Springer Proceedings in Mathematics & Statistics

Matteo Longo
Marco Adamo Seveso
Rodolfo Venerucci
Stefano Vigni *Editors*

Elliptic Curves and Modular Forms in Arithmetic Geometry

Celebrating Massimo Bertolini's 60th Birthday, Milano, Italy, September 12–16, 2022

Springer

Springer Proceedings in Mathematics & Statistics

Volume 527

Matteo Longo · Marco Adamo Seveso ·
Rodolfo Venerucci · Stefano Vigni
Editors

Elliptic Curves and Modular Forms in Arithmetic Geometry

Celebrating Massimo Bertolini's 60th Birthday, Milano, Italy, September 12–16, 2022

Springer

Contents

Flach Classes and Generalised Hecke Eigenvalues

Henri Darmon and Alice Pozzi

To Massimo Bertolini on his 60th birthday

Abstract We describe the action of Hecke operators on generalised eigenspaces attached to certain mod p cuspidal eigenforms of weight two in terms of certain extension classes of Galois representations constructed by Matthias Flach. This description can be viewed as a partial generalisation to cusp forms of a formula of Barry Mazur for the Eisenstein series of weight two and prime level.

Keywords Modular forms · Elliptic curves · Flach elements · Selmer groups · Galois representations

1 Introduction

Given an integer $N \geq 1$, let $M_2(N)$ denote the space of modular forms of weight two on $\Gamma_0(N)$ with integer Fourier coefficients, and let $\mathbb{T}(N)$ be the Hecke algebra generated over $\mathbb{Z}$ by the prime-to-N Hecke operators in the endomorphism ring of $M_2(N)$.

When N is prime, the space $M_2(N)$ contains a unique holomorphic Eisenstein series $E_{2,N}$, with q-expansion given by

$$E_{2,N}(q) = \tfrac{N-1}{12} + \sum_{n=1}^{\infty} \sigma_{1,N}(n) q^n, \qquad \sigma_{1,N}(n) = \sum_{\substack{d|n, \\ (d,N)=1}} d. \tag{1}$$

H. Darmon (✉)
McGill University, Montreal, Canada
e-mail: darmon@math.mcgill.ca

A. Pozzi
University of Bristol, Bristol, UK
e-mail: alice.pozzi@bristol.ac.uk

M. Longo et al. (eds.), *Elliptic Curves and Modular Forms in Arithmetic Geometry*,
Springer Proceedings in Mathematics & Statistics 527,
https://doi.org/10.1007/978-3-032-13123-2_3

In his celebrated work on the Eisenstein ideal [13], Mazur determines the possible structure of the torsion subgroup of an elliptic curve over $\mathbb{Q}$ by studying congruences between the systems of Hecke eigenvalues of $E_{2,N}$ and cusp forms modulo a prime p (which we assume for simplicity to be strictly greater than 3). Mazur shows that such congruences occur precisely when p divides $(N-1)$. At such primes, let $\mathbb{T}(N)_{p,\mathrm{eis}}$ be the localisation of $\mathbb{T}(N)\otimes\mathbb{Z}_p$ at the maximal ideal generated by $(T_\ell-(\ell+1))$ for primes $\ell\nmid Np$. The kernel of the morphism

$$\varphi_{\mathrm{eis}}\colon \mathbb{T}(N)_{p,\mathrm{eis}}\longrightarrow\mathbb{Z}_p$$

sending T_ℓ to $(\ell+1)$ for primes $\ell\nmid N$ is the *Eisenstein ideal*, denoted by $I_{\mathrm{eis},(N)}$. An important result towards arithmetic applications is the principality of this ideal, which is deduced from the construction of a canonical isomorphism

$$\lambda_{\mathrm{eis}}\colon I_{\mathrm{eis},(N)}/I^2_{\mathrm{eis},(N)}\xrightarrow{\sim}(\mathbb{Z}/N\mathbb{Z})^\times\otimes\mathbb{Z}_p \tag{2}$$

satisfying

$$\lambda_{\mathrm{eis}}(T_\ell-(\ell+1))=[\ell]\otimes(\ell-1),\ \text{ for all primes } \ell\nmid Np. \tag{3}$$

In other words, after fixing an $m\geq 1$ for which p^m divides $N-1$, and a mod p^m discrete logarithm

$$\log_{N,p}:(\mathbb{Z}/N\mathbb{Z})^\times\longrightarrow\mathbb{Z}/p^m\mathbb{Z},$$

the mod p^m reduction of φ_{eis} lifts to a surjective homomorphism

$$\tilde{\varphi}_{\mathrm{eis}}:\mathbb{T}(N)\longrightarrow\left(\mathbb{Z}/p^m\mathbb{Z}\right)[\varepsilon]/(\varepsilon^2)$$

satisfying

$$\tilde{\varphi}_{\mathrm{eis}}(T_\ell)=a_\ell+a'_\ell\cdot\varepsilon,\qquad\text{with}\quad\begin{cases}a_\ell=(\ell+1)\\ a'_\ell=(\ell-1)\log_{N,p}(\ell),\end{cases}\qquad\text{for all primes } \ell\neq N. \tag{4}$$

The collection $\{a'_\ell\}_\ell$ of *generalised Hecke eigenvalues* is independent of the choice of discrete logarithm up to simultaneous rescaling. This intriguing arithmetic invariant arises precisely when the action of the Hecke operators on the generalised eigenspace attached to $E_{2,N}$ mod p is non-semisimple. (Cf. Remark 12.2.) The formulation (4) suggests that the generalised eigenvalues a'_ℓ are governed by the images of global elements in $(\mathbb{Z}/N\mathbb{Z})^\times$, their dependence on the primes N and $p\mid(N-1)$ arising only through the choice of a discrete mod p^m logarithm on $(\mathbb{Z}/N\mathbb{Z})^\times$.

The study of generalised eigenvalues was taken up subsequently from the analytic perspective of Eisenstein series and L-functions by Merel [14] and then by Lecouturier [12], where it constitutes the starting point for his theory of *higher Eisenstein elements*. It was further explored from a more Galois deformation theoretic per-

spective in [3] and [18] Among several applications, the notion of higher Eisenstein element plays an important role in formulating a conjecture of Harris and Venkatesh [11] on derived Hecke operators acting on the coherent cohomology of modular curves attached to spaces of weight one forms, and in the proof of this conjecture for dihedral forms [5].

It is natural to seek analogous formulae for the quantities a'_ℓ when the underlying eigenform is not an Eisenstein series. That such generalised eigenvalues might encode rich arithmetic information is suggested by a number of results already in the literature. For instance, when $E_{2,N}$ is replaced by a classical eigenform of weight one, and Φ_p by $\bar{\mathbb{Q}}_p$, the generalised eigenvalues can be expressed in terms of p-adic logarithms of algebraic numbers in the field cut out by the adjoint of the associated two-dimensional Artin representation [6, 7], a circumstance that provides a key to a better understanding of explicit class field theory for real quadratic fields [8, 9].

The present work considers the setting where the weight two Eisenstein series is replaced by a *cuspidal* newform f of weight two on $\Gamma_0(M)$. It is convenient (but entirely inessential, of course) to assume that f has integer Fourier coefficients, i.e., that it corresponds to an elliptic curve E over $\mathbb{Q}$ by the construction of Eichler and Shimura.

Given a prime p, the circumstances under which f is congruent to a modular form of level M occur somewhat sporadically: one needs to assume, essentially, that p divides the degree of the optimal modular parametrisation $\phi_E : X_0(M) \longrightarrow E$. The present work has nothing interesting to say about the generalised eigenvalues that arise from such homomorphisms. Rather, a prime $p \nmid 6M$ is fixed at the outset for which the Galois action on the p-division points $E[p] \subset E$ has full image $\mathrm{Aut}(E[p])$, and which does *not* divide the degree of ϕ_E. It is also assumed that the conductor of E is minimal among those of its quadratic twists. As recalled in Sect. 9, it then follows that the generalised eigenspace attached to f in $M_2(M) \otimes \Phi_p$ is spanned by f.

The mechanism whereby generalised Hecke eigenvalues can nonetheless be conjured from this setting involves level-raising. Namely, choose a prime $N \nmid Mp$ for which

$$p \text{ divides } (N-1)\cdot(N+1-a_N(f))\cdot(N+1+a_N(f)), \tag{5}$$

and replace $\mathbb{T}(M)$ by the larger Hecke algebra $\mathbb{T}(MN^2)$ of level MN^2, which is endowed with a natural surjective map $\mathbb{T}(MN^2) \longrightarrow \mathbb{T}(M)$. Let $\mathbb{T}(MN^2)_{p,f}$ denote the localisation of $\mathbb{T}(MN^2) \otimes \mathbb{Z}_p$ at the maximal ideals attached to $f \pmod p$. The morphism

$$\varphi_{f,(N)} : \mathbb{T}(MN^2)_{p,f} \longrightarrow \mathbb{Z}_p$$

sends a Hecke operator T_ℓ to the coefficient $a_\ell(f)$ for $\ell \nmid MNp$. Its kernel, denoted by $I_{f,(N)}$, can be viewed as the analogue of the Eisenstein ideal in the elliptic setting.

The desired extension of Mazur's formula to cusp forms can be better explained by reinterpreting the latter in the language of Galois cohomology (see Sect. 4). Let T_pE be the Tate module of the elliptic curve E, and let

$$T_f := \mathrm{Sym}^2(T_p E)$$

denote its symmetric square, viewed as a $G_{\mathbb{Q}}$-module. A fundamental construction of M. Flach [10] associates to each rational prime $\ell \nmid pMN$ a global class

$$c_f[\ell] \in H^1(\mathbb{Q}, T_f)$$

which is "singular only at ℓ", i.e., is crystalline at p and minimally ramified at all primes different from ℓ and p. In particular, its restriction $\mathrm{res}_N(c_f[\ell])$ to the decomposition group at N belongs to the finite part $H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f)$ of the local cohomology at N. (Cf. Sect. 2.) The class $c_f[\ell]$ is the p-adic étale regulator of a global element in a higher Chow group of $X_0(M)^2$, as described in Sect. 10 below. It plays the same role as the class $[\ell^{(\ell-1)}]$ in Mazur's identity (3), as the following theorem illustrates.

Theorem 1.1 *There is a unique isomorphism*

$$\lambda_f : I_{f,(N)}/I_{f,(N)}^2 \longrightarrow H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f)$$

characterised by

$$\lambda_f(T_\ell - a_\ell) = \mathrm{res}_N(c_f[\ell]), \textit{for all primes } \ell \nmid MNp.$$

Let us assume for simplicity that $p \nmid (N \pm 1)$. As explained in Sect. 5, the assumption that N is a level-raising prime for f implies that the local cohomology group $H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f)$ is cyclic of order p^m for some $m > 0$. In Sect. 6, an identification of $H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f)$ with $\mathbb{Z}/p^m\mathbb{Z}$ is given, depending quadratically on the choice of a mod p^m discrete elliptic logarithm on $E(\Phi_{N^2})$, which is therefore denoted

$$\log^{\otimes 2}_{E,N,p} : H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f) \xrightarrow{\sim} \mathbb{Z}/p^m\mathbb{Z}.$$

Under these assumptions, there is a surjective homomorphism

$$\tilde{\varphi}_f : \mathbb{T}(MN^2) \longrightarrow \left(\mathbb{Z}/p^m\mathbb{Z}\right)[\varepsilon]/(\varepsilon^2) \tag{6}$$

lifting the mod p^m-reduction of φ_f, and for which

$$\tilde{\varphi}_f(T_\ell) = a_\ell(f) + a'_\ell(f) \cdot \varepsilon.$$

Corollary 1.2 *After possibly rescaling the collection $\{a'_\ell(f)\}_\ell$ by a common factor, the generalised eigenvalues satisfy*

$$a'_\ell(f) = \log^{\otimes 2}_{E,N,p}(\mathrm{res}_N(c_f[\ell])), \quad \textit{for all } \ell \nmid MNp.$$

Corollary 1.2 reveals that $a'_\ell(f)$ is accounted for by a global class in a higher Chow group which depends neither on N nor on p, suggesting that the generalised

eigenvalues attached to f have a motivic incarnation. In the opposite direction, the relation between Flach's classes and generalised Hecke eigenvalues gives some insights into the local behaviours of the global classes $c_f[\ell]$ as the prime ℓ varies but N and p are fixed.

2 Selmer Groups

Let V be a finite dimensional $\mathbb{Q}_p$-vector space with a continuous action of $G_{\mathbb{Q}}$ (unramified outside a finite set of places of $\mathbb{Q}$). Fix a $G_{\mathbb{Q}}$-stable $\mathbb{Z}_p$-lattice T, and write

$$A = V/T = T \otimes \mathbb{Q}_p/\mathbb{Z}_p \text{ and } A_n = p^{-n}T/T \hookrightarrow A$$

for $n \in \mathbb{Z}_{>0}$. For $W \in \{V, T, A, A_n\}$, let $H^1(\mathbb{Q}, W)$ denote the continuous Galois cohomology with coefficients in W. It is equipped, for each rational prime q, with a localisation map

$$\mathrm{res}_q : H^1(\mathbb{Q}, W) \longrightarrow H^1(\mathbb{Q}_q, W)$$

obtained by restricting a one-cocycle to a decomposition group $G_q = \mathrm{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$ at q.

Let I_q denote the inertia subgroup of G_q. The quotient G_q/I_q is topologically procyclic with a canonical generator: the *arithmetic Frobenius element* at q, denoted σ_q, which acts as $x \mapsto x^q$ on the residue field of any unramified extension of $\mathbb{Q}_q$. For W as above, the inflation-restriction exact sequence identifies the subgroup of $H^1(\mathbb{Q}_q, W)$ of unramified cohomology classes

$$H^1_{\mathrm{ur}}(\mathbb{Q}_q, W) = \ker\left(H^1(\mathbb{Q}_q, W) \to H^1(I_q, W)\right)$$

with

$$H^1(\mathbb{Q}_q^{\mathrm{ur}}/\mathbb{Q}_q, W^{I_q}) = W^{I_q}/(\sigma_q - 1)W^{I_q} \tag{7}$$

where $\mathbb{Q}_q^{\mathrm{ur}}$ is the maximal unramified extension of $\mathbb{Q}_q$ and the superscript I_q denotes inertia invariants.

The local cohomology group $H^1(\mathbb{Q}_q, W)$ contains a distinguished subgroup $H^1_{\mathrm{fin}}(\mathbb{Q}_q, W)$. When $W = V$ is a $\mathbb{Q}_p$-vector space, this is defined as

$$H^1_{\mathrm{fin}}(\mathbb{Q}_q, V) := \begin{cases} H^1_{\mathrm{ur}}(\mathbb{Q}_q, V) & \text{if } q \neq p, \\ H^1_{\mathrm{cris}}(\mathbb{Q}_p, V) & \text{if } q = p, \end{cases}$$

where $H^1_{\mathrm{cris}}(\mathbb{Q}_p, V) = \ker\left(H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, V \otimes B_{\mathrm{cris}})\right)$ and B_{cris} is the period ring defined by Fontaine [2]. (The assumption that $p \neq 2$ obviates the need to treat the case $q = \infty$.) When $W = T$ (resp. $W = A$), the subgroup $H^1_{\mathrm{fin}}(\mathbb{Q}, W)$ is defined as the natural preimage (resp. the image) of $H^1_{\mathrm{fin}}(\mathbb{Q}, V)$ in $H^1(\mathbb{Q}, W)$. Similarly,

for $n \in \mathbb{Z}_{>0}$, the subgroup $H^1_{\mathrm{fin}}(\mathbb{Q}, A_n)$ is the preimage of $H^1_{\mathrm{fin}}(\mathbb{Q}, A)$ in $H^1(\mathbb{Q}, A_n)$. Note that if T is unramified at $q \neq p$, the subgroups $H^1_{\mathrm{fin}}(\mathbb{Q}_q, W)$ and $H^1_{\mathrm{ur}}(\mathbb{Q}_q, W))$ agree for all choices of W as above (see [15, Lemma 3.5, 3.8]).

Let

$$H^1_{\mathrm{sing}}(\mathbb{Q}_q, W) := \frac{H^1(\mathbb{Q}_q, W)}{H^1_{\mathrm{fin}}(\mathbb{Q}_q, W)},$$

denote the *singular quotient* of the local cohomology at q and write ∂_q for the natural map obtained by composing res_q with the projection to this quotient.

When $q \neq p$ and W is unramified at q, the map ∂_q corresponds to the restriction to I_q. Because the maximal pro p-quotient of I_q is isomorphic to $\mathbb{Z}_p(1)$ as a G_q-module, the image of ∂_q is identified with

$$H^1(I_q, W)^{G_q} = H^1(\mathbb{Z}_p(1), W)^{G_q} = W(-1)^{G_q},$$

and it will be convenient to view ∂_q as a map

$$\partial_q : H^1(\mathbb{Q}, W) \longrightarrow W(-1)^{G_q}.$$

Given a global class $c \in H^1(\mathbb{Q}_q, W)$, its restriction $\mathrm{res}_q(c)$ belongs to $H^1_{\mathrm{fin}}(\mathbb{Q}_q, W)$ for all but finitely many q. A *set of local conditions* for $H^1(\mathbb{Q}, W)$ is a collection $\Sigma = \{\Sigma_q\}_q$ indexed by the places of $\mathbb{Q}$, and satisfying

$$\Sigma_q = H^1_{\mathrm{fin}}(\mathbb{Q}_q, W), \quad \text{for all but finitely many } q.$$

The *Selmer group* attached to W and Σ is defined to be

$$H^1_\Sigma(\mathbb{Q}, W) = \{\kappa \in H^1(\mathbb{Q}, W) \text{ for which } \mathrm{res}_q(\kappa) \in \Sigma_q, \text{ for all } q\}.$$

When $\Sigma_q = H^1_{\mathrm{fin}}(\mathbb{Q}_q, W)$ for all q, then $H^1_\Sigma(\mathbb{Q}, W)$ is just called the *Selmer group* attached to W, and is denoted $H^1_\emptyset(\mathbb{Q}, W)$. More generally, the *relaxed Selmer group* at $S \in \mathbb{Z}_{>0}$, denoted $H^1_{(S)}(\mathbb{Q}, W)$, is obtained by setting

$$\Sigma_q = \begin{cases} H^1(\mathbb{Q}_q, W) & \text{if } q | S, \\ H^1_{\mathrm{fin}}(\mathbb{Q}_q, W) & \text{if } q \nmid S, \end{cases}$$

i.e.,

$$H^1_{(S)}(\mathbb{Q}, W) = \left\{c \in H^1(\mathbb{Q}, W) \text{ such that } \partial_q(c) = 0, \text{ for all } q \nmid S\right\}. \tag{8}$$

For any set of local conditions Σ, the Selmer groups $H^1_\Sigma(\mathbb{Q}, A_n)$ is finite, and $H^1_\Sigma(\mathbb{Q}, T)$ and is a finitely generated $\mathbb{Z}_p$-module. The Pontryagin dual of $H^1_\Sigma(\mathbb{Q}, A_n)$ is also a finitely generated $\mathbb{Z}_p$-module (cf. [15, Lemma 5.7]).

3 Local and Global Duality

Given V a finite dimensional $\mathbb{Q}_p$-vector space with a continuous $G_{\mathbb{Q}}$-action and a $G_{\mathbb{Q}}$-stable $\mathbb{Z}_p$-lattice $T \subset V$, let $T^* = \mathrm{Hom}(T, \mathbb{Z}_p(1))$ be the dual of T. Denote

$$V^* = T^* \otimes \mathbb{Q}_p, \quad A^* = V^*/T^*, \text{ and } A_n^* = p^{-n}T^*/T^*$$

for $n \in \mathbb{Z}_{>0}$.

Let q be a rational prime. The cup product combined with the tautological pairings

$$\langle\ ,\ \rangle : A_n \times A_n^* \longrightarrow \mu_{p^n} \quad \text{and} \quad \langle\ ,\ \rangle : T \times A^* \longrightarrow \mu_{p^\infty}$$

give rise to the perfect local Tate pairings

$$\begin{aligned} \langle\ ,\ \rangle_q &: H^1(\mathbb{Q}_q, A_n) \times H^1(\mathbb{Q}_q, A_n^*) \longrightarrow H^2(\mathbb{Q}_q, \mu_{p^n}) \xrightarrow{\mathrm{inv}_q} \tfrac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p, \\ \langle\ ,\ \rangle_q &: H^1(\mathbb{Q}_q, T) \times H^1(\mathbb{Q}_q, A^*) \longrightarrow H^2(\mathbb{Q}_q, \mu_{p^\infty}) \xrightarrow{\mathrm{inv}_q} \mathbb{Q}_p/\mathbb{Z}_p, \end{aligned} \tag{9}$$

relative to which the respective finite parts are orthogonal complements of each other when $q \neq p$. Thus, for $W \in \{T, A, A_n\}$, the Tate pairing induces a perfect duality

$$[\ ,\ ]_q : H^1_{\mathrm{sing}}(\mathbb{Q}_q, W) \times H^1_{\mathrm{fin}}(\mathbb{Q}_q, \mathrm{Hom}(W, \mu_{p^\infty})) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p. \tag{10}$$

In the special case where $q \neq p$ and W is unramified at q, the local Tate pairing is given by the following explicit formula:

$$\langle c, \kappa\rangle_q = \langle \partial_q(c), \kappa(\sigma_q)\rangle, \qquad \text{for all } c \in H^1(\mathbb{Q}_q, W), \quad \kappa \in H^1_{\mathrm{fin}}(\mathbb{Q}_q, \mathrm{Hom}(W, \mu_{p^\infty})), \tag{11}$$

where the pairing $\langle\ ,\ \rangle$ on the right hand side is induced from the tautological $\mathbb{Q}_p/\mathbb{Z}_p$-valued pairing between $W(-1)$ and $\mathrm{Hom}(W, \mu_{p^\infty})$, after restricting to the Frobenius invariants and co-invariants respectively.

The reciprocity law of global class field asserts that

$$\sum_q \mathrm{inv}_q(b) = 0, \qquad \text{for all } b \in H^2(\mathbb{Q}, \mu_{p^\infty}),$$

and implies that

$$\sum_q \langle \mathrm{res}_q(c), \mathrm{res}_q(\kappa)\rangle_q = 0, \quad \text{for all } c \in H^1(\mathbb{Q}, W),\ \kappa \in H^1(\mathbb{Q}, \mathrm{Hom}(W, \mu_{p^\infty})), \tag{12}$$

where the sum need only be taken over the non-archimedean places in light of the running assumption that $p \neq 2$.

For $W \in \{T, A, A_n\}$, let $\Sigma = \{\Sigma_q\}_q$ be a set of local conditions for $H^1(\mathbb{Q}, W)$. The orthogonal complements

$$\Sigma_q^* \subset H^1(\mathbb{Q}_q, \mathrm{Hom}(W, \mu_{p^\infty}))$$

of Σ_q relative to the local Tate pairings (9) form a collection of local conditions. The Selmer group $H^1_{\Sigma^*}(\mathbb{Q}, \mathrm{Hom}(W, \mu_{p^\infty}))$ is called the *dual Selmer group* of $H^1_\Sigma(\mathbb{Q}, W)$. For instance, the dual of the relaxed Selmer group $H^1_{(S)}(\mathbb{Q}, W)$ is the *restricted Selmer group* at S,

$$H^1_{[S]}(\mathbb{Q}, \mathrm{Hom}(W, \mu_{p^\infty})) := \{c \in H^1_\emptyset(\mathbb{Q}, W^*) \text{ such that } \mathrm{res}_q(c) = 0, \quad \text{for all } q|S\}. \tag{13}$$

For $W = A_n$, while the size of a single Selmer group often represents a subtle global invariant, the ratio of the cardinalities of a Selmer group and its dual is accounted for by a simple explicit product of local quantities:

$$\frac{\#H^1_\Sigma(\mathbb{Q}, A_n)}{\#H^1_{\Sigma^*}(\mathbb{Q}, A_n^*)} = \frac{\#H^0(\mathbb{Q}, A_n)}{\#H^0(\mathbb{Q}, A_n^*)} \prod_q \frac{\#\Sigma_q}{\#H^0(G_q, A_n)}. \tag{14}$$

The proof of this identity rests on the Poitou–Tate long exact sequence in Galois cohomology (cf. [4, Theorem 2.19]). Notice that the ostensibly infinite product on the right is really a finite one since $\#H^1_{\mathrm{fin}}(\mathbb{Q}_q, A_n) = \#H^0(G_q, A_n)$ for all $q \neq p$.

4 Cohomological Reinterpretation of Mazur's Formula

This section recasts Mazur's formula (4) in cohomological terms. This formulation is amenable to generalisation to the elliptic setting. Recall that the Hecke eigenvalues of the Eisenstein series $E_{2,N}$ are encoded by the traces of the image of σ_ℓ of the $G_\mathbb{Q}$-representation

$$\varrho_{\mathrm{eis}} := \mathbb{Z}_p \oplus \mathbb{Z}_p(1)$$

for primes $\ell \nmid Np$.

Denote $T_\mu := \mathbb{Z}_p(1)$ and $A_\mu^* := \mathbb{Q}_p/\mathbb{Z}_p$. For each rational prime $\ell \neq p$, there is a distinguished global class

$$c_\mu[\ell] \in \mathbb{Q}^\times \otimes \mathbb{Z}_p \simeq H^1(\mathbb{Q}, T_\mu)$$

which is unramified at all primes $q \nmid p\ell$, is crystalline at p, and is ramified at ℓ. This class is simply the image of ℓ under the identification provided by classical Kummer theory. The class $c_\mu[\ell]$ is a canonical choice of generator for the Selmer group $H^1_{(\ell)}(\mathbb{Q}, T_\mu) \simeq \mathbb{Z}_p$.

Let $N \nmid p\ell$ be a prime. The Kronecker-Weber Theorem provides an isomorphism

$$H^1_{(N)}(\mathbb{Q}, A^*_\mu) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \otimes \mathbb{Z}_p,$$

so that the choice of a generator κ amounts to giving a discrete logarithm $\log_{N,p}$ modulo p^m for $p^m \parallel (N-1)$. Mazur's formula can thus be rewritten in terms of local Tate duality (at least, up to sign) as

$$a'_\ell = (\ell - 1) \cdot \log_{N,p}(\mathrm{res}_N(c_\mu[\ell])) = (\ell - 1) \cdot \langle \kappa, c_\mu[\ell] \rangle_N.$$

Remark 4.1 Formulae for generalised eigenvalues in the Eisenstein setting can be obtained through the study of the deformation theory of the mod p-reduction of ϱ_{eis} (or more precisely, of the corresponding pseudo-representation), as carried out by Wake and Wang-Erickson [18]. The deceptively simple expression for generalised eigenvalues in the prime-level setting follows from the fact the first-order deformations of the residual representation that are unramified away from $\{p, N\}$, crystalline at p and Steinberg at N are reducible (cf. *op.cit.* §9.1). When studying generalised eigenvalues arising from congruences between the Eisenstein $E_{2,N}$ series and cusp forms of a more general level, one should expect formulae involving Massey products (cf. *op.cit.* Part 3).

5 The Symmetric Square and Adjoint Representations

We place ourselves in the setting of the introduction, namely, assume that f is a weight two cusp form attached to an elliptic curve E over $\mathbb{Q}$ of conductor M, and let

$$\varrho_f : G_\mathbb{Q} \longrightarrow \mathrm{Aut}(T_p E)$$

be the representation arising from the Galois action on the p-adic Tate module of E. For every prime $N \nmid Mp$, the characteristic polynomial of σ_N is given by

$$x^2 - a_N(f)x + N = (x - \alpha_N)(X - \beta_N) \tag{15}$$

for some α_N and $\beta_N \in \overline{\mathbb{Z}}$ which have complex absolute value $\sqrt{N}$ and hence are different from ± 1 and $\pm N$.

It is assumed that the mod p reduction of $\overline{\varrho}_f : G_\mathbb{Q} \to \mathrm{Aut}(E[p])$ is surjective and that p does not divide the minimal degree of a modular parametrisation $X_0(M) \longrightarrow E$. Let

$$\mathrm{Sym}^2 \varrho_f : G_\mathbb{Q} \to \mathrm{Aut}(\mathrm{Sym}^2(T_p E))$$

be the symmetric square representation of ϱ_f. The action of $G_\mathbb{Q}$ by conjugation on the module $\mathrm{Ad}^0(T_p E)$ of trace zero endomorphisms of $T_p E$ gives rise to the adjoint representation

$$\mathrm{Ad}^0 \varrho_f : G_\mathbb{Q} \to \mathrm{Aut}(\mathrm{Ad}^0(T_p E)).$$

The perfect $G_{\mathbb{Q}}$-equivariant pairing

$$\langle\ ,\ \rangle_f : \mathrm{Ad}^0(T_pE) \times \mathrm{Ad}^0(T_pE) \longrightarrow \mathbb{Z}_p, \qquad \langle A, B\rangle_f = \mathrm{Trace}(AB),$$

identifies $\mathrm{Ad}^0(T_pE)$ with its $\mathbb{Z}_p$-linear dual as a $G_{\mathbb{Q}}$-module. The classical Weil pairing $\langle\ ,\ \rangle_{\mathrm{Weil}}$ on T_pE yields a pairing

$$\langle\ ,\ \rangle_f : \mathrm{Sym}^2(T_pE) \times \mathrm{Ad}^0(T_pE) \longrightarrow \mathbb{Z}_p(1), \qquad \langle P \otimes Q, \lambda\rangle_f = \langle \lambda(P), Q\rangle_{\mathrm{Weil}}. \tag{16}$$

Following the introduction, we shall denote $T_f := \mathrm{Sym}^2\, T_pE$. The above discussion implies that the dual of T_f is

$$T_f^* \simeq \mathrm{Ad}^0(T_pE) \simeq T_f(-1).$$

We shall denote

$$A_f = T_f \otimes \mathbb{Q}_p/\mathbb{Z}_p \quad \text{and} \quad A_f^* = T_f^* \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

the p-divisible groups attached to T_f and T_f^* and

$$A_{f,n} = p^{-n}T_f/T_f \quad \text{and} \quad A_{f,n}^* = p^{-n}T_f^*/T_f^*.$$

their p^n-torsion parts.

Remark 5.1 The representation T_f plays a similar role to that of T_μ in Mazur's Eisenstein ideal setting. The crucial shared feature is that they are isomorphic to their duals up to twisting by $\mathbb{Z}_p(-1)$.

6 Local Cohomology Groups for the Symmetric Square Representation

This section describes the singular and finite part of the local cohomology of the representations T_f and T_f^* for all primes $N \nmid pM$.

Lemma 6.1 *Let $N \nmid pM$ be a prime. Then $H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f)$ is the torsion subgroup of $H^1(\mathbb{Q}_N, T_f)$, and there are isomorphisms*

$$H^1_{\mathrm{sing}}(\mathbb{Q}_N, T_f) \simeq \mathbb{Z}_p, \qquad H^1_{\mathrm{fin}}(\mathbb{Q}_N, A_f^*) \simeq \mathbb{Q}_p/\mathbb{Z}_p.$$

Proof Let $V_f = T_f \otimes \mathbb{Q}_p$. It follows from (15) that the eigenvalues of σ_N on V_f are α_N^2, β_N^2 and N, with

$$\alpha_N^2, \beta_N^2 \notin \{1, N^2\}.$$

Since no eigenvalue is equal to 1, the group $H^1_{\text{fin}}(\mathbb{Q}_N, V_f)$ is trivial. Thus, $H^1_{\text{fin}}(\mathbb{Q}_N, T_f)$ is the torsion subgroup of $H^1(\mathbb{Q}_N, T_f)$. Since the representation T_f is unramified at N, the morphism ∂_N identifies

$$H^1_{\text{sing}}(\mathbb{Q}_N, T_f) \xrightarrow{\sim} T_f(-1)^{G_N}$$

and the latter is isomorphic to $\mathbb{Z}_p$. The description of $H^1_{\text{fin}}(\mathbb{Q}_N, A_f^*)$ is then obtained via local Tate duality (10). □

We now turn to describing the finite part of the local cohomology $H^1_{\text{fin}}(\mathbb{Q}_N, T_f)$, which is the target of the isomorphism of Theorem 1.1. For a prime $N \nmid pM$, denote

$$r_f^+ = (N+1) - a_N(f) \qquad \text{and} \qquad r_f^- = a_N(f) + (N+1).$$

Definition 6.2 A prime $N \nmid pM$ that is called a *level-raising prime* for (f, p) if

$$p \text{ divides } r_f^+ r_f^- (N-1).$$

The terminology level-raising prime will be justified in light of Corollary 9.3. Note that, since p is assumed to be odd, it can divide at most two of the factors r_f^+, r_f^- and $(N-1)$.

Lemma 6.3 *The cohomology groups $H^1_{\text{fin}}(\mathbb{Q}_N, T_f)$ and $H^1_{\text{sing}}(\mathbb{Q}_N, A_f^*)$ are isomorphic finite abelian groups of order equal to*

$$\#\mathbb{Z}_p/(r_f^+ r_f^- (N-1)).$$

More precisely:

(i) if $p \nmid (N \pm 1)$, or if $p \mid (N-1)$ and $p \nmid r_f^+ r_f^-$, the group $H^1_{\text{fin}}(\mathbb{Q}_N, T_f)$ is cyclic.
(ii) If $p \mid (N+1)$, there is an isomorphism

$$H^1_{\text{fin}}(\mathbb{Q}_N, T_f) \simeq \mathbb{Z}_p/(r_f^+) \oplus \mathbb{Z}_p/(r_f^-).$$

Proof By Lemma 6.1, the finite local cohomology group $H^1_{\text{fin}}(\mathbb{Q}_N, T_f)$ is a finite abelian group, so it is isomorphic to its Pontryagin dual, which can be identified with $H^1_{\text{sing}}(\mathbb{Q}_N, A_f^*)$ by (10). Since T_f is unramified at N, Equation 7 yields an isomorphism

$$H^1_{\text{fin}}(\mathbb{Q}_N, T_f) \simeq T_f/(\sigma_N - 1)T_f.$$

Thus, describing the group structure of $H^1_{\text{fin}}(\mathbb{Q}_N, T_f)$ amounts to determining the Smith normal form of $(\text{Sym}^2 \varrho_f(\sigma_N) - 1)$. In particular, the order of the group is equal to p^v, where v is the p-adic valuation of $\det(\text{Sym}^2 \varrho_f(\sigma_N) - 1)$. A direct

calculation shows that the characteristic polynomial of σ_N acting on $V_f = T_f \otimes \mathbb{Q}_p$ is given by

$$x^3 - (a_N^2(f) - N)x^2 + N(a_N^2(f) - N)x^2 - N^3, \tag{17}$$

so that

$$\det(\mathrm{Sym}^2 \varrho_f(\sigma_N) - 1) = r_f^+ r_f^- \cdot (N-1).$$

Let p be a prime dividing $r_f^+ r_f^- \cdot (N-1)$. We shall consider the following cases.

(i) If either $p \nmid (N \pm 1)$ or $p \nmid r_f^+ r_f^-$, two of the eigenvalues of the matrix $(\mathrm{Sym}^2 \varrho_f(\sigma_N) - 1)$ are invertible in $\bar{\mathbb{Z}}_p$. On the other hand, it follows from properties of the Smith normal form that each eigenvalue of $\mathrm{Sym}^2 \varrho_f(\sigma_N) - 1$ must divide the exponent of $T_f/(\sigma_N - 1)T_f$ (in $\bar{\mathbb{Z}}_p$). As all but one eigenvalues are invertible, this forces $T_f/(\sigma_N - 1)T_f$ to be cyclic.

(ii) Suppose $p \mid (N+1)$, and $p \mid r_f^+ r_f^-$. Under these assumptions, the characteristic polynomial of $\bar{\varrho}_f(\sigma_N)$ has distinct roots equal to $\pm 1 \bmod p$; we shall assume that the eigenvalues of $\varrho_f(\sigma_N)$ are $\alpha_N, \beta_N \in \mathbb{Z}_p$ with

$$\alpha_N = 1 \mod p \quad \text{and} \quad \beta_N = -1 \mod p. \tag{18}$$

Since the eigenvalues residually distinct, σ_N acts semisimply on $T_p E$ and, as a consequence on T_f as well, with eigenvalues α_N^2, β_N^2, N on the latter. Hence,

$$T_f/(\sigma_N - 1)T_f \simeq \mathbb{Z}_p/(\alpha_N^2 - 1) \oplus \mathbb{Z}_p/(\beta_N^2 - 1) \oplus \mathbb{Z}_p/(N-1)\mathbb{Z}_p,$$

with $\mathbb{Z}_p/(N-1)\mathbb{Z}_p = 0$ under the running assumptions. Denote by v_p the p-adic valuation in $\mathbb{Z}_p$. The conclusion follows observing that

$$v_p(\alpha_N^2 - 1) = v_p(r_f^+), \quad \text{and} \quad v_p(\beta_N^2 - 1) = v_p(r_f^-),$$

in light of (18).

□

7 Local Cohomology via Discrete Elliptic Logarithms

This section describes the finite part of the cohomology group $H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f)$ in terms of the finite group $E(\Phi_{N^2})$ for every level-raising prime $p \nmid (N-1)$. This description is immaterial to the proof of Theorem 1.1. It is primarily motivated by the interpretation of generalised eigenvalues in terms of suitable discrete logarithms on the group $(\mathbb{Z}/N\mathbb{Z})^\times$ in the Eisenstein ideal setting given by (4).

Let τ be the generator of the group $\mathrm{Gal}(\Phi_{N^2}/\Phi_N)$. Since p is odd, every $\mathbb{Z}_p$-module L with an action of $\mathrm{Gal}\,(\Phi_{N^2}/\Phi_N)$ decomposes as $L = L^+ \oplus L^-$, where

$L^{\pm}$ is the ± 1-eigenspace for the action of τ. In particular, for $E(\Phi_{N^2}) \otimes \mathbb{Z}_p$, we obtain a decomposition

$$E(\Phi_{N^2}) \otimes \mathbb{Z}_p = (E(\Phi_{N^2}) \otimes \mathbb{Z}_p)^+ \oplus (E(\Phi_{N^2}) \otimes \mathbb{Z}_p)^-,$$

where $\#(E(\Phi_{N^2}) \otimes \mathbb{Z}_p)^{\pm} = \#\mathbb{Z}_p/(r_f^{\pm})$. There is a $\mathrm{Gal}(\Phi_{N^2}/\Phi_N)$-equivariant isomorphism

$$\nu\colon E(\Phi_{N^2}) \otimes \mathbb{Z}_p \xrightarrow{\sim} T_p E/(\sigma_N^2 - 1)T_p E,$$

induced by the isomorphisms given by the Kummer maps

$$E(\Phi_{N^2}) \otimes \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} E[p^n]/(\sigma_N^2 - 1)E[p^n], \qquad P \mapsto Q^{\sigma_N^2} - Q$$

where Q satisfies $p^n Q = P$ and n is a positive integer.

The natural map

$$\theta\colon (T_f/(\sigma_N^2 - 1)T_f)^+ \to T_f/(\sigma_N - 1)T_f \simeq H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f). \tag{19}$$

is an isomorphism, since p is an odd prime. It will be convenient to identify $H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f)$ with the source of θ.

For any $\mathbb{Z}_p[\mathrm{Gal}\,(\bar{\Phi}_N/\Phi_N)]$-module L, let $\mathrm{Sym}^2 L$ denote its symmetric square as a $\mathbb{Z}_p$-module, with the natural $\mathrm{Gal}\,(\bar{\Phi}_N/\Phi_N)$-action. The projection

$$\mathrm{Sym}^2(T_p E) \longrightarrow \mathrm{Sym}^2\left(T_p E/(\sigma_N^2 - 1)T_p E\right)$$

gives rise to a surjective homomorphism

$$\psi\colon T_f/(\sigma_N^2 - 1)T_f \longrightarrow \mathrm{Sym}^2\left(T_p E/(\sigma_N^2 - 1)T_p E\right)$$

compatible with the action of τ.

Let

$$j\colon H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f) \longrightarrow \left(\mathrm{Sym}^2(E(\Phi_{N^2}) \otimes \mathbb{Z}_p)\right)^+.$$

be the composition $j = (\nu^{-1} \otimes \nu^{-1}) \circ \psi \circ \theta^{-1}$, where $\nu^{-1} \otimes \nu^{-1}$ denotes the map induced by ν^{-1} on the respective symmetric squares.

Proposition 7.1 *If $p \nmid (N-1)$, then j is an isomorphism.*

Proof The composition j is surjective, so it suffices to compare cardinalities. Note that the target can be described as

$$\left(\mathrm{Sym}^2(E(\Phi_{N^2}) \otimes \mathbb{Z}_p)\right)^+ \simeq \mathrm{Sym}^2((E(\Phi_{N^2}) \otimes \mathbb{Z}_p)^+) \oplus \mathrm{Sym}^2((E(\Phi_{N^2}) \otimes \mathbb{Z}_p)^-).$$

Consider the exact sequence of $\mathbb{Z}_p[\mathrm{Gal}\,(\Phi_{N^2}/\Phi_N)]$-modules

$$0 \to E[p](\Phi_{N^2}) \to E(\Phi_{N^2}) \xrightarrow{p} E(\Phi_{N^2}) \to E(\Phi_{N^2}) \otimes \Phi_p \to 0$$

induced by multiplication by p. Then $(E(\Phi_{N^2}) \otimes \Phi_p)^{\pm}$ is isomorphic to the ± 1-eigenspace of $\bar{\varrho}_f(\sigma_N)$, since they are Φ_p-vector spaces of the same cardinality. If the characteristic polynomial of $\bar{\varrho}_f(\sigma_N)$ has a double root equal to ± 1, then $p \mid (N-1)$. Thus, we shall assume that $\dim_{\Phi_p}(E(\Phi_{N^2}) \otimes \Phi_p)^{\pm} \leq 1$, which implies that $E(\Phi_{N^2})^{\pm} \otimes \mathbb{Z}_p$ is cyclic and isomorphic to $\mathbb{Z}_p/(r_f^{\pm})$; the same is true for $\mathrm{Sym}^2((E(\Phi_{N^2}) \otimes \mathbb{Z}_p)^{\pm})$. The conclusion now follows from Lemma 6.3. □

Assume that $p \nmid (N-1)$ and that N is a level raising prime for (f, p). Let $n_{\pm}$ denote the p-adic valuation of $r_f^{\pm}$. If $n^{\pm} > 0$, a discrete logarithm for $E(\Phi_{N^2}) \otimes \mathbb{Z}_p$ is a surjective group homomorphism

$$\log_{E,N,p}^{\pm} \colon (E(\Phi_{N^2}) \otimes \mathbb{Z}_p)^{\pm} \to \mathbb{Z}/p^{n_{\pm}}\mathbb{Z}.$$

This choice is unique up to rescaling by a unit in $(\mathbb{Z}/p^{n_{\pm}}\mathbb{Z})^{\times}$, and both $\log_{E,N,p}^{+}$ and $\log_{E,N,p}^{-}$ exist if and only if, additionally, $p \mid (N+1)$. We shall drop the sign from the notation when $p \nmid (N+1)$. By abuse of notation, let

$$(\log_{E,N,p}^{\pm})^{\otimes 2} \colon H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f) \to \mathbb{Z}/p^{n_{\pm}}\mathbb{Z} \tag{20}$$

denote the homomorphism sending a class c to $(\log_{E,N,p}^{\pm})^{\otimes 2}(j(c))$. It follows from Proposition 7.1 that the $\mathbb{Z}_p$-module $\mathrm{Hom}(H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f), \mathbb{Q}_p/\mathbb{Z}_p)$ is generated by either the symmetric square of the unique discrete logarithm of $E(\Phi_{N^2}) \otimes \mathbb{Z}_p$ up to rescaling if $p \nmid (N+1)$ or

$$\{(\log_{E,N,p}^{+})^{\otimes 2}, (\log_{E,N,p}^{-})^{\otimes 2}\}$$

when $p \mid (N+1)$, where we view $\mathbb{Z}/p^{n_{\pm}}\mathbb{Z}$ as embedded in $\mathbb{Q}_p/\mathbb{Z}_p$ in the standard way.

8 Selmer Groups for the Symmetric Square Representation

Proposition 8.1 *The Selmer groups $H^1_{\emptyset}(\mathbb{Q}, T_f)$ and $H^1_{\emptyset}(\mathbb{Q}, A_f^*)$ are trivial.*

Proof The triviality of $H^1_{\emptyset}(\mathbb{Q}, A_f^*)$ is the main theorem of [10, Theorem 1] in light of the running assumptions on f and on p that were made in the introduction. From the long exact sequences in cohomology induced by multiplication by p^n on A_f^* it follows that for every $n \geq 1$, the Selmer group

$$H^1_{\emptyset}(\mathbb{Q}_N, A_{f,n}^*) \simeq H^1_{\emptyset}(\mathbb{Q}, A_f^*)[p^n]$$

is also trivial. Formula (14) applied to $W = A_{f,n}$ and $\Sigma_q = H^1_{\mathrm{fin}}(\mathbb{Q}_q, A_{f,n})$ for all q gives

$$\#H^1_{\emptyset}(\mathbb{Q}, A_{f,n}) = \#H^1_{\emptyset}(\mathbb{Q}, A^*_{f,n}) = 0,$$

and the proposition follows from passing to the inverse limit. □

Proposition 8.2 *Let $N \nmid pM$ be a rational prime. Restricting to the decomposition group at N and projecting onto the singular cohomology gives rise to isomorphisms*

$$\partial_N \circ \mathrm{res}_N \colon H^1_{(N)}(\mathbb{Q}, T_f) \xrightarrow{\sim} H^1_{\mathrm{sing}}(\mathbb{Q}_N, T_f)$$

and

$$\partial_N \circ \mathrm{res}_N \colon H^1_{(N)}(\mathbb{Q}, A^*_f) \xrightarrow{\sim} H^1_{\mathrm{sing}}(\mathbb{Q}_N, A^*_f).$$

In particular, $H^1_{(N)}(\mathbb{Q}, T_f) \simeq \mathbb{Z}_p$ for every $N \nmid pM$, and $H^1_{(N)}(\mathbb{Q}, A^*_f)$ is finite; it is non-trivial if and only if N is a level-raising prime for (f, p).

Proof Let $n \in \mathbb{Z}_{>0}$, and consider the cartesian diagram

$$\begin{array}{ccc} H^1_{\emptyset}(\mathbb{Q}, A_{f,n}) & \longrightarrow & H^1_{(N)}(\mathbb{Q}, A_{f,n}) \\ \downarrow & & \downarrow \\ H^1_{\mathrm{fin}}(\mathbb{Q}_N, A_{f,n}) & \longrightarrow & H^1(\mathbb{Q}_N, A_{f,n}) \end{array}$$

where the vertical arrows are given by restricting to the decomposition group at N. A similar cartesian diagram is obtained for $A^*_{f,n}$. The triviality of $H^1_{\emptyset}(\mathbb{Q}_N, A_{f,n})$ and $H^1_{\emptyset}(\mathbb{Q}_N, A^*_{f,n})$ shows that the natural maps

$$H^1_{(N)}(\mathbb{Q}, A_{f,n}) \to H^1_{\mathrm{sing}}(\mathbb{Q}_N, A_{f,n}) \text{ and } H^1_{(N)}(\mathbb{Q}, A^*_{f,n}) \to H^1_{\mathrm{sing}}(\mathbb{Q}_N, A^*_{f,n})$$

are injective. Proposition 8.1 implies that the restricted Selmer groups $H^1_{[N]}(\mathbb{Q}, A_{f,n})$ and $H^1_{[N]}(\mathbb{Q}, A^*_{f,n})$ are trivial *a fortiori*, and it follows from (14) that

$$\#H^1_{(N)}(\mathbb{Q}, A_{f,n}) = \#H^1_{\mathrm{sing}}(\mathbb{Q}_N, A_{f,n}), \qquad \#H^1_{(N)}(\mathbb{Q}, A^*_{f,n}) = \#H^1_{\mathrm{sing}}(\mathbb{Q}_N, A^*_{f,n}).$$

The conclusion is obtained by passing to inverse and direct limits and invoking Lemmas 6.1 and 6.3, respectively. □

Remark 8.3 Note how the hypothesis that N is a level-raising prime for (f, p) is essential for the non-triviality of $H^1_{(N)}(\mathbb{Q}, A^*_f)$, while $H^1_{(N)}(\mathbb{Q}, T_f)$ is always non-trivial for any prime $N \nmid 6Mp$, a key fact that underlies the existence of Flach classes described in Sect. 10.

9 Deformations of Galois Representations

The celebrated theorem of Wiles [17] and Taylor-Wiles [16] identifies certain localisations of Hecke algebras at the maximal ideal attached to f with suitable deformation rings. More precisely, let

$$\mathbb{T}(M)_{p,f} \quad \text{and} \quad \mathbb{T}(MN^2)_{p,f}$$

denote the localisations of the semi-local rings $\mathbb{T}(M) \otimes \mathbb{Z}_p$ and $\mathbb{T}(MN^2) \otimes \mathbb{Z}_p$ at the maximal ideals attached to $f \pmod p$. The morphisms

$$\varphi_{f,\emptyset} \colon \mathbb{T}(M)_{p,f} \to \mathbb{Z}_p \qquad \text{and} \qquad \varphi_{f,(N)} \colon \mathbb{T}(MN^2)_{p,f} \to \mathbb{Z}_p$$

are determined by sending the Hecke operator T_ℓ to the coefficient $a_\ell(f)$ for $\ell \nmid MNp$. Let $I_{f,\emptyset}$ and $I_{f,(N)}$ denote the kernels of the morphisms $\varphi_{f,\emptyset}$ and $\varphi_{f,(N)}$ respectively.

Let $R_{\bar{\varrho}_f,\emptyset}$ be the universal deformation ring parametrising lifts of the residual representation $\bar{\varrho}_f \colon G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ with fixed determinant, that are minimally ramified, in the sense of [4, Sect. 2.7], at primes $q \neq p$ and crystalline at p. Denote by $R_{\bar{\varrho}_f,(N)}$ the deformation ring classifying the lifts as above for which the local condition at N is omitted. Note that, since the residual representation $\bar{\varrho}_f$ is unramified at N, the highest power of N dividing the conductor of a lift of $\bar{\varrho}_f$ is at most N^2 (cf.[4, Lemma 2.7]). The universal properties of the deformation rings $R_{\bar{\varrho}_f,(N)}$ and $R_{\bar{\varrho}_f,\emptyset}$ give rise to a commutative diagram

$$\begin{array}{ccc} R_{\bar{\varrho}_f,(N)} & \xrightarrow{\gamma_{(N)}} & \mathbb{T}(MN^2)_{p,f} \\ \downarrow & & \downarrow \\ R_{\bar{\varrho}_f,\emptyset} & \xrightarrow{\gamma_\emptyset} & \mathbb{T}(M)_{p,f} \end{array}$$

where the vertical arrows are surjective. The Taylor-Wiles modularity lifting theorem (proved in full generality in [1]) implies that $\gamma_{(N)}$ and $\gamma_\emptyset$ are isomorphisms.

Definition 9.1 Given a cocycle κ representing a class in $H^1_{(N)}(\mathbb{Q}, A_f^*)$, and a prime $\ell \nmid NMp$, the *generalised eigenvalue* attached to κ at ℓ is

$$a'_\ell(f,\kappa) := \mathrm{Tr}(\kappa(\sigma_\ell)\varrho_f(\sigma_\ell)).$$

Note that this is independent of the choice of the representative of the cohomology class and of the Frobenius element $\sigma_\ell \in G_\ell$. When the group $H^1_{(N)}(\mathbb{Q}, A_f^*)$ is cyclic, a choice of generator κ can be fixed throughout, and we will simply denote $a'_\ell(f) := a'_\ell(f,\kappa)$.

The term generalised eigenvalue is justified by the following immediate consequence of the modularity lifting theorem.

Proposition 9.2 *For $\bigstar \in \{\emptyset, (N)\}$, there is an isomorphism*

$$H^1_{\bigstar}(\mathbb{Q}, A_f^*) \xrightarrow{\sim} \mathrm{Hom}(I_{f,\bigstar}/I_{f,\bigstar}^2, \mathbb{Q}_p/\mathbb{Z}_p)$$

sending a class $\kappa \in H^1_{\bigstar}(\mathbb{Q}, A_f^*)$ to the morphism $F_\kappa : I_{f,\bigstar}/I_{f,\bigstar}^2 \to \mathbb{Q}_p/\mathbb{Z}_p$ characterised by

$$F_\kappa(T_\ell - a_\ell) = a'_\ell(f, \kappa)$$

for every $\ell \nmid MNp$.

Proof Let $J_\bigstar$ be the kernel of $\phi_{f,\bigstar} \circ \gamma_\bigstar$. A standard calculation (see, for example, [4, Lemma 2.40]) identifies $H^1_{\bigstar}(\mathbb{Q}, T_f^*)$ with $\mathrm{Hom}(J_\bigstar/J_\bigstar^2, \mathbb{Q}_p/\mathbb{Z}_p)$ via the map induced by

$$H^1_{\bigstar}(\mathbb{Q}, A^*_{f,n}) \xrightarrow{\sim} \mathrm{Hom}_{(\mathbb{Z}/p^n\mathbb{Z})-\mathrm{aug}}(R_{\bar{\varrho}_f,\bigstar}, \mathbb{Z}/p^n\mathbb{Z}[\varepsilon]/(\varepsilon^2))$$

for $n \in \mathbb{Z}_{>0}$, where the target denotes homomorphisms of $\mathbb{Z}/p^n\mathbb{Z}$-augmented rings, which sends a cohomology class κ to

$$\tilde{\varrho}_f = (1 + \varepsilon \cdot \kappa) \cdot \varrho_f.$$

Upon identifying $I_{f,\bigstar} \simeq J_\bigstar$, the conclusion follows from the fact that

$$\mathrm{Trace}(\tilde{\varrho}_f(\sigma_\ell)) = a_\ell(f) + a'_\ell(f, \kappa) \cdot \varepsilon.$$

□

Combining this result with Propositions 8.1 and 8.2, we obtain the following corollary.

Corollary 9.3 *Let $p \nmid 6\deg(\phi_E)$ be a prime such that $\bar{\varrho}_f$ is surjective. Then:*

1. *The ideal $I_{f,\emptyset}$ is trivial;*
2. *The ideal $I_{f,(N)}$ is non-trivial if and only if N is a level-raising prime for (f, p). If $p \nmid (N \pm 1)$ or if $p \mid (N-1)$ and $p \nmid r_f^+ r_f^-$, the ideal $I_{f,(N)}$ is cyclic.*

In particular, it follows that the generalised eigenspace attached to f in $M_2(M) \otimes \Phi_p$ is spanned by f, while it is strictly larger in $M_2(MN^2) \otimes \Phi_p$ when N is a level-raising prime for (f, p).

10 Flach Classes

The goal of this section is to introduce the Flach classes $c_f[\ell] \in H^1_{(\ell)}(\mathbb{Q}, T_f)$, following [10, Sect. 2]. These classes are the key ingredient in Flach's proof of Propo-

sition 8.1. This section and the next complements this by reinterpreting the generalised eigenvalues $a'_\ell(f,\kappa)$ appearing in Proposition 9.2 as the local Tate pairing at ℓ between the classes κ and $c_f[\ell]$.

Let X be an irreducible regular Notherian scheme which is either of finite type over a field or is smooth over a discrete valuation ring. Of importance for the constructions of [10, Sect. 2] are the cases where:

1. X is the modular surface $X_0(M)^2$ viewed as a scheme over spec $\mathbb{Q}$;
2. $X = \mathscr{X}_0(M)^2_{\mathbb{Z}_\ell}$ is the smooth proper integral model of $X_0(M)^2$ over spec $\mathbb{Z}_\ell$ for $\ell \nmid M$.

Let $\mathscr{K}_2$ be the sheaf associated to the Quillen's second K-group functor $U \mapsto K_2(U)$. The group $H^1(X, \mathscr{K}_2)$ is the first homology of the complex

$$K_2(k(X)) \xrightarrow{\partial} \oplus_{x\in X^{(1)}} k(x)^\times \xrightarrow{\text{div}} \oplus_{x\in X^{(2)}} \mathbb{Z}, \tag{21}$$

where $X^{(n)}$ is the set of codimension n subschemes of X, and $k(x)$ is the residue field of the local ring of X at x. The map ∂ is a residue map and div sends an element $u \in k(x)^\times$ to the pushforward to X of its divisor on x.

Let $\ell \nmid M$ be a prime, and let

$$\pi_1, \pi_2 : X_0(M\ell) \longrightarrow X_0(M), \qquad \pi := (\pi_1, \pi_2) : X_0(M\ell) \longrightarrow X := X_0(M)^2$$

be the maps arising from the two standard degeneracy maps sending a pair (A_1, A_2) of elliptic curves with level M structure related by a cyclic ℓ-isogeny to the points of $X_0(M)$ attached to A_1 and A_2 respectively. The image

$$T_\ell := \pi(X_0(M\ell)) \subset X$$

is birational to $X_0(M\ell)$ and is the graph of the ℓ-th Hecke correspondence on $X_0(M)$. The modular unit $\Delta(z)/\Delta(\ell z)$ has divisor supported at the cusps of $X_0(M\ell)$, and the pushforward of this divisor to X vanishes [10, p. 317]. It follows that the element

$$\varepsilon(\ell) := (\Delta(z)/\Delta(\ell z)) \in k(T_\ell)^\times$$

belongs to the kernel of the map div of (21), and thus defines an element of $H^1(X, \mathscr{K}_2)$.

The special element $\varepsilon(\ell)$ can be parlayed into the construction of global cohomology classes

$$c[\ell] \in H^1(\mathbb{Q}, H^2_{\text{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2))), \qquad c_f[\ell] \in H^1(\mathbb{Q}, T_f)$$

by setting

$$c[\ell] := h \cdot \kappa(\varepsilon(\ell)), \qquad c_f[\ell] := \text{Sym}_*(\phi_E \times \phi_E)_*(c[\ell]),$$

where

(1) the map
$$\kappa : H^1(X, \mathscr{K}_2) \longrightarrow H^3_{\text{et}}(X, \mathbb{Z}_p(2))$$
is an étale regulator map. Roughly speaking, it is obtained by combining the Kummer maps
$$\delta_x : k(x)^\times \longrightarrow H^1_{\text{et}}(k(x), \mathbb{Z}_p(1))$$
of Kummer theory with the pushforward maps
$$i_{x*} : H^1_{\text{et}}(x, \mathbb{Z}_p(1)) \longrightarrow H^3_{\text{et}}(X, \mathbb{Z}_p(2))$$
in étale cohomology, induced by the inclusions $i_x : x \hookrightarrow X$;

(2) the map
$$h : H^3_{\text{et}}(X, \mathbb{Z}_p(2)) \longrightarrow H^1(\mathbb{Q}, H^2_{\text{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2)))$$
arises from an edge map in the Hochschild-Serre spectral sequence
$$H^p(\mathbb{Q}, H^q_{\text{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2))) \Rightarrow H^{p+q}_{\text{et}}(X, \mathbb{Z}_p(2)),$$
in light of the triviality of $H^3(X_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2))^{G_{\mathbb{Q}}}$ which follows from weight considerations ([10, Proposition 2.2]);

(3) the map
$$(\phi_E \times \phi_E)_* : H^1(\mathbb{Q}, H^2(X_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2))) \longrightarrow H^1(\mathbb{Q}, H^2(E^2_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2)))$$
is the pushforward induced by the map $\phi_E \times \phi_E : X \longrightarrow E^2$ arising from the modular parametrisation ϕ_E;

(4) the last map
$$\text{Sym}_* : H^1(\mathbb{Q}, H^2(E^2_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2))) \longrightarrow H^1(\mathbb{Q}, T_f)$$
is induced from the natural Kunneth projection from $H^2(E^2_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2))$ to $H^1(E_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(1))^{\otimes 2}$ composed with the projection to the space
$$T_f = \text{Sym}^2(H^1_{\text{et}}(E_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(1)))$$
of symmetric tensors.

Remark 10.1 When $p|(N-1)$, Chris Skinner has proposed an interesting construction of a global class in the cohomology of the adjoint representation, which is somewhat dual to Flach's construction. This class is obtained from the *Shimura class*
$$\mathfrak{S} \in H^1_{\text{et}}(X_0(MN), \mathbb{Z}/p^n\mathbb{Z})$$

arising by applying the discrete logarithm $(\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ to the class of the étale covering $X_1(N) \longrightarrow X_0(N)$ with Galois group $(\mathbb{Z}/N\mathbb{Z})^\times/(\pm 1)$. The image of $\mathfrak{S}$ under pushforward by the diagonal embedding $\Delta\colon X_0(MN) \hookrightarrow X_0(MN)^2$ yields a class

$$\kappa \in H^3_{\text{ét}}(X_0(MN)^2, \mathbb{Z}/p^n\mathbb{Z}(1))$$

to which steps (2)-(3)-(4) above can be applied, leading ultimately to a class in $H^1(\mathbb{Q}, A^*_{f,n})$. This class appears to play a role analogous to the class in $H^1_{(N)}(\mathbb{Q}, \mathbb{Z}/p^n\mathbb{Z})$ arising from global class field theory (or the Kronecker-Weber theorem) which also depends linearly on the choice of a discrete logarithm on $(\mathbb{Z}/N\mathbb{Z})^\times$.

11 Local Behaviour of the Flach Classes

If r is a prime that does not divide M, then the curve $X_0(M)$ extends to a smooth proper model $\mathscr{X}_0(M)_{\mathbb{Z}_r}$ over $\text{spec}(\mathbb{Z}_r)$. Let $\mathscr{X}_0(M)_{\Phi_r}$ denote its special fiber, and write

$$\mathscr{X}_{\mathbb{Z}_r} := \mathscr{X}_0(M)^2_{\mathbb{Z}_r}, \qquad X_{\mathbb{Q}_r} := X_0(M)^2_{\mathbb{Q}_r}, \qquad \mathscr{X}_{\Phi_r} := \mathscr{X}_0(M)^2_{\Phi_r}.$$

There is an exact localisation sequence ([10, (17)])

$$H^1(\mathscr{X}_{\mathbb{Z}_r}, \mathscr{K}_2) \longrightarrow H^1(X_{\mathbb{Q}_r}, \mathscr{K}_2) \xrightarrow{\partial_r} \text{Pic}(\mathscr{X}_{\Phi_r}),$$

where ∂_r sends $u \in k(x)^\times$ to its divisor along the special fiber. It is shown (cf. [10, (19)]) that

$$\partial_r(\varepsilon(\ell)) = \begin{cases} 0 & \text{if } r \neq \ell; \\ 6 \cdot (\Gamma_\ell - \Gamma'_\ell) & \text{if } r = \ell, \end{cases} \tag{22}$$

where $\Gamma_\ell \in \text{Pic}(\mathscr{X}_{\Phi_\ell})$ is the class of the graph of the Frobenius morphism $\mathscr{X}_0(M)_{\Phi_\ell} \longrightarrow \mathscr{X}_0(M)_{\Phi_\ell}$, and Γ'_ℓ is the class of its transpose.

The elliptic curve E extends to a smooth proper model $\mathscr{E}$ over $\mathbb{Z}_\ell$, with special fiber $\mathscr{E}_{\Phi_\ell}$. Let

$$\Gamma_{\ell,E} \in \text{Pic}((\mathscr{E} \times \mathscr{E})_{\Phi_\ell})$$

be the class of the graph of the Frobenius endomorphism on $\mathscr{E}_{\Phi_\ell}$, and let $\Gamma'_{\ell,E}$ be the class of its transpose. They are related to Γ_ℓ and Γ'_ℓ by the formulae

$$(\phi_E \times \phi_E)_*(\Gamma_\ell) = \deg(\phi_E) \cdot \Gamma_{\ell,E}, \qquad (\phi_E \times \phi_E)_*(\Gamma'_\ell) = \deg(\phi_E) \cdot \Gamma'_{\ell,E}. \tag{23}$$

Proposition 11.1 *Let $\ell \nmid Mp$ be a rational prime.*

1. *The global class $c[\ell]$ belongs to $H^1_{(\ell)}(\mathbb{Q}, H^2_{\text{ét}}(X_{\bar{\mathbb{Q}}}, \mathbb{Z}_p(2)))$, and*

$$\partial_\ell(c[\ell]) = 6 \cdot \text{cl}(\Gamma_\ell - \Gamma'_\ell),$$

where

$$\mathrm{cl} : \mathrm{Pic}(\mathscr{X}_{\Phi_\ell}) \longrightarrow H^2_{\mathrm{et}}(\mathscr{X}_{\bar{\Phi}_\ell}, \mathbb{Z}_p(2))^{G_{\Phi_\ell}}$$

is the étale cycle class map.

2. *The global class $c_f[\ell]$ belongs to $H^1_{(\ell)}(\mathbb{Q}, T_f)$, and*

$$\partial_\ell(c_f[\ell]) = 6 \cdot \deg(\phi_E) \cdot \mathrm{Sym}_*(\mathrm{cl}(\Gamma_{\ell,E} - \Gamma'_{\ell,E})).$$

Proof These two assertions follow from chasing through the top and bottom parts of the commutative diagram

$$\begin{array}{ccccc}
H^1(\mathscr{X}_{\mathbb{Z}_r}, \mathscr{K}_2) & \longrightarrow & H^1(X_{\mathbb{Q}_r}, \mathscr{K}_2) & \xrightarrow{\partial_r} & \mathrm{Pic}(\mathscr{X}_{\Phi_r}) \\
\downarrow{\scriptstyle h\cdot\kappa} & & \downarrow{\scriptstyle h\cdot\kappa} & & \downarrow{\scriptstyle \mathrm{cl}} \\
 & & & & H^2_{\mathrm{et}}(\mathscr{X}_{\Phi_r}, \mathbb{Z}_p(1)) \\
 & & & & \| \\
H^1_{\mathrm{fin}}(\mathbb{Q}_r, H^2_{\mathrm{et}}(X, \mathbb{Z}_p(2))) & \longrightarrow & H^1(\mathbb{Q}_r, H^2_{\mathrm{et}}(X, \mathbb{Z}_p(2))) & \xrightarrow{\partial_r} & H^2_{\mathrm{et}}(X, \mathbb{Z}_p(1))^{G_{\mathbb{Q}_r}} \\
\downarrow{\scriptstyle \mathrm{Sym}(\phi_E\times\phi_E)_*} & & \downarrow{\scriptstyle \mathrm{Sym}(\phi_E\times\phi_E)_*} & & \downarrow{\scriptstyle \mathrm{Sym}(\phi_E\times\phi_E)_*} \\
H^1_{\mathrm{fin}}(\mathbb{Q}_r, T_f) & \longrightarrow & H^1(\mathbb{Q}_r, T_f) & \xrightarrow{\partial_r} & T_f(-1)^{G_{\mathbb{Q}_r}},
\end{array}$$

and invoking (22) for the first, and (23) for the second. □

This determination of $\partial_\ell(c_f[\ell])$ can be used to compute the local Tate pairing between $c_f[\ell]$ and a global class $\kappa \in H^1_{(N)}(\mathbb{Q}, A_f^*)$.

Proposition 11.2 *For all primes $\ell \nmid MNp$, and $\kappa \in H^1_{(N)}(\mathbb{Q}, A_f^*)$*

$$\langle c_f[\ell], \kappa\rangle_\ell = 12 \cdot \deg(\phi_E) \cdot a'_\ell(f, \kappa).$$

Proof By setting $c = c_f[\ell]$ in (11), we obtain

$$\langle c_f[\ell], \kappa\rangle_\ell = \langle \partial_\ell(c_f[\ell]), \kappa(\sigma_\ell)\rangle, \tag{24}$$

where the pairing on the right is induced from the natural $\mathbb{Q}_p/\mathbb{Z}_p$-valued trace pairing between $T_f(-1)$ and $T_f^* \simeq T_f(-1) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

On the other hand, Proposition 11.1 gives

$$\partial_\ell(c_f[\ell]) = 6 \cdot \deg(\phi_E) \cdot \mathrm{Sym}_*\mathrm{cl}(\Gamma_{\ell,E} - \Gamma'_{\ell,E}) = 6 \cdot \deg(\phi_E) \cdot (\varrho_f(\sigma_\ell) - \varrho_f(\sigma_\ell)'),$$

where $\varrho_f(\sigma_\ell)$ is viewed as an element of $\mathrm{End}(T_pE) \supset \mathrm{Aut}(T_pE)$, and $\varrho_f(\sigma_\ell)'$ is the adjoint of $\varrho_f(\sigma_\ell)$ relative to the Weil pairing on T_pE, i.e., its *adjugate*

$$\varrho_f(\sigma_\ell)' = a_\ell(f) - \varrho_f(\sigma_\ell).$$

It follows that

$$\partial_\ell(c_f[\ell]) = 6 \cdot \deg(\phi_E) \cdot (2 \cdot \varrho_f(\sigma_\ell) - a_\ell(f)). \tag{25}$$

Combining (24) with (25) gives

$$\begin{aligned} \langle c_f[\ell], \kappa \rangle_\ell &= 12 \cdot \deg(\phi_E) \cdot \langle \varrho_f(\sigma_\ell), \kappa(\sigma_\ell) \rangle \\ &= 12 \cdot \deg(\phi_E) \cdot \mathrm{Trace}(\varrho_f(\sigma_\ell) \cdot \kappa(\sigma_\ell)) \end{aligned}$$

and the formula follows. □

12 An Application of Global Reciprocity

Proposition 12.1 *For all primes $\ell \nmid MNp$, and $\kappa \in H^1_{(N)}(\mathbb{Q}, A_f^*)$,*

$$\langle c_f[\ell], \kappa \rangle_N = -12 \cdot \deg(\phi_E) \cdot a'_\ell(f, \kappa).$$

Proof Since $c_f[\ell]$ belongs to $H^1_{(\ell)}(\mathbb{Q}, T_f)$, and κ belongs to $H^1_{(N)}(\mathbb{Q}, A_f^*)$, it follows that

$$\langle c_f[\ell], \kappa \rangle_q = 0 \qquad \text{for all } q \neq \ell, N.$$

Therefore, (12) implies that

$$\langle c_f[\ell], \kappa \rangle_\ell + \langle c_f[\ell], \kappa \rangle_N = 0,$$

and the result follows from Proposition 11.2. □

Proof The isomorphism defined in Proposition 9.2 sends a global class κ in $H^1_{(N)}(\mathbb{Q}, A_f^*)$ to the map $F_\kappa : I_{f,(N)}/I^2_{f,(N)} \to \mathbb{Q}_p/\mathbb{Z}_p$ characterised by the property

$$F_\kappa(T_\ell - a_\ell) = \mathrm{Trace}(\kappa(\sigma_\ell)\varrho_f[\ell]) = (12 \cdot \deg(\phi_E))^{-1} \langle c_f[\ell], \kappa \rangle_\ell$$

for every prime $\ell \nmid MNp$ by Lemma 11.2. On the other hand, by Proposition 8.2, the restriction to the decomposition group at N, combined with local Tate duality gives an isomorphism

$$H^1_{(N)}(\mathbb{Q}, A_f^*) \xrightarrow{\sim} \mathrm{Hom}(H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f), \mathbb{Q}_p/\mathbb{Z}_p)$$

sending κ to the homomorphism $\kappa \mapsto \langle c, \kappa \rangle_N$ for $c \in H^1_{\mathrm{fin}}(\mathbb{Q}_N, T_f)$. The result now follows from Proposition 12.1 by passing to Pontryagin duals. □

Proof of Corollary 1.2 This follows immediately from Theorem 1.1, and the fact that if $p \nmid (N \pm 1)$, the ideal $I_{f,(N)}$ is cyclic by Corollary 9.3. □

Remark 12.2 The generalised eigenvalues attached to a cusp form f can be easily computed numerically. For simplicity, assume that $p \parallel r_f^+ r_f^-(N-1)$. Then $I_{f,(N)}/I_{f,(N)}^2 = \mathbb{Z}/p\mathbb{Z} \cdot T$, for some Hecke operator $T \in I_{f,(N)}$. This implies that the generalised eigenspace attached to the system of eigenvalues of f in the space of mod p modular forms of weight 2 and level $\Gamma_0(MN^2)$ admits a basis $f = f_1, \ldots, f_r$ for some $r > 1$ such that

$$Tf_i = f_{i-1} \qquad \text{for every } 1 \leq i \leq r.$$

where we set $f_0 = 0$. The generalised eigenvalues are characterised by the property

$$(T_\ell - a_\ell(f))f_i = a'_\ell(f)\ f_{i-1} \mod (f_0, \ldots, f_{i-2}), \qquad \text{for every } \ell \nmid NMp.$$

for $i > 1$, up to rescaling by a common constant in $(\mathbb{Z}/p\mathbb{Z})^\times$ (cf. [12, Sect. 2]).

Remark 12.3 For any prime $\ell \nmid Mp$, the Flach class $c_f[\ell]$ is obtained from the image of a canonical element in motivic cohomology $H^1(\mathscr{X}_{\Phi_N}, \mathscr{K}_2)$ under the composition of the maps described in Sect. 10. An independent description of the image of the resulting local class under the morphism $\log^{\otimes 2}_{E,N,p}$, suitable for machine calculations for instance, appears somewhat elusive. The connection between $c_f[\ell]$ and the generalised eigenvalues a'_ℓ, which are more readily calculated numerically, supplies non-trivial information about the behaviour of Flach's classes as the prime ℓ varies.

References

1. Breuil, C., Conrad, B., Diamond, F., Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Am. Math. Soc. **14**(4), 843–939 (2001)
2. Bloch, S., Kato, K.: L-functions and Tamagawa numbers of motives. The Grothendieck Festschrift, Collect. Artic. in Honor of the 60th Birthday of A. Grothendieck. Vol. I, Prog. Math. **86**, 333–400 (1990)
3. Calegari, F., Emerton, M.: On the ramification of Hecke algebras at Eisenstein primes. Invent. Math. **160**(1), 97–144 (2005)
4. Darmon, H., Diamond, F., Taylor, R., Theorem, F.L., Current, I., developments in mathematics, 1995. Lectures of a seminar, held in Boston, MA, USA, May 7–8, 1995, pp. 1–107 (1–154, preliminary version,: Cambridge, p. 1995. International Press, MA (1994)
5. Darmon, H., Harris, M., Rotger, V., Venkatesh, A.: The derived Hecke algebra for dihedral weight one forms. Mich. Math. J. **72**, 145–207 (2022)
6. Darmon, H., Lauder, A., Rotger, V.: Overconvergent generalised eigenforms of weight one and class fields of real quadratic fields. Adv. Math. **283**, 130–142 (2015)
7. Darmon, H., Lauder, A., Rotger, V.: First order p-adic deformations of weight one newforms. In: L-functions and automorphic forms. LAF, Heidelberg, Germany, February 22–26, 2016, pp. 39–80. Springer, Cham (2017)

8. Darmon, H., Pozzi, A., Vonk, J.: The values of the Dedekind-Rademacher cocycle at real multiplication points. J. EMS (2023)
9. Darmon, H., Vonk, J.: Heights of RM divisors and real quadratic singular moduli. In progress
10. Flach, M.: A finiteness theorem for the symmetric square of an elliptic curve. Invent. Math. **109**(2), 307–327 (1992)
11. Harris, M., Venkatesh, A.: Derived Hecke algebra for weight one forms. Exp. Math. **28**(3), 342–361 (2019)
12. Lecouturier, E.: Higher Eisenstein elements, higher Eichler formulas and rank of Hecke algebras. Invent. Math. **223**(2), 485–595 (2021)
13. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. Inst. Hautes Étud. Sci. **47**, 33–186 (1977)
14. Merel, L.: The Weil pairing between the Shimura subgroup and the cuspidal subgroup of $J_0(p)$. J. Reine Angew. Math. **477**, 71–115 (1996)
15. Rubin, K.: Euler systems. (Hermann Weyl lectures), volume 147 of Ann. Math. Stud. Princeton, NJ, Princeton University Press (2000)
16. Taylor, R., Wiles, A.: Ring-theoretic properties of certain Hecke algebras. Ann. Math. (2) **141**(3), 553–572 (1995)
17. Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. Ann. Math. (2) **141**(3), 443–551 (1995)
18. Wake, P., Wang-Erickson, C.: The rank of Mazur's Eisenstein ideal. Duke Math. J. **169**(1), 31–115 (2020)