provide the foundation for providing the lower bound on the size of the appropriate Selmer group in Section 8.

Let $k > 9$ be an even 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 ϖ. 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 $\mathrm{ord}_{\varpi}(A_F(T) - A_G(T)) \geq m$ for all T. If F and G are Hecke eigenforms, we denote a congruence between the eigenvalues as $F \equiv_{\mathrm{ev}} G \pmod{\varpi^m}$.

Let $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$ be a newform and F_f the Saito–Kurokawa lift of f. As in [4], we begin by replacing the normalized Eisenstein series $D_{E|_\rho}(\mathrm{diag}[Z, W], (5-k)/2)$ by its trace so as to work with level 1. Write

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

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 [10, Proposition 1.5].

Let $f_0 = f, f_1, \ldots, f_m$ be an orthogonal basis of newforms for $S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}))$, and let $F_0 = F_f, F_1 = F_{f_1}, \ldots, F_m = F_{f_m}, F_{m+1}, \ldots, F_r$ be an orthogonal basis of eigenforms of $\mathcal{S}_k(\mathrm{Sp}_4(\mathbb{Z}))$. Note that 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 χ. 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 [29, Lemma 1.1] or [15] for the general principles of such expansions.

Proposition 5.1. With the notation as above, we have

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

that is, $c_{i,j} = 0$ unless $i = j$. In particular, one has

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

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

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

On the other hand, combining the facts that

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

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

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

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

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

Since j_0 was arbitrary, we have

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

with the $c_{i,i}$ as desired. ■

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 $1 \le i \le m$. First, we need the following result, giving the existence of complex periods.

Theorem 5.2. [28, Theorem 1] Let $f \in S_{2k-2}(\mathrm{SL}_2(\mathbb{Z}), \mathcal{O})$ 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 χ, 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 χ and $\mathcal{O}_\chi$ is the extension of $\mathcal{O}$ generated by the values of χ. We write $L_{\mathrm{alg}}(m, f, \chi)$ to denote the value $L(m, f, \chi)/(\tau(\chi)(2\pi i)^m)$. □

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

Theorem 5.3. [4, Theorem 5.4] Let $f = f_0, f_1, \ldots, f_m$ 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 $\overline{\rho}_{f,\mathfrak{p}}$ 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 $\alpha = u\langle f, f\rangle / \Omega_f^+ \Omega_f^-$, u is a unit in $\mathcal{O}$. □

From this point on we assume that f is ordinary at $\mathfrak{p}$ and $\overline{\rho}_{f,\mathfrak{p}}$ 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, that is, the congruence is a congruence of Fourier coefficients.

Applying the fact that the Saito–Kurokawa correspondence is Hecke-equivariant, we are able to conclude that 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

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

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 $\mathrm{ord}_{\varpi}(\alpha c_{0,0}) = M < 0$, that is, there exists a ϖ-unit β 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 ϖ-integral Fourier coefficients, $t^S\mathcal{E}(Z, W)$ does as well. Thus, upon multiplying both sides of the equation by ϖ^{-M}, we obtain that $F_0(Z)F_0^c(W) \equiv 0 (\mathrm{mod}\, \varpi)$, clearly a contradiction.

We now expand each side of equation (10) in terms of W, reduce modulo ϖ, and equate T_0^{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

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

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 $G \equiv 0 (\mathrm{mod}\, \varpi^{-M})$, 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 $\mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z}))$ and as we noted earlier that this space is stable under Hecke operators, we have that $t^S F_j$ is in $\mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z}))$ for $m < j \leq r$. As G is a linear combination of forms in $\mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z}))$, we must have $G \in \mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z}))$. Thus, if we show that $\mathrm{ord}_{\varpi}(\alpha c_{0,0})$ is less then 0, we have a nontrivial congruence between F_f and a form in $\mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z}))$, 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 [4] 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 $\langle F_f, F_f \rangle$. Following the same argument as in [4], we are able to conclude that

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

where

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

and

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

where $D<0$ is a fundamental discriminant so that $\chi_D(-1)=-1$. It was shown in [4] that as long as $\gcd(p, D[\mathrm{Sp}_4(\mathbb{Z}):\Gamma_0^{(4)}(N)])=1$ one has $\mathrm{ord}_\varpi(\mathcal{B}_{k,N,D,\chi})\leq 0$. Thus, we obtain a divisibility condition on L-functions associated to f guaranteeing the existence of the congruence which allows us to conclude the following theorem.

Theorem 5.4. Let $k>9$ be an even 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 and F_f the Saito–Kurokawa lift of f. Let f be ordinary at p and $\overline{\rho}_{f,\mathfrak{p}}$ be irreducible. If there exists $N>1$, a fundamental discriminant $D<0$ so that $\chi_D(-1)=-1$, $p\nmid ND[\mathrm{Sp}_4(\mathbb{Z}):\Gamma_0^{(4)}(N)]$, and a Dirichlet character χ of conductor N so that

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

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

$$F_f \equiv G(\mathrm{mod}\,\varpi^M). \qquad \square$$

We repeat Lemma 6.4 of [4] here for completeness, though it will not be needed.

Lemma 5.5. With the setup as in Theorem 5.4, there exists an eigenform $F\in\mathcal{S}_k^{\mathrm{NM}}(\mathrm{Sp}_4(\mathbb{Z}))$ so that $F_f\equiv_{\mathrm{ev}} F(\mathrm{mod}\,\varpi)$. $\square$

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 ϖ. Write $\mathfrak{m}_{F_f}$ for the maximal ideal corresponding to F_f, that is, $\mathfrak{m}_{F_f}$ is the kernel of the $\mathcal{O}$-algebra homomorphism $\lambda_{F_f}:\mathbb{T}_{\mathcal{O}}^S\to\mathcal{O}$ 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 $\mathfrak{m}_{F_f}$, that is, if $F\not\equiv_{\mathrm{ev}} F_f(\mathrm{mod}\,\varpi)$.

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

We close this section by phrasing our results in terms of the CAP ideal [19]. This ideal can be thought of as a generalization of the Eisenstein ideal to our situation. As the Eisenstein ideal measures congruences to be Eisenstein series, the CAP ideal measures congruences between F_f and non-CAP modular forms.

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

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

As the map ϕ is surjective, one has that $\phi(\mathrm{Ann}(F_f))$ is an ideal in $\mathbb{T}_{\mathcal{O}}^{\mathrm{NM}}$. 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: 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 $r \geq M$. □

$$\begin{tikzcd}
\mathbb{T}_{\mathcal{O}}^{S} \arrow[r, "\phi"] \arrow[d] & \mathbb{T}_{\mathcal{O}}^{\mathrm{NM}} \arrow[d] \\
\mathbb{T}_{\mathcal{O}}^{S}/\,\mathrm{Ann}(F_f) \arrow[r, "\phi"] \arrow[d, "\lambda_{F_f}"] & \mathbb{T}_{\mathcal{O}}^{\mathrm{NM}}/\phi(\mathrm{Ann}(F_f)) \arrow[d, "\simeq"] \\
\mathcal{O} \arrow[r] & \mathcal{O}/\varpi^r\mathcal{O}.
\end{tikzcd}$$

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 $t \in \mathrm{Ann}(F_f)$, and so the congruence in Theorem 5.4 gives $\varpi^r G \equiv 0 (\mathrm{mod}\, \varpi^M)$, that is,

$$G \equiv 0 (\mathrm{mod}\, \varpi^{M-r}).$$

Now assume that $r < M$. The fact that $F_f \equiv G(\operatorname{mod} \varpi^M)$ and $G \equiv 0(\operatorname{mod} \varpi)$ implies that

$$F_f \equiv 0(\operatorname{mod} \varpi).$$

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

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 [38]. Whereas his result deals with the case of $\overline{\rho}^{\mathrm{ss}}$ splitting into two irreducible representations, our results are for when $\overline{\rho}^{\mathrm{ss}}$ splits into three irreducible representations. The proofs given here are adapted from those in [38] to our situation. As Theorem 1.1 of [38] is a variant of the main result of [36], our result here is very much a variant of the main result of [5]. The results contained in this section or some alternative version of them will also appear in [34].

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

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

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

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

1. the coefficients of the characteristic polynomial of ρ belong to $\mathscr{R}$;
2. the characteristic polynomials of ρ and $\rho_1 \oplus \rho_2 \oplus \rho_3$ are congruent modulo I;
3. the residual representations $\overline{\rho}_i$ are absolutely irreducible for $1 \leq i \leq 3$;
4. $\overline{\rho}_i \not\equiv \overline{\rho}_j$ if $i \neq j$.

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

$$\begin{tikzcd} 0 \arrow[r] & \mathscr{N}_1 \oplus \mathscr{N}_2 \arrow[r] & \mathscr{L} \otimes \mathscr{R}/I \arrow[r] & \rho_3 \otimes \mathscr{R}/I \arrow[l, bend right, "s"'] \arrow[r] & 0, \end{tikzcd}$$

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

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

$$\rho_\wp : \mathscr{A} \to \mathrm{M}_n(\mathcal{O}_\wp) \tag{11}$$

with

$$\overline{\rho}_\wp(a) = \begin{pmatrix} \overline{\rho}_1(a) & \star_1 & \star_2 \\ \star_3 & \overline{\rho}_2(a) & \star_4 \\ 0 & 0 & \overline{\rho}_3(a) \end{pmatrix} \tag{12}$$

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

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

We adopt the convention that $\sigma(3) = 3$. Write $n_i' = \sum_{j=1}^{i} n_i$, $\varrho_i = \rho_{\sigma(i)}$, $m_i = n_{\sigma(i)}$, and $m_i' = \sum_{j=1}^{i} m_j$. Set $\rho_{\widetilde{\mathscr{R}}} = (\rho_\wp)_\wp : \mathscr{A} \to \mathrm{M}_n(\widetilde{R})$.

The fact that each $\overline{\rho}_i$ is absolutely irreducible implies that $\mathrm{im}\overline{\rho}_i = \mathrm{M}_{n_i}(\kappa_{\mathscr{R}})$. Combining this with $\overline{\rho}_i \not\equiv \overline{\rho}_j$ if $i \neq j$ allows us to conclude that there exists $a_0 \in \mathscr{A}$ so that $\det(X - \overline{\rho}_{\widetilde{\mathscr{R}}}(a_0))$ has n distinct roots $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ where $\overline{\rho}_{\widetilde{\mathscr{R}}}(a) \in \mathrm{M}_n(\widetilde{R}/\operatorname{Rad}(\widetilde{\mathscr{R}}))$. Hensel's lemma guarantees that there exist n distinct elements $\alpha_1, \dots, \alpha_n \in \mathscr{R}$ that are roots of $\det(X - \rho_{\widetilde{\mathscr{R}}}(a_0))$ so that $\alpha_i \equiv \overline{\alpha}_i (\operatorname{mod} \mathfrak{m}_{\mathscr{R}})$. After a change of basis, we may assume that

$$\rho_{\widetilde{\mathscr{R}}}(a_0) = \operatorname{diag}(\alpha_1, \dots, \alpha_n).$$

Lemma 2.1 of [5] gives that the $\mathscr{R}$-submodule of $\mathrm{M}_n(\widetilde{\mathscr{R}})$ generated by the powers of $\rho_{\widetilde{\mathscr{R}}}(a_0)$ is exactly the set of diagonal matrices with entries in $\mathscr{R}$. So for all i with $1 \leq i \leq n$, there exists $f_i \in \mathscr{A}$ so that

$$\rho_{\widetilde{\mathscr{R}}}(f_i) = E(\alpha_i) = \operatorname{diag}(0, \dots, 0, 1, 0, \dots 0)$$

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

$$\rho_{\widetilde{\mathscr{R}}}(a_1) = E_1 = \begin{pmatrix} 1_{n_1} & 0 & 0 \\ 0 & 0_{n_2} & 0 \\ 0 & 0 & 0_{n_3} \end{pmatrix},$$

$$\rho_{\widetilde{\mathscr{R}}}(a_2) = E_2 = \begin{pmatrix} 0_{n_1} & 0 & 0 \\ 0 & 1_{n_2} & 0 \\ 0 & 0 & 0_{n_3} \end{pmatrix},$$

and

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

Similarly, we define a_1', a_2', and a_3' to be the elements in $\mathscr{A}$ so that

$$\rho_{\widetilde{\mathscr{R}}}(a_1') = E_1' = \begin{pmatrix} 1_{m_1} & 0 & 0 \\ 0 & 0_{m_2} & 0 \\ 0 & 0 & 0_{m_3} \end{pmatrix},$$

$$\rho_{\widetilde{\mathscr{R}}}(a_2') = E_2' = \begin{pmatrix} 0_{m_1} & 0 & 0 \\ 0 & 1_{m_2} & 0 \\ 0 & 0 & 0_{m_3} \end{pmatrix},$$

and

$$\rho_{\widetilde{\mathscr{R}}}(a_3') = E_3' = \begin{pmatrix} 0_{m_1} & 0 & 0 \\ 0 & 0_{m_2} & 0 \\ 0 & 0 & 1_{m_3} \end{pmatrix}.$$

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

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

Proof. This is Lemma 1.1 of [38]. We give the proof here for $i = 3$ as the other two cases are identical. The definition of $\mathscr{L}_3$ given that $\mathscr{L}_3 \otimes_{\mathscr{R}} \kappa_{\mathscr{R}}$ is generated by

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

as a runs through $\mathscr{A}$. The fact that $\mathrm{im}\overline{\rho}_3 = \mathrm{M}_{n_3}(\kappa_{\mathscr{R}})$ gives that $\mathscr{L}_3 \otimes_{\mathscr{R}} \kappa_{\mathscr{R}} = \kappa_{\mathscr{R}}\overline{e}_{n_2'+1} \oplus \cdots \oplus \kappa_{\mathscr{R}}\overline{e}_n$. For $n_2' + 1 \leq i \leq n$, let $e_i' \in \mathscr{L}_3$ be a lifting of $\overline{e}_i$. Theorem 2.3 in [23] (essentially Nakayama's lemma) gives that $\mathscr{L}_3 = \mathscr{R}e'_{n_2'+1} + \cdots + \mathscr{R}e'_n$. We can now use the fact that $\mathscr{L}_3 \otimes_{\mathscr{R}} F_{\mathscr{R}}$ is of rank $n_3 = n - n_2'$ over $F_{\mathscr{R}}$ to conclude that the sum must be direct. ■

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

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

where

$$A^{i,j}(a) = \mathrm{Res}_{\mathscr{L}_{\sigma(j)}}(E_i' \circ \rho_{\widetilde{\mathscr{R}}}(a)) \in \mathrm{Hom}_{\mathscr{R}}(\mathscr{L}_{\sigma(j)}, \mathscr{L}_{\sigma(i)}).$$

Lemma 6.3. The map

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

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

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

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

Proof. This is a generalization of Lemma 1.2 of [38]. The necessary work was done in Lemma 2.3 of [5], so here we merely reduce to what was shown there.

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

$$\begin{aligned}\mathscr{A} \otimes_{\mathscr{R}} \kappa_{\mathscr{R}} &\xrightarrow{\vartheta} \mathrm{Hom}_{\kappa_{\mathscr{R}}}(\mathscr{L}_3 \otimes_{\mathscr{R}} \kappa_{\mathscr{R}}, \mathscr{L}_{\sigma(1)} \otimes_{\mathscr{R}} \kappa_{\mathscr{R}}) \oplus \mathrm{Hom}_{\kappa_{\mathscr{R}}}(\mathscr{L}_3 \otimes_{\mathscr{R}} \kappa_{\mathscr{R}}, \mathscr{L}_{\sigma(2)} \otimes_{\mathscr{R}} \kappa_{\mathscr{R}})\\ &\cong \bigoplus_{i=m_2'+1}^{n} \mathrm{Hom}_{\kappa_{\mathscr{R}}}(\kappa_{\mathscr{R}}\bar{e}_i, \mathscr{L}_{\sigma(1)} \otimes_{\mathscr{R}} \kappa_{\mathscr{R}}) \oplus \bigoplus_{k=m_2'+1}^{n} \mathrm{Hom}_{\kappa_{\mathscr{R}}}(\kappa_{\mathscr{R}}\bar{e}_k, \mathscr{L}_{\sigma(2)} \otimes_{\mathscr{R}} \kappa_{\mathscr{R}})\\ &\cong \bigoplus_{i=m_2'+1}^{n} \bigoplus_{j=1}^{m_1'} \mathrm{Hom}_{\kappa_{\mathscr{R}}}(\kappa_{\mathscr{R}}\bar{e}_i, \kappa_{\mathscr{R}}\bar{e}_j) \oplus \bigoplus_{k=m_2'+1}^{n} \bigoplus_{l=m_1'+1}^{m_2'} \mathrm{Hom}_{\kappa_{\mathscr{R}}}(\kappa_{\mathscr{R}}\bar{e}_k, \kappa_{\mathscr{R}}\bar{e}_l)\end{aligned}$$

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 uvth entry and 0's elsewhere. That this is true is shown in Lemma 2.3 of [5].

The second statement follows from the same method. ■

As we are viewing these morphisms of $\mathscr{R}$-modules as matrices with entries in $F_{\mathscr{R}}$, we can compute their traces. We now rehash the work in [5] in our current setting.

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

$$\mathrm{Tr}(A^{i,i}(a)) \equiv \mathrm{Tr}(\varrho_i(a))(\mathrm{mod}\, I).$$ □

Proof. Observe that one has $\mathrm{Tr}(A^{i,i}(a)) = \mathrm{Tr}(E_i'\rho_{\widetilde{\mathscr{R}}}(a)E_i') = \mathrm{Tr}(\rho_{\widetilde{\mathscr{R}}}(a_i'aa_i')) \in \mathscr{R}$, and so the first statement holds.

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

$$\mathrm{Tr}(\varrho_1(a_i'aa_i')) + \mathrm{Tr}(\varrho_2(a_i'aa_i')) + \mathrm{Tr}(\varrho_3(a_i'aa_i')) \equiv \mathrm{Tr}(\rho_{\widetilde{\mathscr{R}}}(a_i'aa_i')) = \mathrm{Tr}(A^{i,i}(a))(\mathrm{mod}\, I).$$

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

$$\mathrm{Tr}(A^{i,i}(a)) \equiv \mathrm{Tr}(\varrho_i(a))(\mathrm{mod}\, I)$$

for $1 \leq i \leq 3$. ■

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

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

and

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

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

$$\begin{aligned}\mathrm{Tr}\left(\sum_{i=1}^{2} A^{3,i}(a)A^{i,3}(b)\right) &= \mathrm{Tr}(E_3'\rho_{\widetilde{\mathscr{R}}}(ab)E_3')\\ &= \mathrm{Tr}(\rho_{\widetilde{\mathscr{R}}}(a_3aba_3)) \in \mathscr{R}.\end{aligned}$$

This proves the first claim.

Using the previous lemma, we have that

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

Thus, $\mathrm{Tr}(A^{3,3}(ab)) \equiv \mathrm{Tr}(A^{3,3}(ba))(\mathrm{mod}\, I)$ for all $a, b \in \mathscr{A}$. We combine this with the fact that $\rho_{\widetilde{\mathscr{R}}}(ab) = \rho_{\widetilde{\mathscr{R}}}(a)\rho_{\widetilde{\mathscr{R}}}(b)$ to reach the desired congruence modulo I. ■

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

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

We use this lemma as our base case in an induction argument as used in [5] and [38]. We prove that for $i > j$, we have

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

for all $a \in \mathscr{A}$. 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 $a \in \ker(\rho \otimes_{\mathscr{R}} \kappa_{\mathscr{R}})$.

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

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

for $i > j$. □

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

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

Thus, by Lemma 6.5, we have

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

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

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

for some $\alpha_s \in \mathscr{R}$. Lemma 6.3 guarantees that for each $m'_{i_0-1} + 1 \leq s \leq m'_{i_0}$, there exists a $t_s \in \mathscr{A}$ 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 $\alpha_{i_0} = \mathrm{Tr}(A^{i_0,j_0}(a)A^{j_0,i_0}(t_s)) \in \mathfrak{m}_{\mathscr{R}}^{k+1} + I$ for each $m'_{i_0-1} + 1 \leq s \leq m'_{i_0}$, which gives the first result. ■

Lemma 6.8. Under our induction hypothesis, we have

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

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

Proof. Consider $\mathrm{Im}\,\rho \otimes \kappa_{\mathscr{R}} \subset \mathrm{Hom}(\mathscr{L} \otimes \kappa_{\mathscr{R}}, \mathscr{L} \otimes \kappa_{\mathscr{R}})$. We denote the projection of $\overline{\rho}(a)$ on to $\mathrm{Hom}(\mathscr{L}_{\sigma(t)} \otimes \kappa_{\mathscr{R}}, \mathscr{L}_{\sigma(s)} \otimes \kappa_{\mathscr{R}})$ by $\overline{A}^{s,t}$. Applying Lemma 6.6, we have a decomposition

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

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

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

with $\overline{A}^{s,t} \in (\mathrm{Im}\,\rho \otimes \kappa_{\mathscr{R}})_{s,t}$.

Lemma 6.7 gives well-defined linear maps

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

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 equation

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

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

$$\begin{aligned}
\Phi_{i,j}(\overline{D}) &= \Phi_{i,j}(\overline{D}\overline{\rho}(a'_v)) \\
&= \sum_{s=1}^{j} \Phi_{i,s}(\overline{D})\overline{\rho}(a'_v)^{s,j} + \sum_{s=j+1}^{i} \Phi_{i,s}(\overline{D})\Phi_{s,j}(\overline{\rho}(a'_v)) + \sum_{s=i+1}^{3} \overline{D}^{i,s}\Phi_{s,j}(\overline{\rho}(a'_v)) \\
&= \sum_{s=1}^{j} \Phi_{i,s}(\overline{D})\overline{\rho}(a'_v)^{s,j} && (15) \\
&= \Phi_{i,j}(\overline{D}) && (16) \\
&= 0. && (17)
\end{aligned}$$

Note that equation (15) follows from the fact that $\overline{\rho}(a'_v) = E'_v$, $j < s$, and $\Phi_{s,j}$ of a diagonal matrix is 0 for $s \ne j$. Equation (16) follows from noting $\overline{\rho}(a'_v)^{s,j} = 0$ unless $s = j = v$, in which case $\overline{\rho}(a'_v)^{v,v} = I_v$. Finally, we see that $\Phi_{i,j}(\overline{D}) = 0$ unless $(i, j) = (u, v)$, but this is impossible since $i > j$ and $u \le v$. This completes the proof and hence the induction. ■

We summarize what we have proven thus far (in terms of ρ_i's and $\mathscr{L}_i$'s) in the following proposition. The only point that needs mentioning is the statement about the action on the quotient that also requires Theorem 1 in [9].

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

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

Lemma 6.10.

1. The $\mathscr{R}$-modules

$$\mathscr{L}_1(\alpha_i) = E(\alpha_i)\mathscr{L}_1 = \ker(\rho_{\widetilde{\mathscr{R}}}(a_0) - \alpha_i \,\mathrm{Id}) \cap \mathscr{L}_1$$

are mutually isomorphic to some module $\mathscr{T}_1$ for $1 \le i \le n_1$ and similarly the $\mathscr{R}$-modules

$$\mathscr{L}_2(\alpha_i) = E(\alpha_i)\mathscr{L}_2 = \ker(\rho_{\widetilde{\mathscr{R}}}(a_0) - \alpha_i \,\mathrm{Id}) \cap \mathscr{L}_2$$

are mutually isomorphic to some module $\mathscr{T}_2$ for $n_1 + 1 \le i \le n_2$.

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

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

Fix an isomorphism $\mathscr{L}_1 \otimes \mathscr{R}/I \cong (\mathscr{T}_1/I\mathscr{T}_1)^{n_1}$. Set $\mathscr{E} = \mathrm{End}_{\mathscr{R}/I}(\mathscr{T}_1/I\mathscr{T}_1)$ (a noncommutative Artinian algebra) and $\theta : \mathscr{R}/I \to \mathscr{E}$ the canonical algebra homomorphism. The action of $\mathscr{A}$ on $\mathscr{L}_1 \otimes \mathscr{R}/I$ gives a representation ρ_1' in $\mathrm{M}_{n_1}(\mathscr{E})$ so that $\mathrm{Tr}(\rho_1'(a)) \in \theta(\mathscr{R}/I)$ is defined for all $a \in \mathscr{A}$, and we have $\mathrm{Tr}(\rho_1'(a)) = \theta(\mathrm{Tr}(\rho_1(a)))$ for all $a \in \mathscr{A}$. A generalization of Theorem 1.1.2 in [9] then gives the result. See the proof of Lemma 1.5 in [38] for the proof of this generalization. ■

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 $\mathscr{L}$ is isomorphic to $\overline{\rho}'$ with $\overline{\rho}'^{\,\mathrm{ss}} = \overline{\rho}_1 \oplus \overline{\rho}_2$. Let $\mathscr{L}'$ be the sublattice of $\mathscr{L}$ that is stable under the action of $\mathscr{A}$ so that $\mathscr{L}/\mathscr{L}' \cong \overline{\rho}'$. From our decomposition of $\mathscr{L}$, we inherit a decomposition of $\mathscr{L}'$ as $\mathscr{L}' = \mathscr{L}_1' \oplus \mathscr{L}_2' \oplus \mathscr{L}_3'$. Thus, we have

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

However, our assumption on $\overline{\rho}'^{\,\mathrm{ss}}$ gives that $\mathscr{L}_3 = \mathscr{L}_3'$. This, combined with the fact that $\mathscr{L}$ is generated by $\mathscr{L}_3$ over $\mathscr{A}$, gives $\mathscr{L} = \mathscr{L}'$, 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. ■

7 Selmer Groups

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

Let $E/\mathbb{Q}_p$ be a finite extension. Let $\mathcal{O}$ be the ring of integers of E and ϖ a uniformizer. Let V be a finite dimensional Galois representation over E. We will also find it convenient to write $\rho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{GL}_n(E)$ 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, that is, T is stable under the action of $\mathrm{G}_{\mathbb{Q}}$ and $T \otimes_{\mathcal{O}} E \cong V$. Set $W = V/T$.

We write $\mathbb{B}_{\mathrm{cris}}$ for the ring of p-adic periods [14]. Set

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

and

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

We say the representation V is *crystalline* if $\dim_{\mathbb{Q}_p} V = \dim_{\mathbb{Q}_p} \mathrm{Cris}(V)$. Let $\mathrm{Fil}^i D$ be a decreasing filtration of D. If V is crystalline, we say V is *short* if $\mathrm{Fil}^0 D = D$, $\mathrm{Fil}^p D = 0$, 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 nth power of the p-adic cyclotomic character.

The local Selmer groups are defined as follows. Set

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

where

$$\mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}_\ell, M) = \ker(\mathrm{H}^1(\mathbb{Q}_\ell, M) \to \mathrm{H}^1(I_\ell, M))$$

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

Definition 7.1. The Selmer group of W is given by

$$\mathrm{Sel}(W) = \ker\left(\mathrm{H}^1(\mathbb{Q}, W) \to \bigoplus_\ell \frac{\mathrm{H}^1(\mathbb{Q}_\ell, W)}{\mathrm{H}^1_f(\mathbb{Q}_\ell, W)}\right),$$

that is, it is the cocycles $\mathfrak{c} \in \mathrm{H}^1(\mathbb{Q}, W)$ that lie in $\mathrm{H}^1_f(\mathbb{Q}_\ell, W)$ when restricted to D_ℓ. □

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 α and β 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 γ making the following diagram commute

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\alpha_X"] \arrow[d, "\mathrm{id}_N"'] & X \arrow[r, "\beta_X"] \arrow[d, "\gamma"'] & M \arrow[r] \arrow[d, "\mathrm{id}_M"'] & 0 \\ 0 \arrow[r] & N \arrow[r, "\alpha_Y"] & Y \arrow[r, "\beta_Y"] & M \arrow[r] & 0. \end{tikzcd}$$

Let $\mathrm{Ext}^1_{R[G]}(M, N)$ denote the set of equivalence classes of $R[G]$-extensions of M by N which split as extensions of R-modules, that is, 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 [41].

Theorem 7.2. [7, Theorem 9.2] Let M and N be $R[G]$-modules. There is a one–one correspondence between the sets $\mathrm{H}^1(G, \mathrm{Hom}_R(M, N))$ and $\mathrm{Ext}^1_{R[G]}(M, N)$. $\square$

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

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\alpha"] & X \arrow[r, "\beta"'] & M \arrow[l, bend right, "s_X"'] \arrow[r] & 0 \end{tikzcd}$$

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

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

where ρ denotes the G-action on X and ρ_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

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

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 $X \in \mathrm{Ext}^1_{R[G]}(M, N)$, 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 ϖ^n. The previous theorem gives a bijection between $\mathrm{Ext}^1_{(\mathcal{O}/\varpi^n)[D_p]}(\mathcal{O}/\varpi^n, W[n])$ and $\mathrm{H}^1(D_p, W[n])$. For

$\ell \neq p$, we define the local degree n Selmer groups by $\mathrm{H}^1_f(\mathbb{Q}_\ell, W[n]) = \mathrm{H}^1_{\mathrm{ur}}(\mathbb{Q}, W[n])$. 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 Section 1.1 of [11]. 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 [11, §2.1]. For our purposes, the following two propositions are what are needed.

Proposition 7.3. [11, p. 670] If V is a short crystalline representation at p, T a D_p-stable lattice, and X a subquotient of T/ϖ^n that gives an extension of D_p-modules as above, then the class of this extension is in $\mathrm{H}^1_f(\mathbb{Q}_p, W[n])$. □

Proposition 7.4. [11, 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

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

and

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

□

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. [19, Lemma 9.4] $S(W)$ is a finitely generated $\mathcal{O}$-module. □

Lemma 7.6. [19, Lemma 9.5] If the modulo ϖ reduction $\overline{\rho}$ of ρ 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 Section 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, ϖ the uniformizer, $\mathfrak{p} = (\varpi)$ the prime ideal over p, and $\mathbb{F}$ the residue field.

Let $\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}(V_{f,\mathfrak{p}})$ be the p-adic Galois representation associated to an eigenform f, $T_{f,\mathfrak{p}}$ a $G_{\mathbb{Q}}$-stable $\mathcal{O}$-lattice, and $W_{f,\mathfrak{p}} = V_{f,\mathfrak{p}}/T_{f,\mathfrak{p}}$. We denote twists by the mth 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 the statement of theorems as they are fixed throughout the section, that is, 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. [35, 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 $\wp$ a prime of K_F over p. There exists a finite extension E of the completion of $K_{F,\wp}$ of K_F at $\wp$ and a continuous semi-simple Galois representation

$$\rho_{F,\wp} : G_{\mathbb{Q}} \to \mathrm{GL}_4(E)$$

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

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

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

Theorem 8.2. [13, 37] Let F be as in Theorem 8.1. The restriction of $\rho_{F,\wp}$ to the decomposition group D_p is crystalline at p. In addition, if $p > 2k-2$, then $\rho_{F,\wp}$ is short. $\square$

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 ϕ 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 ϕ and $\mathcal{M}^{nc} = \mathcal{M}^S - \mathcal{M}^c$. Our factorization of $\mathbb{T}^S_{\mathcal{O}}$ and $\mathbb{T}^{\mathrm{NM}}_{\mathcal{O}}$ allows us to factor the map ϕ 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 $\phi_{\mathfrak{m}} : \mathbb{T}^S_{\mathcal{O},\mathfrak{m}} \to \mathbb{T}^S_{\mathcal{O},\mathfrak{m}'}$ 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

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

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 $k > 9$ be an even 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 and F_f the Saito–Kurokawa lift of f. Let f be ordinary at p and $\overline{\rho}_{f,\mathfrak{p}}$ be irreducible. If there exists $N > 1$, a fundamental discriminant $D < 0$ so that $\chi_D(-1) = -1$, $p \nmid ND[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma_0^{(4)}(N)]$, and a Dirichlet character χ of conductor N so that

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

then

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

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. ■

The work in Section 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 [19].

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 $\rho_i : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}_E(V_i)$ for $1 \leq i \leq 3$. Assume the residual representations $\overline{\rho}_i$ are irreducible and non-isomorphic for $1 \leq i \leq 3$. Let $\mathscr{V}_1, \ldots, \mathscr{V}_m$ be n-dimensional E vector spaces affording absolutely irreducible continuous representations $\varrho_i : \mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}_E(\mathscr{V}_i)$ for $1 \leq i \leq m$. Further assume that the modulo ϖ reductions of ϱ_i satisfy

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

for some $\mathrm{G}_{\mathbb{Q}}$-stable lattice in $\mathscr{V}_i$ (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 $\{c_j(\sigma) : \sigma \in \mathrm{G}_{\mathbb{Q}}, 0 \leq j \leq n-1\}$. We can use the continuity of the ϱ_i along with the Chebotarev density theorem to conclude that

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

Observe that $\mathbb{T}$ is a finite $\mathcal{O}$-algebra. Let $I \subset \mathbb{T}$ be the ideal generated by the set $\{c_j(\mathrm{Frob}_\ell) - a_j(\mathrm{Frob}_\ell) : 0 \leq j \leq n-1, \ell \neq p\}$. The definition of I gives that the map $\mathcal{O} \to \mathbb{T}/I$ 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 $G_\mathbb{Q}$-stable $\mathbb{T}$-submodule $\mathscr{L} \subset \bigoplus_{i=1}^m \mathscr{V}_i$, $\mathbb{T}$-submodules $\mathscr{L}_1, \mathscr{L}_2$, and $\mathscr{L}_3$ contained in $\mathscr{L}$ and finitely generated $\mathbb{T}$-modules $\mathscr{T}_1$ and $\mathscr{T}_2$ such that

1. as $\mathbb{T}$-modules we have $\mathscr{L} = \mathscr{L}_1 \oplus \mathscr{L}_2 \oplus \mathscr{L}_3$ and $\mathscr{L}_i \cong \mathbb{T}^{n_i}$ for $1 \leq i \leq 3$;
2. $\mathscr{L}$ has no $\mathbb{T}[G_\mathbb{Q}]$-quotient isomorphic to $\overline{\rho}'$ where $\overline{\rho}'^{\,\mathrm{ss}} = \overline{\rho}_1 \oplus \overline{\rho}_2$;
3. $(\mathscr{L}_1 \oplus \mathscr{L}_2)/I(\mathscr{L}_1 \oplus \mathscr{L}_2)$ is $G_\mathbb{Q}$-stable and there exists a $\mathbb{T}[G_\mathbb{Q}]$-isomorphism
$$\mathscr{L}/(\mathscr{L} + I(\mathscr{L}_1 \oplus \mathscr{L}_2)) \cong M_3 \otimes_\mathcal{O} \mathbb{T}/I$$
for any $G_\mathbb{Q}$-stable $\mathcal{O}$-lattice $M_3 \subset V_3$;
4. one has either $\mathrm{Hom}_{\mathbb{T}/I}(M_1 \otimes_\mathcal{O} \mathscr{T}_1/I\mathscr{T}_1, M_2 \otimes_\mathcal{O} \mathscr{T}_2/I\mathscr{T}_2) = 0$ or $\mathrm{Hom}_{\mathbb{T}/I}(M_2 \otimes_\mathcal{O} \mathscr{T}_2/I\mathscr{T}_2, M_1 \otimes_\mathcal{O} \mathscr{T}_1/I\mathscr{T}_1) = 0$ for any $G_\mathbb{Q}$-stable $\mathcal{O}$-lattices $M_i \subset V_i$ for $i = 1, 2$;
5. $\mathrm{Fitt}_\mathbb{T}(\mathscr{T}_i) = 0$ for $i = 1, 2$ and there exists a $\mathbb{T}[G_\mathbb{Q}]$-isomorphism
$$\mathscr{L}_i/I\mathscr{L}_i \cong M_i \otimes_\mathcal{O} \mathscr{T}_i/I\mathscr{T}_i$$
for any $G_\mathbb{Q}$-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 $\mathrm{Fitt}_\mathbb{T}(\mathscr{T}_i) = 0$ follows immediately from our work in Section 6. See Lemma 9.13 of [19] for the details. ■

We now specialize to our situation.

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

Let M_i be a $G_\mathbb{Q}$-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 Section 6 when it is convenient for our purposes. We now break into two cases depending on whether $\mathrm{Hom}_{\mathbb{T}/I}(M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1, M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2) = 0$ or $\mathrm{Hom}_{\mathbb{T}/I}(M_2 \otimes_{\mathcal{O}} \mathcal{T}_2/I\mathcal{T}_2, M_1 \otimes_{\mathcal{O}} \mathcal{T}_1/I\mathcal{T}_1) = 0$.

We 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

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{N}_1 \oplus \mathcal{N}_2 \arrow[r] & \mathcal{L} \otimes \mathbb{T}/I \arrow[r] & \rho_3 \otimes \mathbb{T}/I \arrow[l, bend right, "s"'] \arrow[r] & 0, \end{tikzcd}$$

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 Section 7, this gives rise to a cocycle

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

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 $\mathfrak{c}_2$ 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

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

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 ϖ reduction of $\rho_{f,\mathfrak{p}} \otimes \varepsilon^{1-k}$ 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

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

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

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

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

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

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

$$\begin{tikzcd} & \mathrm{H}^1(\mathrm{G}_\mathbb{Q}, T\otimes_\mathcal{O} \mathscr{T}_2/I\mathscr{T}_2) \arrow[d, "\phi"] \arrow[dr, "\mathrm{H}^1(1\otimes f)"] & \\ \mathrm{H}^0(\mathrm{G}_\mathbb{Q}, T\otimes_\mathcal{O} \mathscr{I}_f) \arrow[r] & \mathrm{H}^1(\mathrm{G}_\mathbb{Q}, T\otimes_\mathcal{O} \mathscr{B}_f) \arrow[r, "\mathrm{H}^1(1\otimes f)"] & \mathrm{H}^1(\mathrm{G}_\mathbb{Q}, T\otimes_\mathcal{O} E/\mathcal{O}). \end{tikzcd}$$

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 $\mathrm{H}^0(\mathrm{G}_\mathbb{Q}, T\otimes_\mathcal{O} \mathscr{I}_f) = 0$. Thus, we must have that $\mathrm{H}^1(1\otimes f)$ 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 ϕ.

Given any $g \in \mathrm{Hom}_\mathcal{O}(\mathscr{T}_2/I\mathscr{T}_2, E/\mathcal{O})$, one has that $\ker g$ has finite index in $\mathscr{T}_2/I\mathscr{T}_2$. So in particular, we have that there exists an $\mathcal{O}$-module A with $\ker f \subseteq A \subset \mathscr{T}_2/I\mathscr{T}_2$ such that $(\mathscr{T}_2/I\mathscr{T}_2)/A \cong \mathcal{O}/\varpi \cong \mathbb{F}$. 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

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

We now consider $\mathfrak{c}_1 \in \mathrm{H}^1(\mathrm{G}_\mathbb{Q}, \mathrm{Hom}_{\mathbb{T}/I}(M_3\otimes_\mathcal{O} \mathbb{T}/I, M_1\otimes_\mathcal{O} \mathscr{T}_1/I\mathscr{T}_1))$. Let $T' = \mathrm{Hom}_\mathcal{O}(M_3, M_1)$. Choose an $\mathcal{O}$-module $B \subset \mathscr{T}_1/I\mathscr{T}_1$ so that $(\mathscr{T}_1/I\mathscr{T}_1)/B \cong \mathbb{F}$. 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 ω^{-1}. Thus, if $\mathfrak{c}_1$ is nonzero in $\mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, T' \otimes_{\mathcal{O}} \mathbb{F})$, that is, 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 nontrivial 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 ω^{-1}. Thus, we obtain a nontrivial subgroup of the ω^{-1}-isotypical piece of the p-part of the class group of $\mathbb{Q}(\mu_p)$. However, Herbrand's theorem says that this implies $p \mid \mathrm{B}_2 = 1/30$, 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 [4] pages 316–317 for the details of the argument showing $\mathfrak{c}_2$ must be zero). However, this gives that the exact sequence

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

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

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

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

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

Applying [18, page 98] to our situation, we obtain

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

This allows us to conclude that

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

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

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

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

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

as desired. ■

It now only remains to deal with the case where $\mathrm{Hom}_{\mathbb{T}/I}(M_2 \otimes_{\mathcal{O}} \mathscr{T}_2/I\mathscr{T}_2, M_1 \otimes_{\mathcal{O}} \mathscr{T}_1/I\mathscr{T}_1) = 0$. We will see that 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

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

As before, we have

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

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

$$\begin{gathered}\iota_1 : \mathrm{Hom}_{\mathcal{O}}(\mathscr{T}_1/I\mathscr{T}_1, E/\mathcal{O}) \to \mathrm{H}^1(\mathrm{G}_{\mathbb{Q}}, \mathrm{Hom}_{\mathcal{O}}(M_3, M_1) \otimes_{\mathcal{O}} E/\mathcal{O}) \\ f \mapsto (1 \otimes f)(\mathfrak{c}_1).\end{gathered}$$

Our assumption that $\mathrm{Hom}_{\mathbb{T}/I}(M_2 \otimes_{\mathcal{O}} \mathscr{T}_2/I\mathscr{T}_2, M_1 \otimes_{\mathcal{O}} \mathscr{T}_1/I\mathscr{T}_1) = 0$ gives 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 ι_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.

Acknowledgement

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

References

[1] Andrianov, A. “Modular descent and the Saito–Kurokawa conjecture.” *Inventiones Mathematicae* 53 (1980): 267–80.

[2] Andrianov, A. *Modular Forms and Hecke Operators*. Translations of Mathematical Monographs 145. Providence, RI: American Mathematical Society, 1995.

[3] Böcherer, S. “Über die funktionalgleichung automorpher L-funktionen zur Siegelscher modulgruppe.” *Journal für die Reine und Angewandte Mathematik* 362 (1985): 146–68.

[4] Brown, J. “Saito–Kurokawa lifts and applications to the Bloch–Kato conjecture.” *Compositio Mathematica* 143, no. 2 (2007): 290–322.

[5] Brown, J. “Residually reducible representations of algebras over local Artinian rings.” *Proceedings of the American Mathematical Society* 136, no. 10 (2008): 3409–14.

[6] Brown, J. “On the cuspidality of pullbacks of Siegel Eisenstein series to $\mathrm{Sp}(2m) \times \mathrm{Sp}(2n)$.” (2010): preprint available at http://www.math.clemson.edu/~jimlb/ResearchPapers/Eisenstein2010.pdf.

[7] Brown, J. “Special values of L-functions on $\mathrm{GSp}(4) \times \mathrm{GL}(2)$ and the non-vanishing of Selmer groups.” *International Journal of Number Theory* (forthcoming).

[8] Bruinier, J. “Nonvanishing modulo ℓ of Fourier coefficients of half-integral weight modular forms.” *Duke Mathematical Journal* 98, no. 3 (1999): 595–611.

[9] Carayol, H. “Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet.” *Contemporary Mathematics* 165 (1994): 213–35.

[10] Chai, C., and G. Faltings. “Degeneration of Abelian Varieties.” Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge Band 22, A Series of Modern Surveys in Mathematics. Berlin: Springer, 1980.

[11] Diamond, F., M. Flach, and L. Guo. “The Tamagawa number conjecture of adjoint motives of modular forms.” *Annales Scientifiques de l’École Normale Supérieure* 37, no. 4 (2004): 663–727.

[12] Eichler, M., and D. Zagier. “The Theory of Jacobi Forms.” Progress in Mathematics 55. Boston: Birkhäuser, 1985.

[13] Faltings, G. “Crystalline cohomology and p-Adic Galois representations.” In *Algebraic Analysis, Geometry and Number Theory, Proceedings of JAMI Inaugural Conference*. Baltimore, MD: John Hopkins University Press, 1989.

[14] Fontaine, J. M. “Sur certains types de représentations p-adiques du groupe de Galois d’un corps local; construction d’un anneau de Barsotti–Tate.” *Annals of Mathematics* 115 (1982): 529–77.

[15] Garrett, P. “Pullbacks of Eisenstein Series: Applications.” Progress in Mathematics vol. 46. Boston: Birkhäuser, 1984.

[16] Garrett, P. “Petersson inner products and Fourier coefficients.” *Inventiones Mathematicae* 107, no. 3 (1992): 453–81.

[17] van der Geer, G. “Siegel Modular Forms.” In *The 1-2-3 of Modular Forms*. Universitext. Berlin: Springer, 2008.

[18] Hida, H. "Modular Forms and Galois Cohomology." Cambridge Studies in Advanced Mathematics vol. 69. Cambridge: Cambridge University Press, 2000.

[19] Klosin, K. "Congruences among modular forms on $U(2,2)$ and the Bloch–Kato conjecture." *Annales de l'Institut Fourier* 59, no. 1 (2009): 81–166.

[20] Kohnen, W., and N. P. Skoruppa. "A certain Dirichlet series attached to Siegel modular forms of degree two." *Inventiones Mathematicae* 95 (1989): 541–58.

[21] Kohnen, W., and D. Zagier. "Values of L-Series of modular forms at the center of the critical strip." *Inventiones Mathematicae* 64 (1981): 175–98.

[22] Langlands, R. "On the functional equations satisfied by Eisenstein series." Lecture Notes in Mathematics vol. 544. Berlin: Springer, 1976.

[23] Matsumura, H. "Commutative Ring Theory." Cambridge Advanced Studies in Mathematics vol. 8. Cambridge: Cambridge University Press, 1994.

[24] Ono, K., and C. Skinner. "Fourier coefficients of half-integral weight modular forms modulo ℓ." *Annals of Mathematics* 147 (1998): 453–70.

[25] Piatetski-Shapiro, I., and S. Rallis. "L-functions of automorphic forms on simple classical groups." In *Modular Forms (Durham, 1983)*, 251–61. Ellis Horwood Series in Mathematics and Its Applications: Statistics, Operational Research. Chichester: Horwood, 1984.

[26] Ribet, K. "A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$." *Inventiones Mathematicae* 34 (1976): 151–62.

[27] Shimura, G. "The special values of the zeta functions associated to cusp forms." *Communications on Pure and Applied Mathematics* 29 (1976): 783–804.

[28] Shimura, G. "On the periods of modular forms." *Mathematische Annalen* 229 (1977): 211–21.

[29] Shimura, G. "Algebraic relations between critical values of zeta functions and inner products." *American Journal of Mathematics* 104 (1983): 253–85.

[30] Shimura, G. "Nearly holomorphic functions on Hermitian symmetric space." *Annales de Mathématiques* 278 (1987): 1–28.

[31] Shimura, G. "Eisenstein series and zeta functions on symplectic groups." *Inventiones Mathematicae* 119 (1995): 539–84.

[32] Shimura, G. "Euler products and Eisenstein series." CBMS Regional Conference Series in Mathematics vol. 93. Providence, RI: American Mathematical Society, 1997.

[33] Siegel, C. L. "Einführung in die theorie der modulfunktionen n-ten grades." *Mathematische Annalen* 116 (1939): 617–57.

[34] Skinner, C., and E. Urban. "The Iwasawa main conjecture for GL(2)."

[35] Skinner, C., and E. Urban. "Sur les déformations p-adiques de certaines représentations automorphes." *Journal of the Institute of Mathematics of Jussieu* 5 (2006): 629–98.

[36] Urban, E. "On residually reducible representations on local rings." *Journal of Algebra* 212 (1999): 738–42.

[37] Urban, E. *Sur les représentations p-adiques associées aux représentations cuspidales de $GSp_{4/\mathbb{Q}}$*, à paraître aux actes du congrès "Formes Automorphes" du centre Emile Borel, Institute Henri Poincaré, 2000.

[38] Urban, E. “Selmer groups and the Eisenstein–Klingen ideal.” *Duke Mathematical Journal* 106, no. 3 (2001): 485–525.

[39] Vatsal, V. “Canonical periods and congruence formulae.” *Duke Mathematical Journal* 98, no. 2 (1999): 397–419.

[40] Waldspurger, J.-L. “Sur les coefficients de Fourier des formes modulaires de poids demi-entier.” *Journal de Mathématiques Pures et Appliquées* 60 (1981): 375–484.

[41] Washington, L. “Galois Cohomology.” In *Modular Forms and Fermat’s Last Theorem (Boston, MA, 1995)*, 101–20. New York: Springer, 1997.

[42] Wiles, A. “The Iwasawa conjecture for totally real fields.” *Annals of Mathematics* 131, no. 3 (1990): 493–540.

[43] Zagier, D. “Sur la conjecture de Saito–Kurokawa.” In *Sé Delange-Pisot-Poitou 1979/80*, 371–94. Progress in Mathematics 12. Basel: Birkhäuser, 1980.