Modular symbols and the integrality of zeta elements

Takako Fukaya, Kazuya Kato, Romyar Sharifi

Dedicated to Professor Glenn Stevens on the occasion of his 60th birthday

Abstract

We consider modifications of Manin symbols in first homology groups of modular curves with $\mathbb{Z}_p$-coefficients for an odd prime p. We show that these symbols generate homology in primitive eigenspaces for the action of diamond operators, with a certain condition on the eigenspace that can be removed on Eisenstein parts. We apply this to prove the integrality of maps taking compatible systems of Manin symbols to compatible systems of zeta elements. In the work of the first two authors on an Iwasawa-theoretic conjecture of the third author, these maps are constructed with certain bounded denominators. As a consequence, their main result on the conjecture was proven after inverting p, and the results of this paper allow one to remove this condition.

1   Introduction

1.1   Homology and (c, d)-symbols

Let $p \geq 5$ be a prime, and let N be a positive integer. We let $X_1(N)$ denote the compact modular curve of level N over $\mathbb{C}$ and let $C_1(N)$ denote its set of cusps. Consider the relative homology group

$$\tilde{H} = H_1(X_1(N), C_1(N), \mathbb{Z}_p).$$

Manin showed that $\tilde{H}$ is generated by elements $[u : v]$ attached to pairs (u, v) with $u, v \in \mathbb{Z}/N\mathbb{Z}$ and $(u, v) = (1)$ (see Section 3.1). For integers c and d greater than 1 and prime to $6N$, we define the (c, d)-symbol for the pair (u, v) by

$$_{c,d}[u : v] = c^2 d^2 [u : v] - c^2 [u : d v] - d^2 [c u : v] + [c u : d v].$$

Let $\tilde{C}$ denote the $\mathbb{Z}_p$-span in $\tilde{H}$ of all (c, d)-symbols as we vary c and d. We will examine the difference between $\tilde{C}$ and $\tilde{H}$.

Now, let M a positive integer such that $p \nmid M\varphi(M)$, and set $N = M$ or Mp. Let θ be an even p-adic character of $(\mathbb{Z}/N\mathbb{Z})^\times$ of conductor divisible by M. Let $\tilde{H}^{(\theta)}$ denote the θ-eigenspace of $\tilde{H}$ under the action of inverse diamond operators, and similarly for $\tilde{C}$. Let $\mathcal{O}_\theta$ denote the $\mathbb{Z}_p$-algebra generated by the values of θ. Let ω denote the Teichmüller character on $(\mathbb{Z}/p\mathbb{Z})^\times$, and note that we can view both it and θ as characters on $(\mathbb{Z}/Mp\mathbb{Z})^\times$. We prove the following result (and a counterpart for $p = 3$):

Theorem 1.1.1. *If $\theta \neq \omega^2$, then the $\mathcal{O}_\theta$-module $\tilde{H}^{(\theta)}$ is spanned by $\tilde{C}^{(\theta)}$ and the projection of $[1 : p]$ to $\tilde{H}^{(\theta)}$. Moreover, if $\theta\omega^{-2}|_{(\mathbb{Z}/p\mathbb{Z})^\times} \neq 1$, then $\tilde{H}^{(\theta)} = \tilde{C}^{(\theta)}$.*

Let I denote the Eisenstein ideal of the Hecke algebra $\mathfrak{H}$ in $\mathrm{End}_{\mathbb{Z}_p}(\tilde{H})$ generated by $T_\ell - 1 - \ell\langle\ell\rangle$ for primes $\ell \nmid N$ and $U_\ell - 1$ for primes $\ell \mid N$, and let $\mathfrak{m} = I + (p, \langle 1+p\rangle - 1)$. We exhibit the following strengthening of Theorem 1.1.1 on Eisenstein components (i.e., for the localization $\tilde{H}^{(\theta)}_{\mathfrak{m}}$ of $\tilde{H}^{(\theta)}$ at the maximal ideal $\mathfrak{m}\mathfrak{H}^{(\theta)}$ of $\mathfrak{H}^{(\theta)}$).

Theorem 1.1.2. *For $\theta \neq \omega^2$, the $\mathcal{O}_\theta$-modules $\tilde{H}^{(\theta)}_{\mathfrak{m}}$ and $\tilde{C}^{(\theta)}_{\mathfrak{m}}$ are equal.*

Theorems 1.1.1 and 1.1.2 are derived in Section 3.1 from the results of Section 2. We actually derive these results as simple corollaries of variants of arithmetic interest for the $\mathbb{Z}_p$-submodule H of $\tilde{H}$ generated by those Manin symbols $[u : v]$ with $u, v \neq 0$. This H is the relative homology group $H_1(X_1(N), C_1^0(N), \mathbb{Z}_p)$, where $C_1^0(N)$ denotes those cusps of $X_1(N)$ that do not lie above the zero cusp of $X_0(N)$.

Remark 1.1.3. If we let C denote the $\mathbb{Z}_p$-span of all (c, d)-symbols $_{c,d}[u : v]$ for nonzero u and v, then both of the above results hold with $\tilde{H}$ replaced by H and $\tilde{C}$ replaced by C, the second theorem even for $\theta = \omega^2$.

In Section 3.1, we explain how these results can be used to prove that compatible sequences of (c, d)-symbols generate the ordinary and Eisenstein parts of homology up the tower $X_1(Mp^r)$ of modular curves.

1.2 Application to Iwasawa theory

Let $\mathscr{S}$ denote the space of Λ-adic cusp forms of level Mp^∞, where $\Lambda \cong \mathbb{Z}_p[\![1 + p\mathbb{Z}_p]\!]$ is the usual Iwasawa algebra. The group elements in Λ act as inverses of diamond operators on $\mathscr{S}$. Let I denote the Eisenstein ideal in the Hecke algebra acting on $\mathrm{End}_{\mathbb{Z}_p}(\mathscr{S})$, defined as above. Let X denote the unramified Iwasawa module over the cyclotomic $\mathbb{Z}_p$-extension K of $\mathbb{Q}(\mu_N)$ for $N = Mp$, i.e., the Galois group of the maximal unramified abelian pro-p extension of K. It has the structure of a $\mathbb{Z}_p[\![\mathrm{Gal}(K/\mathbb{Q})]\!] \cong \Lambda[(\mathbb{Z}/N\mathbb{Z})^\times]$-module under conjugation by lifts of group elements.

Suppose now that $\theta\omega^{-1}$ has conductor N or that $\theta\omega^{-1}|_{(\mathbb{Z}/M\mathbb{Z})^\times}(p) \neq 1$, and also that $\theta \neq 1, \omega^2$. Set

$$P = \mathscr{S}^{(\theta)}/I\mathscr{S}^{(\theta)} \quad \text{and} \quad Y = X(1)^{(\theta)}$$

As defined in [Sh1, FK], there are canonical Λ-module homomorphisms

$$\varpi\colon P \to Y \quad \text{and} \quad \Upsilon\colon Y \to P,$$

the first being explicitly defined to take a sequence of Manin symbols to a certain sequence of cup products of cyclotomic N-units (see also [Bu] at level p), and the second being defined via the action of Galois on étale cohomology groups of modular curves (and constructed out of maps occurring in Hida-theoretic proofs of the main conjecture [Wi, Oh2]). In [Sh1], it was conjectured that these maps are inverse to each other, up to a unit suspected to be 1. This was shown to be true in [FK] upon tensoring with $\mathbb{Q}_p$, after multiplication by a power series ξ' interpolating the derivative of the p-adic L-function of $\omega^2\theta^{-1}$. That is, it was shown that

$$\xi'\Upsilon \circ \varpi = \xi'\colon P \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to P \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Our generation result allows us to remove the tensor product with $\mathbb{Q}_p$, which is to say to not have to work modulo torsion in P.

Theorem 1.2.1. *One has $\xi'\Upsilon \circ \varpi = \xi'$ as endomorphisms of P.*

The key point is that there is an intermediate map $z^\sharp$, used in defining ϖ, and through which both sides of the above identity factor, sending compatible sequences of Manin symbols up the modular tower $X_1(Mp^r)$ to compatible sequences of zeta elements. As constructed in [FK, Section 3.3], the map $z^\sharp$ is only defined rationally, which is to say that it takes values in $H^1(\mathbb{Z}[\frac{1}{N}], \mathscr{T}(1)) \otimes_\Lambda Q(\Lambda)$, where $\mathscr{T}$ is an inverse limit of ordinary parts of étale cohomology groups of the modular curves $X_1(Mp^r)$, and $Q(\Lambda)$ is the quotient field of Λ. In Theorem 3.2.11, we show that $z^\sharp$ can be defined to take values in $H^1(\mathbb{Z}[\frac{1}{N}], \mathscr{T}(1))$ on the eigenspaces relevant for our application. (Here, there is a restriction on the character that can be removed if one takes Eisenstein parts.) For this purpose, we need that $H^1(\mathbb{Z}[\frac{1}{N}], \mathscr{T}(1))$ injects into its tensor product with $Q(\Lambda)$, so we show along the way that this cohomology group is Λ-torsion free.

In the construction of $z^\sharp$, the zeta elements arise from norm compatible sequences of Beilinson elements in $H^2(Y_1(Mp^r)_{/\mathbb{Z}[\frac{1}{N}]}, \mathbb{Z}_p(2))$, which is to say cup products of Siegel units g_u on $Y_1(Mp^r)_{/\mathbb{Z}[\frac{1}{N}]}$. In essence, the map takes a compatible sequence of Manin symbols $[u:v]$ to a sequence of cup products $g_u \cup g_v$. That this map is well-defined is seen via a regulator

computation. One might hope for a direct construction of such a map, as Weierstrass units provide solutions to the unit equation that can be used to produce relations on Beilinson elements (see for instance [Br]). One difficulty with doing this, which is also what leads to $z^\sharp$ not being defined integrally, is that the Siegel units only become true units after being raised to a power, or modified using an auxiliary integer c as above. This appears to necessitate working rationally, or at least restricting to a map which takes sequences of symbols $_{c,d}[u : v]$ to sequences of Beilinson elements $_c g_u \cup _d g_v$. This causes further problems with performing a direct construction, as it is less clear what relations the latter Beilinson elements should satisfy. On the other hand, the fact that (c, d)-symbols generate homology can be used to show that the map $z^\sharp$ is indeed defined integrally on homology itself, the regulator computation being immune to such issues.

The derivation of Theorem 1.2.1 from the integrality of $z^\sharp$ will be explained in the paper [Sh2], which attempts to refine of the method of [FK]. The survey paper [FKS] also contains an exposition of the conjecture of [Sh1] and the method of [FK].

2   Generation by symbols

We provide abstract definitions of spaces of modular symbols in Definitions 2.1.1 and 2.1.2. These are meant to model relative homology groups of modular curves, along with their quotients. That is, the relative homology groups have well-known presentations as modules over an algebra of diamond operators, with Manin symbols providing the generators. We define a space of modular symbols to be a module generated by symbols with the same indexing set as the Manin symbols and satisfying at least the same relations. We then formally define (c, d)-symbols in Definition 2.1.3 using our Manin-type generators. We consider the question of generation by (c, d)-symbols on individual primitive eigenspaces for action of the diamond-type operators. Our main result, Theorem 2.1.6, describes exactly how close the (c, d)-symbols come to generating these eigenspaces.

To prove the theorem, we define eigensymbols as sums of the Manin-type symbols. Their properties are studied in Section 2.2. One advantage of working with eigenspaces is that the

(c, d)-versions of these eigensymbols are multiples of the corresponding unmodified eigensymbols, most of these multiples being by units, reducing the problem to a check that a relative few symbols are contained in the span of the (c, d)-symbols. The proof of the result is contained in Section 2.3.

For our applications in Section 3, we are particularly interested in the generation by (c, d)-symbols of quotients of relative homology groups on which elements of Eisenstein ideals act trivially. For this purpose, we artificially define Hecke-type operators in Section 2.4 that operate on the Manin-type symbols in the same manner that (adjoint) Hecke operators act on Manin symbols. We restrict our definitions to what we actually require, which is to say that we only consider operators U_ℓ and T_2, as they suffice to obtain generation in the remaining primitive eigenspaces in Theorem 2.4.5 and Proposition 2.4.7.

2.1 The result

Let p be an odd prime and M a positive integer with $p \nmid M \varphi(M)$. Set $N = M$ or Mp (and suppose $N > 1$). Let $\Delta = (\mathbb{Z}/N\mathbb{Z})^\times / \langle -1 \rangle$. For $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, let $\langle a \rangle$ denote the group element in $\mathbb{Z}_p[\Delta]$ corresponding to a.

Definition 2.1.1. A *space of level N modular symbols* is a $\mathbb{Z}_p[\Delta]$-module $\tilde{H}$ spanned by symbols $[u : v]$ for pairs of $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u, v) = (1)$ that satisfy relations

$$[u : v] = [-u : -v] = -[-v : u], \tag{2.1}$$

as well as

$$[u : v] = [u : u + v] + [u + v : v], \tag{2.2}$$

and, for every $a \in (\mathbb{Z}/N\mathbb{Z})^\times$,

$$\langle a \rangle [u : v] = [a u : a v]. \tag{2.3}$$

Definition 2.1.2. A *space of level N cuspidal-at-zero modular symbols* is a $\mathbb{Z}_p[\Delta]$-module H spanned by symbols $[u : v]$ for pairs of nonzero $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u, v) = (1)$ that satisfy relations (2.1), (2.2) for $u \neq -v$, and (2.3).

Every space of level N modular symbols has a subspace of a cuspidal-at-zero symbols. Moreover, every space of level N cuspidal-at-zero symbols is also, rather artificially, a space of level N modular symbols in which $[u : 0] = 0$ for every nonzero $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, as the reader can easily check. Let us fix a space H of level N modular symbols (which may or may not be cuspidal at zero in the sense just described).

5

Definition 2.1.3. For integers c and d greater than 1 and prime to $6N$, the (c, d)-*symbol* for the pair (u, v) is defined as

$$_{c,d}[u : v] = c^2 d^2 [u : v] - c^2 [u : d v] - d^2 [c u : v] + [c u : d v].$$

Let C denote the $\mathbb{Z}_p$-span of all (c, d)-symbols as we vary c and d, which is a $\mathbb{Z}_p[\Delta]$-submodule of H. Our goal is to compare C with H on primitive parts for the action of $(\mathbb{Z}/M\mathbb{Z})^\times$. To make this comparison, we work with individual Δ-eigenspaces for p-adic characters.

So, fix a p-adic character $\theta \colon \Delta \to \mathbb{C}_p^\times$. As before, let $\mathcal{O}_\theta$ denote the ring generated over $\mathbb{Z}_p$ by the values of θ, and now let $\mathcal{O} = \mathbb{Z}_p[\mu_{\varphi(N)}]$, which contains $\mathcal{O}_\theta$. Set $X_N = \mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^\times, \mathcal{O}^\times)$. Given an element of X_N denoted by χ, we will consistently use ψ to denote $\theta \chi^{-1}$.

We have the following two types of eigenspaces. First, for a $\mathbb{Z}_p[\Delta]$-module D, let

$$D^{(\theta)} = D \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}_\theta,$$

where $\mathbb{Z}_p[\Delta] \to \mathcal{O}_\theta$ is induced by θ. Second, let e_θ denote the idempotent

$$e_\theta = \frac{1}{\varphi(N)} \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta^{-1}(a)\langle a \rangle \in \mathcal{O}_\theta[(\mathbb{Z}/N\mathbb{Z})^\times].$$

We then set

$$D^\theta = e_\theta(D \otimes_{\mathbb{Z}_p} \mathcal{O}).$$

Note that $D^\theta \cong D^{(\theta)} \otimes_{\mathcal{O}_\theta} \mathcal{O}$. The advantage of working with eigenspaces D^θ is in the following definition of eigensymbols, the properties of which will be studied in the next subsection.

Definition 2.1.4. For relatively prime divisors g and h of N and $\chi \in X_N$, the *eigensymbol* $\alpha_{\chi,\psi}^{g,h} \in H^\theta$ is defined as

$$\alpha_{\chi,\psi}^{g,h} = \frac{1}{\varphi(N)^2} \sum_{a,b \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(a)\psi^{-1}(b)[g a : h b].$$

The (c, d)-*eigensymbol* $_{c,d}\alpha_{\chi,\psi}^{g,h}$ is defined by the same formula after replacing $[g a : h b]$ by $_{c,d}[g a : h b]$. We set $\alpha_{\chi,\psi} = \alpha_{\chi,\psi}^{1,1}$ and $_{c,d}\alpha_{\chi,\psi} = {}_{c,d}\alpha_{\chi,\psi}^{1,1}$.

Remark 2.1.5. By convention, if H is cuspidal at zero, then the symbols $\alpha_{\chi,\psi}^{N,1}$ with $\chi \in X_N$ are all zero.

Let $\omega \colon (\mathbb{Z}/M p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ denote the Teichmüller character (factoring through $(\mathbb{Z}/p\mathbb{Z})^\times$). The following is the main result of this section.

Theorem 2.1.6.

a. *If $p \geq 5$ and $\theta \omega^{-2}$ has conductor N, then $H^\theta = C^\theta$.*

b. *If $N = Mp$ with $p \geq 5$, and $\theta \omega^{-2}$ has conductor $M > 1$, then $H^\theta = C^\theta + \mathcal{O}\alpha^{1,p}_{\omega^2, \theta\omega^{-2}}$.*

c. *If $N = Mp$ with $p = 3$, and θ has conductor N, then $H^\theta = C^\theta + \mathcal{O}\alpha_{1,\theta} + \mathcal{O}\alpha^{N,1}_{1,\theta}$.*

2.2 Eigensymbols

In this subsection, we study the eigensymbols $\alpha^{g,h}_{\chi,\psi}$, starting with the following remarks.

Remark 2.2.1. We have $\alpha^{g,h}_{\chi,\psi} = -\chi(-1)\alpha^{h,g}_{\psi,\chi}$.

Remark 2.2.2. We have

$$\alpha^{g,h}_{\chi,\psi} = e_\theta \cdot \frac{1}{\varphi(N)} \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(a)[ga:h].$$

For $\chi \in X_N$, we let f_χ denote its conductor. We will also view such a χ as a primitive Dirichlet character of modulus f_χ. Note that if 2 divides f_χ, then so does 4. For a divisor D of N, set $Q_D = \frac{N}{D}$.

Lemma 2.2.3. *The element $\alpha^{g,h}_{\chi,\psi}$ is zero unless f_χ divides Q_g and f_ψ divides Q_h.*

Proof. For $u, v \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have

$$\frac{1}{\varphi(N)^2} \sum_{a,b \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(a)\psi^{-1}(b)[gau:hbv] = \chi(u)\psi(v)\alpha^{g,h}_{\chi,\psi}.$$

The right-hand side depends exactly (i.e., modulo no smaller integers) on the image of u in $(\mathbb{Z}/f_\chi\mathbb{Z})^\times$ and the image of v in $(\mathbb{Z}/f_\psi\mathbb{Z})^\times$. Since the left-hand side depends only on u modulo Q_g and v modulo Q_h, the eigensymbol $\alpha^{g,h}_{\chi,\psi}$ can only be nonzero if $f_\chi \mid Q_g$ and $f_\psi \mid Q_h$. $\qquad\square$

Lemma 2.2.4. *If $u, v \in (\mathbb{Z}/N\mathbb{Z})^\times$ and g and h are relatively prime divisors of N, then we have*

$$e_\theta[gu:hv] = \sum_{\chi \in X_N} \chi(u)\psi(v)\alpha^{g,h}_{\chi,\psi}.$$

Proof. We have the following equalities:

$$\sum_{\chi \in X_N} \chi(u)\psi(v)\alpha_{\chi,\psi}^{g,h} = \frac{1}{\varphi(N)} e_\theta \sum_{\chi \in X_N} \chi(uv^{-1})\theta(v) \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(c^{-1})[cg:h]$$

$$= \frac{1}{\varphi(N)} e_\theta \sum_{\chi \in X_N} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \theta(v)\chi(c^{-1})[cguv^{-1}:h]$$

$$= \frac{1}{\varphi(N)} e_\theta \theta(v)\langle v \rangle^{-1} \sum_{c \in (\mathbb{Z}/N\mathbb{Z})^\times} \sum_{\chi \in X_N} \chi(c^{-1})[cgu:hv]$$

$$= \frac{1}{\varphi(N)} e_\theta \varphi(N)[gu:hv] = e_\theta[gu:hv],$$

where in the second to last step we have used that $e_\theta\langle v \rangle = \theta(v)$ and that $\sum_{\chi \in X_N} \chi(c^{-1}) = 0$ unless $c = 1$. $\qquad\square$

Corollary 2.2.5. *The elements* $\alpha_{\chi,\psi}^{g,h}$ *for* $\chi \in X_N$ *and relatively prime divisors* g *and* h *of* N *generate* H^θ *as an* $\mathcal{O}$*-module.*

Similarly, C^θ is spanned by the $_{c,d}\alpha_{\chi,\psi}^{g,h}$ as c, d, χ, g, and h vary over the relevant sets. Moreover, note that

$$_{c,d}\alpha_{\chi,\psi}^{g,h} = (c^2 - \chi(c))(d^2 - \psi(d))\alpha_{\chi,\psi}^{g,h}. \tag{2.4}$$

Remark 2.2.6. For $\chi \in X_N$ with $\chi \neq \omega^2$ and $\psi \neq \omega^2$, we can choose c, d prime to $6N$ such that $\chi(c) \not\equiv c^2 \bmod p$ and $\psi(d) \not\equiv d^2 \bmod p$. By (2.4), it follows that $\alpha_{\chi,\psi}^{g,h}$ is a unit multiple of the resulting $_{c,d}\alpha_{\chi,\psi}^{g,h}$.

2.3   Proof of generation

In this subsection, we prove Theorem 2.1.6. Let us outline our strategy. First, placing ourselves in the setting of the theorem for an odd prime p, we suppose in this subsection that $f = f_{\theta\omega^{-2}}$ is divisible by M (so is M or Mp), which forces M to be odd or divisible by 4. Moreover, if $p = 3$, we suppose that $f = Mp$. Either $2 \nmid f$ or $4 \mid f$, and in that θ is even, $f \neq 3, 4$. For brevity, for relatively prime divisors g and h of N, let us set

$$\beta_{g,h} = \alpha_{\omega^2,\theta\omega^{-2}}^{g,h}$$

and $\beta = \beta_{1,1} = \alpha_{\omega^2,\theta\omega^{-2}}$.

By Remark 2.2.6, we have that $\alpha_{\chi,\psi}^{g,h} \in C^\theta$ if $\chi \in X_N - \{\omega^2, \theta\omega^{-2}\}$. Let us use $A \subseteq C^\theta$ to denote the $\mathcal{O}$-span of all symbols $\alpha_{\chi,\psi}^{g,h}$ with $\chi \notin \{\omega^2, \theta\omega^{-2}\}$ and g and h relatively prime divisors of N. By Corollary 2.2.5, in order to prove Theorem 2.1.6, we need only see that each

$\alpha_{\chi,\psi}^{g,h}$ with $\chi \in \{\omega^2, \theta\,\omega^{-2}\}$ lies in A in case (i), in $A + \mathcal{O}\beta_{1,p}$ in case (ii), and in $A + \mathcal{O}\beta + \mathcal{O}\beta_{N,1}$ in case (iii).

If $N = M$ and $p \geq 5$, we have $\chi \notin \{\omega^2, \theta\,\omega^{-2}\}$ automatically since $\omega^2 \notin X_N$, so there is nothing more to show. (It is not much harder to show that, for $p \geq 5$, Theorem 2.1.6a holds for $N = M$ without the assumption $p \nmid \varphi(M)$ and without restriction on the conductor of θ.) So, suppose from now on that $N = Mp$. The proof of Theorem 2.1.6 is contained in the lemmas that follow.

Lemma 2.3.1. *Let g and h be relatively prime divisors of N. If $p \nmid g$, then we have $\beta_{g,h} = 0$ unless $h = 1$, or $f = M$ and $h = p$. If $p \geq 5$ and $p \mid g$, then $\beta_{g,h} = 0$.*

Proof. This is a a direct corollary of Lemma 2.2.3. For the second statement, we note for $p \geq 5$ that $f_{\omega^2} = p$ does not divide Q_g. $\qquad\square$

We deal below with the remaining terms.

Lemma 2.3.2. *Suppose that g and h are relatively prime divisors of N. Let $\delta = 1$ if N is odd or gh is even and $\delta = 2$ otherwise.*

    a. There exist $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $ag + bh = \delta$ in $\mathbb{Z}/N\mathbb{Z}$.

    b. Let $\rho \in X_N$ be nontrivial. If $g \neq N$ and $h = \delta = 1$, then the numbers a and b of the first part can be chosen so that $\rho(b) \neq 1$ unless $f_\rho = 6\gcd(f_\rho, g)$ and $3 \nmid g$.

Proof. Part a is a simple application of the Chinese remainder theorem. We focus on part b. For its purposes, we can replace N by f_ρ and assume that ρ is primitive of conductor N.

Let ℓ be a prime dividing Q_g. Let $\epsilon = 0$ if ℓ is odd and $\epsilon = 1$ if $\ell = 2$, let $r \geq 1$ be such that ℓ^r exactly divides N, and let $s \geq 0$ be such that $\ell^{s+\epsilon}$ exactly divides g (noting for $\ell = 2$ that g is even as $\delta = h = 1$). Since ℓ divides Q_g, we have $r > s + \epsilon$. It suffices to see that either $\rho_\ell = \rho|_{(\mathbb{Z}/\ell^r\mathbb{Z})^\times}$ takes on at least two different values on allowed values of b modulo ℓ^r, or at least one nontrivial value in the case that Q_g is a prime power.

If $s \geq 1$, then primitivity of ρ implies that $\rho_\ell(b)$ can be any one of $\ell^{r-s-\epsilon-1}(\ell-1)$ different primitive $\ell^{r-s-\epsilon}$th roots of unity (noting that $b - 1$ is exactly divisible by $\ell^{s+\epsilon}$). This yields at least two values so long as ℓ is odd or $r > s + 2$. If $s = 0$, then b can be taken to be any prime-to-ℓ value modulo ℓ^r with $b \not\equiv 1 \bmod \ell^{1+\epsilon}$. Again by primitivity, ρ_ℓ will take on at least two values on such b if $\ell \geq 5$, $\ell = 3$ and $r \geq 2$, or $\ell = 2$ and $r \geq 3$. If $\ell = 3$ and $r = 1$, then $b \equiv 2 \bmod 3$ and $\rho_3(b) = -1$. For any $s \geq 0$, if $\ell = 2$ and $r = s+2$, we have $b \equiv 1 + 2^{s+1} \bmod 2^{s+2}$ and $\rho_2(b) = -1$. This covers all cases but the excluded case $Q_g = 6$ and $3 \nmid g$ (for which $\rho(b) = \rho_2(b)\rho_3(b) = 1$). $\qquad\square$

Given relatively prime divisors g and h of N, we may choose $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ with $ag + bh = \delta$ by first part of Lemma 2.3.2. By applying Lemma 2.2.4, the formula

$$[ga : hb] = [ga : \delta] + [\delta : hb]$$

provides the identity

$$\sum_{\chi \in X_N} \chi(a)\psi(b)\alpha_{\chi,\psi}^{g,h} = \sum_{\chi \in X_N} \chi(a)\alpha_{\chi,\psi}^{g,\delta} + \sum_{\chi \in X_N} \psi(b)\alpha_{\chi,\psi}^{\delta,h}. \tag{2.5}$$

There are at most six terms in (2.5) not in A, two from each sum. Using the antisymmetry of the eigensymbols for even characters, equation (2.5) yields

$$\omega^2(a)\theta\,\omega^{-2}(b)\beta_{g,h} - \omega^2(b)\theta\,\omega^{-2}(a)\beta_{h,g}$$
$$\equiv \omega^2(a)\beta_{g,\delta} - \theta\,\omega^{-2}(a)\beta_{\delta,g} + \theta\,\omega^{-2}(b)\beta_{\delta,h} - \omega^2(b)\beta_{h,\delta} \bmod A. \tag{2.6}$$

Lemma 2.3.3. *Suppose that $p \geq 5$. For every proper divisor g of N, we have $\beta_{g,1} \in A + \mathcal{O}\beta$.*

Proof. Set $B = A + \mathcal{O}\beta$. We may assume that $g > 1$, and by Lemma 2.3.1, that $p \nmid g$.

Suppose first that N is odd or g is even, in which case we may choose $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $ag + b = 1$ by Lemma 2.3.2a. By Lemma 2.3.1, we have $\beta_{1,g} = 0$. The last two terms of (2.6) are in B by definition. So, dividing out by $\omega^2(a)$, equation (2.6) reduces to

$$(\theta\,\omega^{-2}(b) - 1)\beta_{g,1} \in B.$$

If either $f \neq 6\gcd(f,g)$ or $3 \mid g$, we may apply Lemma 2.3.2b to choose a such that $b = 1 - ag$ satisfies $\theta\,\omega^{-2}(b) \neq 1$ to conclude that $\beta_{g,1} \in B$. In particular, we are done if N is odd.

Suppose, on the other hand, that g is even, $f = 6\gcd(f,g)$, and $3 \nmid g$. We again apply Lemma 2.3.2a to choose $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $ag + 3b = 1$. Again by Lemma 2.3.1, we have $\beta_{g,3} = \beta_{1,3} = 0$, as the facts that $3 \mid f$ and $M \mid f$ imply that $f \nmid \frac{N}{3}$. We also have $\beta_{3,g} = \beta_{1,g} = 0$. From (2.6) with $h = 3$, we therefore obtain

$$\omega^2(a)\beta_{g,1} - \omega^2(b)\beta_{3,1} \in A.$$

It thus suffices to show that $\beta_{3,1} \in B$ in this case, so to prove the result for $g = 3$ and N even.

We are reduced to the case that N is even and g is odd. Choose $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $ag + b = 2$, and consider (2.6) with $\delta = 2$. Lemma 2.2.3 tells us that $\beta_{1,2} = \beta_{g,2} = \beta_{1,g} = \beta_{2,g} = 0$, so this yields

$$\omega^2(a)\beta_{g,1} - \beta_{2,1} \in A.$$

Since $p \geq 5$, we have that ω^2 takes on at least two values on $a \not\equiv 2g^{-1} \bmod p$, so both $\beta_{g,1}$ and $\beta_{2,1}$ are in A. $\qquad\square$

10

Lemma 2.3.4.

    a. *Suppose that $p \geq 5$ and $f = M$. For every divisor g of M, we have $\beta_{g,p} - \omega^2(g)\beta_{1,p} \in A + \mathcal{O}\beta$.*

    b. *Suppose that $p = 3$ and $f = N$. For every proper divisor g of N, we have $\beta_{g,1} - \beta \in A$.*

Proof. Let $h = p$ in part a and $h = 1$ in part b. We may clearly suppose that $g > 1$. Choose $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ with $ag + bh = \delta$, with δ as in Lemma 2.3.2a. In part a, we have $\beta_{\delta,g} = \beta_{p,g} = \beta_{p,\delta} = 0$ by Lemma 2.3.1, so (2.6) yields

$$\omega^2(a)\theta\,\omega^{-2}(b)\beta_{g,p} \equiv \omega^2(a)\beta_{g,\delta} + \theta\,\omega^{-2}(b)\beta_{\delta,p} \bmod A.$$

If $\delta = 2$ (i.e., g is odd and N is even), we have $\beta_{g,\delta} = 0$ and $a \equiv 2g^{-1} \bmod p$, so this reduces to

$$\omega^2(2)\beta_{g,p} - \omega^2(g)\beta_{2,p} \in A,$$

which puts us back in the setting that $\delta = 1$. If $\delta = 1$, then $a \equiv g^{-1} \bmod p$, and since $\beta_{g,1} \in A + \mathcal{O}\beta$ by Lemma 2.3.3, we obtain that $\beta_{g,p} - \omega^2(g)\beta_{1,p} \in A + \mathcal{O}\beta$.

    For part b, we have $p = 3$ and $\omega^2 = 1$. The module H is trivial if $M = 1$, so we may take $M \geq 4$. By (2.6), we have

$$\theta(b)(\beta_{g,1} - \beta_{\delta,1}) \equiv \theta(a)(\beta_{1,g} - \beta_{\delta,g}) + (\beta_{g,\delta} - \beta_{1,\delta}) \bmod A.$$

If $\delta = 2$ (so g is odd and N is even), then the last two terms are zero. Since $g > 1$ and $f = N$ by assumption, the other two terms on the right are also zero, and we obtain $\beta_{g,1} - \beta_{2,1} \in A$. If $\delta = 1$ (so g is even or N is odd), we obtain $(\theta(b) - 1)(\beta_{g,1} - \beta) \in A$. We may choose b to be any unit which is 1 modulo g, and in particular so that $\theta(b) \neq 1$ since g properly divides $f = N$. $\qquad\square$

    Since we assumed that $f = N = Mp$ if $p = 3$, we are done in that case, and for $p \geq 5$, we are reduced to showing that $\beta \in A$ if $\theta \neq \omega^2$. We consider $M > 1$ and $M = 1$ separately.

Lemma 2.3.5. *If $p \geq 5$ and $M > 1$, then $\beta \in A$.*

Proof. Set $\epsilon = 1$ if N is odd and $\epsilon = 2$ if N is even. Using Lemma 2.3.2a with $g = \epsilon p$ and $h = 1$, choose $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ with $\epsilon pa + b = 1$. As $p \geq 5$, we have $\beta_{\epsilon p,1} = 0$ by Lemma 2.3.1, and (2.6) yields

$$\theta\,\omega^{-2}(a)(\omega^2(b) - 1)\beta_{1,\epsilon p} \equiv (\omega^2(b) - \theta\,\omega^{-2}(b))\beta \bmod A,$$

but note that $b \equiv 1 \bmod p$, so this simplifies to $(1 - \theta(b))\beta \in A$. By Lemma 2.3.2b, we may choose b with $\theta(b) \neq 1$ so long as $M \neq 12$.

If $M = 12$, instead choose $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ with $2a + b = 1$. We then have $b \equiv -1 \bmod 12$, and $12 \mid f$ forces $\theta|_{(\mathbb{Z}/12\mathbb{Z})^\times}(-1) = 1$. Let k be the positive even integer with $k \leq p-1$ such that $\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times} = \omega^k$. Equation (2.6) with $g = 2$ yields

$$\omega^2(a)(\omega^{k-2}(b)-1)\beta_{2,1} \equiv (\omega^{k-2}(b)-\omega^2(b))\beta \bmod A.$$

We then have $\beta \in A$ if there does not exist $w \in \mathbb{F}_p^\times$ such that

$$G(a) = a^2((1-2a)^{k-2}-1) - w((1-2a)^{k-2}-(1-2a)^2)$$

vanishes on all $a \in \mathbb{F}_p - \{0, \frac{1}{2}\}$. As G has degree $k \leq p-1$, we see that G cannot vanish on the the latter set unless $k = p-1$. For $k = p-1$, note that

$$G(a) = (1-2a)^{-2}(a^2(1-(1-2a)^2) - w(1-(1-2a)^4))$$

on $\mathbb{F}_p - \{0, \frac{1}{2}\}$. No polynomial of degree 4 in a can vanish on this set for $p > 5$. For $p = 5$ and $k = 4$, note that G is independent of w and $G(-1) = 3 \neq 0$. $\qquad\square$

Lemma 2.3.6. *Suppose that $M = 1$ and $\theta \neq \omega^2$. The element β is contained in the $\mathcal{O}$-span of the symbols $\alpha_{\chi,\psi}$ with $\chi \in X_N - \{\omega^2, \theta\omega^{-2}\}$. In particular, $\beta \in A$.*

Proof. Suppose that a, b, and $a + b$ are all in $(\mathbb{Z}/p\mathbb{Z})^\times$. From (2.5) with $g = h = 1$, we have

$$\sum_{\chi \in X_N} (\chi(a)\psi(b) - \chi(a)\psi(a+b) - \chi(a+b)\psi(b))\alpha_{\chi,\psi} = 0. \tag{2.7}$$

If $\chi \neq \psi$, the difference of the coefficients of $\alpha_{\chi,\psi}$ and $\alpha_{\psi,\chi}$ on the left of (2.7) is

$$(\chi(a)-\chi(a+b))(\psi(b)-\psi(a+b)) - (\chi(b)-\chi(a+b))(\psi(a)-\psi(a+b)).$$

It suffices to show that this is nonzero in the case $\chi = \omega^2$ (as ω^2 is even, noting that $\alpha_{\omega^2,\omega^2} = 0$) for some choice of a and b, as we can then write β as a sum of the $\alpha_{\chi,\psi}$ with $\chi \notin \{\omega^2, \theta\omega^{-2}\}$. It is sufficient to consider the case $b = 1$, as is seen by dividing (2.7) by $\chi(b)\psi(b)$, so we suppose this from now on.

Now write $\theta = \omega^k$ for an even $4 \leq k \leq p-1$, noting that $k \neq 2$ by assumption. Our difference is then

$$F(a) = (a^2 - (a+1)^2)(1-(a+1)^{k-2}) - (1-(a+1)^2)(a^{k-2}-(a+1)^{k-2})$$

modulo p. The polynomial $F(a)$ has degree at most k and is nonzero as $k \neq 2$ (e.g., note that $F'(0) = k$), so it cannot vanish identically on $\mathbb{F}_p - \{0, -1\}$ unless $k = p-1$. If $k = p-1$, we can

reduce our polynomial on $\mathbb{F}_p - \{0, -1\}$ to

$$(a^2 - (a+1)^2)(1 - (a+1)^{p-3}) - (1 - (a+1)^2)(a^{p-3} - (a+1)^{p-3})$$
$$= a^{-2}(a+1)^{-2}(a^2(a^2 - (a+1)^2)((a+1)^2 - 1) - (1 - (a+1)^2)((a+1)^2 - a^2))$$
$$= -a^{-1}(a+1)^{-1}(a+2)(2a+1)(a-1)$$

which is nonzero at $a = 2$ for $p \geq 7$. Moreover, if $p = 5$, then $\beta = \alpha_{\omega^2, \omega^2} = 0$. $\qquad\square$

2.4 Hecke-type operators

In this subsection, we take a minimalistic approach to "Hecke operators" on H, introducing them only as needed to prove generation, with a view towards ordinary and Eisenstein components of homology, on which our so-called Hecke operators will be actual Hecke operators. For the purpose of our application, it is necessary to distinguish spaces that are cuspidal at zero, so we let H either be a space of level N modular symbols or a space of cuspidal-at-zero modular symbols. We suppose (without loss of generality) in this subsection that $N = Mp$.

The relationship between the following definition, and that of a T_2-operator below, and actual Hecke operators will be explained by the proof of Theorem 1.1.2.

Definition 2.4.1. For a prime ℓ dividing N, a U_ℓ-*operator* on H is a $\mathbb{Z}_p[\Delta]$-linear endomorphism $U_\ell \colon H \to H$ satisfying

$$U_\ell[\ell u : v] = \sum_{k=0}^{\ell-1} [u + k \tfrac{N}{\ell} : v]. \tag{2.8}$$

for all $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(\ell u, v) = (1)$, and $\ell u \neq 0$ if H is cuspidal at zero. We say that H *has a* U_ℓ-*operator* if there exists a U_ℓ-operator on H.

Let ℓ denote a prime dividing N, and let $s \geq 1$ denote the ℓ-adic valuation of N. As before, g and h denote relatively prime divisors of N.

Proposition 2.4.2. *Suppose that H has a U_ℓ-operator and that g and h are not divisible by ℓ. Let $t \leq s$ be a positive integer such that f_χ divides $\frac{N}{\ell^t}$. If $t < s$, then*

$$U_\ell \alpha_{\chi, \psi}^{\ell^t g, h} = \ell \alpha_{\chi, \psi}^{\ell^{t-1} g, h},$$

and if $t = s$ (and $\ell^s g \neq N$ if H is cuspidal at zero), then

$$(U_\ell - \chi^{-1}(\ell)) \alpha_{\chi, \psi}^{\ell^s g, h} = (\ell - 1) \alpha_{\chi, \psi}^{\ell^{s-1} g, h}.$$

13

Proof. By Lemma 2.2.3, we may suppose that f_χ divides $Q_{\ell^t g} = \frac{N}{\ell^t g}$. We have

$$U_\ell \alpha_{\chi,\psi}^{\ell^t g, h} = \sum_{k=0}^{\ell-1} e_\theta \cdot \frac{1}{\varphi(N)} \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(a)[\ell^{t-1} g a + k \tfrac{N}{\ell} : h]. \tag{2.9}$$

Note that

$$\ell^{t-1} g a + k \frac{N}{\ell} = \ell^{t-1} g \left(a + k \frac{N}{\ell^t g} \right),$$

and $a + kQ_{\ell^t g}$ is prime to Q_g except in the case $t = s$ for the unique value of k such that ℓ divides $a + kQ_{\ell^s g}$. If $t < s$, we see that the $a + kQ_{\ell^t g}$ for a fixed k run over all units in $\mathbb{Z}/Q_{\ell^{t-1}g}\mathbb{Z}$ with multiplicity $\ell^{t-1} g$ each. As $f_\chi \mid Q_{\ell^t g}$, we therefore have

$$\sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(a)[\ell^{t-1} g a + k\tfrac{N}{\ell} : h] = \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(a)[\ell^{t-1} g a : h],$$

proving the first statement.

For $t = s$, the $a + kQ_{\ell^s g}$ for all k and a such that $\ell \nmid (a + kQ_{\ell^s g})$ run over $(\mathbb{Z}/Q_{\ell^{s-1}g}\mathbb{Z})^\times$ with multiplicity $(\ell-1)\ell^{s-1} g$, similarly providing the $(\ell-1)\alpha_{\chi,\psi}^{\ell^{s-1}g, h}$ in the second statement. On the other hand, the $\ell^{-1}(a + kQ_{\ell^t g})$ for pairs (k, a) with $\ell \mid (a + kQ_{\ell^s t})$ run over $(\mathbb{Z}/Q_{\ell^s g}\mathbb{Z})^\times$ with constant multiplicity $\ell^s g$. If $a' \in (\mathbb{Z}/N\mathbb{Z})^\times$ is such that $a' \equiv \frac{a+kQ_{\ell^s g}}{\ell} \bmod Q_{\ell^s g}$, then $\chi(\ell a') = \chi(a)$, so the sum of the corresponding terms is the desired value $\chi(\ell)^{-1}\alpha_{\chi,\psi}^{\ell^s g, h}$. $\qquad \square$

In the following nearly immediate corollaries, if H is cuspidal at zero, we implicitly exclude those elements $\alpha_{\chi,\psi}^{g,h}$ that occur with either g or h equal to N.

Corollary 2.4.3. *Suppose that H has a U_ℓ-operator that acts on H^θ as multiplication by an element of $\mathcal{O}^\times$. Then H^θ is the $\mathcal{O}$-span of the elements of the form $\alpha_{\chi,\psi}^{g,h}$ and $\alpha_{\chi,\psi}^{\ell^s g, h}$ with $\ell \nmid g h$.*

Noting that $\ell - 1 \in \mathbb{Z}_p^\times$, and that if $\chi(\ell) \neq 1$, then $1 - \chi^{-1}(\ell)$ is a unit, we have the following.

Corollary 2.4.4. *Suppose that H has a trivial U_ℓ-operator (i.e., $U_\ell - 1$ acts as zero on H). Then H^θ is the $\mathcal{O}$-span of the elements of the form $\alpha_{\chi,\psi}^{g,h}$ with $\ell \nmid g h$ and $\alpha_{\chi,\psi}^{\ell^s g, h}$ with $\ell \nmid g h$ and $\chi(\ell) = 1$. Moreover, if $\ell \nmid f_\chi g h$ and $\chi(\ell) = 1$, then $\alpha_{\chi,\psi}^{g,h} = 0$ (so long as $\ell^s g \neq N$ if H is cuspidal at zero).*

We may now prove the main theorem of this section.

Theorem 2.4.5. *Suppose that $f = f_{\theta\omega^{-2}}$ is divisible by M. If any of the following conditions hold, then $H^\theta = C^\theta$:*

    i. $p \geq 5$ and $f = N$,

ii. $p \geq 5$, $f = M$, $\theta|_{(\mathbb{Z}/M\mathbb{Z})^\times}(p) \neq 1$, and there is a trivial U_p-operator on H,

iii. for some prime ℓ dividing M, there is a trivial U_ℓ-operator on H (and $f = N$ and H is cuspidal at zero if $p = 3$).

Proof. By Theorem 2.1.6, in the case $p \geq 5$ (resp., $p = 3$), we need only show that $\beta_{1,p} \in A$ if $f = M$ (resp., $\beta \in A$). In particular, we already have (i). If $\theta|_{(\mathbb{Z}/M\mathbb{Z})^\times}(p) \neq 1$ and U_p acts trivially, we have $\beta_{1,p} \in A + \mathcal{O}\beta$ by Proposition 2.4.2 for U_p. Since $\beta \in A$ by Lemmas 2.3.5 and 2.3.6, we have (ii).

If $p \geq 5$ and $f = M$ (resp., $p = 3$ and $f = N$), then for $h = p$ (resp., $h = 1$), Lemma 2.3.4 tells us that

$$\omega(\ell)^{-2}\beta_{\ell,h} - \beta_{1,h} \in A$$

for any prime ℓ dividing M. If ℓ^2 divides M (resp., ℓ exactly divides M and $\ell \not\equiv -1 \bmod p$) and U_ℓ acts trivially, then Proposition 2.4.2 yields that $w\beta_{1,h} \in A$, where $w \equiv \frac{1-\ell}{\ell} \bmod p$ (resp., $w \equiv \frac{-\ell}{\ell+1} \bmod p$). Finally, if $\ell \equiv -1 \bmod p$ exactly divides M, then since $\omega^2(\ell) = 1$ and U_ℓ acts trivially, Corollary 2.4.4 tells us that $\beta_{1,h} = 0$. $\square$

We can treat cuspidal-at-zero symbols in the case $M = 1$ and $\theta = \omega^2$ by using a T_2-operator.

Definition 2.4.6. Suppose that N is odd. A T_2-*operator* on H is a $\mathbb{Z}_p[\Delta]$-linear endomorphism of H such that

$$\langle 2 \rangle T_2[u:v] = [2u:v] + [2u:u+v] + [u+v:2v] + [u:2v] \tag{2.10}$$

for all $u, v \in \mathbb{Z}/N\mathbb{Z}$ with $(u,v) = (1)$ (and u, v, and $u+v$ nonzero if H is cuspidal at zero).

Proposition 2.4.7. *Suppose that $M = 1$, that $\theta = \omega^2$, and that H is cuspidal at zero. If T_2 acts as $1 + 2\omega^{-2}(2)$ on H^{ω^2}, then $H^{\omega^2} = C^{\omega^2}$.*

Proof. Since H is cuspidal at zero, it clearly suffices show that $\beta \in A$. Let $a, b \in (\mathbb{Z}/N\mathbb{Z})^\times$ be such that $a + b = 1$. Note that $e_{\omega^2}(\langle 2 \rangle T_2[a:b] - 2[a:b] - [2a:2b]) = 0$ by our assumption on T_2. Applying Lemma 2.2.4 to (2.10) with $u = a$ and $v = b$, we therefore have that

$$\sum_{\chi \in X_N} (2\chi(a)\psi(b) + \chi(2a)\psi(2b) - \chi(2a)\psi(b) - \chi(2a) - \psi(2b) - \chi(a)\psi(2b))\alpha_{\chi,\psi} = 0,$$

where as before ψ is taken to be $\theta\chi^{-1}$. Since $\theta = \omega^2$, we need only see that the difference

$$(\omega^2(a) - \omega^2(2a) - 1) - (\omega^2(b) - \omega^2(2b) - 1) \equiv 3((1-a)^2 - a^2) \bmod p$$

of the coefficients of $\alpha_{\omega^2,1} = \beta$ and $\alpha_{1,\omega^2} = -\beta$ can be nonzero modulo p. For $p \geq 5$, this occurs for $a = -1$, and for $p = 3$, the group H is trivial. $\square$

Remark 2.4.8. The equality in Proposition 2.4.7 does not always hold without the cuspidal-at-zero condition, even on "Eisenstein quotients" involving conditions for all Hecke operators, rather than just T_2.

3   Application to modular curves

In Section 3.1, we first apply the abstract study of Section 2 to prove Theorems 1.1.1 and 1.1.2 on the generation of relative homology groups of modular curves and their Eisenstein parts by the modifications of Manin symbols that we have termed (c,d)-symbols. An application of Nakayama's lemma provides analogous results, Propositions 3.1.5 and 3.1.6, for inverse limits of the ordinary parts and Eisenstein components of these relative homology groups up a tower of modular curves of increasing p-power dividing the level.

   As outlined in the introduction, we apply these generation results in Section 3.2 to prove the integrality of two types of maps taking compatible systems of Manin symbols to compatible systems of zeta elements: see Theorems 3.2.9 and 3.2.11. These maps, first defined in [FK], a priori only take values in a tensor product of a cohomology group with the quotient field of an Iwasawa algebra. However, their values on compatible systems of (c,d)-symbols lie in the (integral) image of the actual cohomology group in the (rational) tensor product. By the generation results of Section 2, the theorems are then reduced to the torsion-freeness of the Iwasawa modules that are the cohomology groups in question, and this is the content of Lemmas 3.2.8 and 3.2.10.

3.1   Homology of modular curves

We explain how the results of Section 2 apply to the homology groups of modular curves. For this, fix an odd prime p, an integer M with $p \nmid M\varphi(M)$, and $r \geq 1$. Set $N_r = Mp^r$, and suppose additionally that $N_r \geq 4$. We set $N = N_1$. Let $G_r = (\mathbb{Z}/N_r\mathbb{Z})^\times/\langle -1\rangle$, let $\Delta = G_1$, and let $\Gamma_r = \ker(G_r \to \Delta)$. Set $\mathcal{O} = \mathbb{Z}_p[\mu_{\varphi(M)}]$.

   Let $C_1(N_r) = \Gamma_1(Np^r)\backslash\mathbb{P}^1(\mathbb{Q})$ denote the set of cusps in $X_1(N_r)$. The relative homology group

$$\tilde{H}_r = H_1(X_1(N_r), C_1(N_r), \mathbb{Z})$$

is generated by the classes $\{x \to y\}_r$ of images of geodesics in the extended upper half-plane from a cusp $x \in \mathbb{P}^1(\mathbb{Q})$ to a cusp $y \in \mathbb{P}^1(\mathbb{Q})$.

Definition 3.1.1. For $u, v \in \mathbb{Z}/N_r\mathbb{Z}$ with $(u,v) = (1)$, choose $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $(u,v) =$

$(c,d) \bmod N_r \mathbb{Z}^2$. The *Manin symbol* of level N_r attached to the pair (u,v) is

$$[u:v]_r = \left\{ \frac{-d}{bN_r} \to \frac{-c}{aN_r} \right\}_r.$$

Remark 3.1.2. Our "Manin symbols" are actually Manin's after application of the Atkin-Lehner involution of level N_r. As a result, we have

$$\langle a \rangle_r^{-1} [u:v]_r = [au:av]_r$$

for $a \in G_r$, where $\langle a \rangle_r$ denotes the diamond operator acting on $\tilde{H}_r$.

It is well-known that $\tilde{H}_r$ is a space of modular symbols of level N_r in the sense previously defined. In fact, we have the following, which follows easily from [Ma, Theorem 1.9].

Theorem 3.1.3 (Manin)**.** *The space $\tilde{H}_r$ has a presentation as a $\mathbb{Z}_p[G_r]$-module on the generators $[u:v]_r$ with relations as in* (2.1), (2.2), *and* (2.3), *where $\langle a \rangle$ in* (2.3) *for $a \in (\mathbb{Z}/N_r\mathbb{Z})^\times$ is taken to be the inverse diamond operator $\langle a \rangle_r^{-1}$ acting on $\tilde{H}_r$.*

Let

$$H_r = H_1(X_1(N_r), C_1^0(N_r), \mathbb{Z}_p),$$

where $C_1^0(N_r) \subset C_1(N_r)$ is the subset of cusps not lying over the zero cusp of the modular curve $X_0(N_r)$. This is the space of cuspidal-at-zero symbols in $\tilde{H}_r$. Let $\tilde{C}_r$ and C_r denote the $\mathbb{Z}_p$-submodules of $\tilde{H}_r$ and H_r, respectively, generated by (c,d)-symbols $_{c,d}[u:v]_r$ as we vary c and d (with $u,v \neq 0$ for H_r).

Fix a p-adic character θ of Δ as before. Theorem 2.1.6 applies directly to H_1 and $\tilde{H}_1$ for the symbols $[u:v]_1$, yielding Theorem 1.1.1 and its analogue for H_1. The proof of Theorem 1.1.2 is only slightly more involved.

Proof of Theorem 1.1.2 and Remark 1.1.3. The Hecke operators U_ℓ for $\ell \mid N$ (resp., T_2 for N odd) on $\tilde{H}_1$ satisfy equation (2.8) (resp., (2.10)) by [Sh1, p. 264] (resp., [Me, Prop. 20], after taking into account the modification to said formula incurred by Remark 3.1.2). Let I_1 be the Eisenstein ideal of the introduction, generated by by $U_\ell - 1$ for $\ell \mid N$ and $T_\ell - 1 - \ell\langle \ell \rangle$ for $\ell \nmid N$. To prove Theorem 1.1.2, we may take $\tilde{H}_1/I_1\tilde{H}_1$ as H in Theorem 2.4.5. For Remark 1.1.3, we may take $H_1/I_1 H_1$ as H in Theorem 2.4.5 and in Proposition 2.4.7 if $\theta = \omega^2$. Consequently, $H^{(\theta)}$ is generated by the images of the $_{c,d}[u:v]_1$. Applying Nakayama's lemma, we obtain Theorem 1.1.2 for $\tilde{H}_1$, and its analogue for H_1. $\qquad\square$

Let $G = \varprojlim_r G_r$ and $\Gamma = \varprojlim_r \Gamma_r$, and set $\tilde{\Lambda} = \mathbb{Z}_p[\![G]\!]$ and $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$. Let us use ord to denote the ordinary part of a Hecke algebra or module, the maximal direct summand on

which (a compatible system of Hecke operators) U_p acts invertibly. We will identify elements with their projections to ordinary parts (via Hida's ordinary idempotent). We then have Λ-modules $\mathcal{H} = \varprojlim_r H_r^{\text{ord}}$, $\tilde{\mathcal{H}} = \varprojlim_r \tilde{H}_r^{\text{ord}}$, $\mathcal{C} = \varprojlim_r C_r^{\text{ord}}$, and $\tilde{\mathcal{C}} = \varprojlim_r \tilde{C}_r^{\text{ord}}$, with $a \in \Gamma$ acting as the inverse diamond operator $\langle a \rangle^{-1}$. As in [Sh1, Lemma 3.2], we have the compatibility of Manin symbols in the following definition.

Definition 3.1.4. For integers u and v with $p \nmid v$ and $(u, v, M) = 1$, let

$$(u : v) = ([p^{r-1} u : v]_r)_r \in \tilde{\mathcal{H}},$$

and given integers $c, d > 1$ prime to $6N$, set

$${}_{c,d}(u : v) = c^2 d^2 (u : v) - d^2 (c u : v) - c^2 (u : d v) + (c u : d v) \in \tilde{\mathcal{H}}.$$

As a $\tilde{\Lambda}$-module, $\tilde{\mathcal{H}}$ is generated by the elements $(u : v)$ for $u, v \in \mathbb{Z}$ as above [FK, Lemma 3.2.5]. The proof is simple: the image of $(u : v)$ in $\tilde{H}_1^{\text{ord}}$ is the ordinary projection of $[u : v]_1$. Since $\tilde{H}_1^{\text{ord}}$ is isomorphic by Hida theory to the group of Γ-coinvariants of $\tilde{\mathcal{H}}$ (see [Oh2, Theorem 1.4.3]), we may apply Nakayama's lemma.

The $\tilde{\Lambda}$-submodule $\mathcal{H}$ of $\tilde{\mathcal{H}}$ is generated by those elements $(u : v)$ with $N \nmid u$. We let $\tilde{\mathcal{C}}$ denote the $\tilde{\Lambda}$-submodule of $\tilde{\mathcal{H}}$ generated by all (c, d)-symbols ${}_{c,d}(u : v)$, and we let $\mathcal{C}$ be the $\tilde{\Lambda}$-submodule generated by those with $N \nmid u$.

We let $\Lambda_\theta = \tilde{\Lambda}^{(\theta)} \cong \mathcal{O}_\theta[\![\Gamma]\!]$. We again set $f = f_{\theta \omega^{-2}}$. We take $p \geq 5$ in the following two results for simplicity of presentation. They are immediate consequences of Theorems 1.1.1 and 1.1.2 (and their cuspidal-at-zero analogues) upon application of Nakayama's lemma.

Proposition 3.1.5. *If $M \mid f$ and $\theta \neq \omega^2$, then*

$$\mathcal{H}^{(\theta)} = \mathcal{C}^{(\theta)} + \Lambda_\theta e_\theta(p : 1) \quad \text{and} \quad \tilde{\mathcal{H}}^{(\theta)} = \tilde{\mathcal{C}}^{(\theta)} + \Lambda_\theta e_\theta(p : 1).$$

Moreover, if $f = N$, then $\mathcal{H}^{(\theta)} = \mathcal{C}^{(\theta)}$ and $\tilde{\mathcal{H}}^{(\theta)} = \tilde{\mathcal{C}}^{(\theta)}$.

Let $\mathfrak{H}$ denote Hida's ordinary Hecke algebra acting as $\tilde{\Lambda}$-linear endomorphisms of $\tilde{\mathcal{H}}$, and let $\mathfrak{h}$ denote the cuspidal Hecke algebra acting on $\mathcal{H}$. Note that $\mathfrak{H}^{(\theta)}$ is a free Λ_θ-module, again by Hida theory. Let I denote the Eisenstein ideal of $\mathfrak{H}$ (and its image in $\mathfrak{h}$) that is generated by $T_\ell - 1 - \ell \langle \ell \rangle$ for primes $\ell \nmid N$ and $U_\ell - 1$ for primes $\ell \mid N$. Let $\mathfrak{m}$ denote the unique maximal ideal of $\mathfrak{H}^{(\theta)}$ containing $I \mathfrak{H}^{(\theta)}$. We write the localization of $\mathfrak{H}^{(\theta)}$ at $\mathfrak{m}$ more briefly as $\mathfrak{H}_{\mathfrak{m}}$, and similarly for $\mathfrak{H}$-modules.

Proposition 3.1.6. *If $M \mid f$, then $\mathcal{H}_{\mathfrak{m}}$ is equal to $\mathcal{C}_{\mathfrak{m}}$. If $\theta \neq \omega^2$ as well, then $\tilde{\mathcal{H}}_{\mathfrak{m}}$ is equal to $\tilde{\mathcal{C}}_{\mathfrak{m}}$.*

3.2 Zeta elements

In this subsection, we consider the integrality of maps that take Manin symbols to zeta elements. These maps were defined rationally in [FK, Section 3]. We suppose that $p \geq 5$.

For $s \geq 0$, let $\mathbb{Z}_s$ denote the ring of integers of $\mathbb{Q}_s$, the maximal p-extension of $\mathbb{Q}$ in $\mathbb{Q}(\mu_{p^s})$, and let $\mathbb{Z}_\infty$ denote the ring of integers of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. Set

$$\mathscr{T}_r = H^1(X_1(N_r)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^{\mathrm{ord}} \quad \text{and} \quad \tilde{\mathscr{T}}_r = H^1(Y_1(N_r)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^{\mathrm{ord}},$$

and let $\mathscr{T}$ and $\tilde{\mathscr{T}}$ denote the corresponding inverse limits under trace maps. We let Hida's Hecke algebras $\mathfrak{h}$ and $\mathfrak{H}$ act on $\mathscr{T}$ and $\tilde{\mathscr{T}}$, respectively, via the adjoint actions of Hecke operators (and here, ordinary parts have been taken with respect to the adjoint action of U_p). For any compact $\mathbb{Z}_p[\![G_{\mathbb{Q}}]\!]$-module $\mathscr{A}$ that is unramified outside of N, set

$$H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \mathscr{A}) = \varprojlim_s H^1(\mathbb{Z}_s[\tfrac{1}{N}], \mathscr{A}).$$

Definition 3.2.1. For $r, s \geq 0$ and $u, v \in \mathbb{Z}/N_r\mathbb{Z}$ with $(u, v) = (1)$ (and $u, v \neq 0$ if $s = 0$) and $c, d > 1$ and prime to $6N$, we define $_{c,d}z_{r,s}(u : v)$ to be the image under the norm and Hochschild-Serre maps

$$H^2(Y(p^s, N_{r+s})_{/\mathbb{Z}[\frac{1}{N}]}, \mathbb{Z}_p(2)) \to H^2(Y_1(N_r)_{/\mathbb{Z}_s[\frac{1}{N}]}, \mathbb{Z}_p(2)) \xrightarrow{\mathrm{HS}} H^1(\mathbb{Z}_s[\tfrac{1}{N}], H^1(Y_1(N_r)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(2)))$$

of the cup product $_c g_{\frac{w}{p^s}, \frac{y}{N_{r+s}}} \cup {_d g_{\frac{x}{p^s}, \frac{z}{N_{r+s}}}}$ of Siegel units on $Y(p^s, N_{r+s})_{/\mathbb{Z}[\frac{1}{N}]}$, where $\left(\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $u = y \bmod N_r$ and $v = z \bmod N_r$.

Remark 3.2.2. In defining $_{c,d}z_{r,s}(u : v)$, we have taken corestriction from $\mathbb{Z}[\mu_{p^s}]$ to $\mathbb{Z}_s$ as part of the first map. The latter discards information but is sufficient for the purposes of studying the conjecture of [Sh1].

Remark 3.2.3. For $\alpha, \beta \in \mathbb{Q}$ not both zero and with denominators dividing $L > 1$, there is a rationally-defined Siegel unit $g_{\alpha,\beta} \in \mathscr{O}(Y(L)_{/\mathbb{Z}[\frac{1}{L}]})^\times \otimes_{\mathbb{Z}} \mathbb{Q}$ which satisfies $_c g_{\alpha,\beta} = g_{\alpha,\beta}^{c^2} g_{c\alpha,c\beta}^{-1} \in \mathscr{O}(Y(L)_{/\mathbb{Z}[\frac{1}{L}]})^\times$ for $c > 1$ prime to $6L$. Taking a cup product followed by a norm of two Siegel units attached to a pair (u, v) as in Definition 3.2.1, we obtain an element

$$z_{r,s}(u : v) \in H^1(\mathbb{Z}_s[\tfrac{1}{N}], H^1(Y_1(N_r)_{/\overline{\mathbb{Q}}}, \mathbb{Q}_p(2))).$$

For $s = 0$, the relationship between this zeta element and the (c, d)-version is given in the latter cohomology group by

$$_{c,d}z_{r,0}(u : v) = c^2 d^2 z_{r,0}(u : v) - d^2 z_{r,0}(cu : v) - c^2 z_{r,0}(u : dv) + z_{r,0}(cu : dv),$$

mirroring our definition of (c, d)-symbols in Definition 2.1.3. For $s > 0$, the relationship between the zeta elements $z_{r,s}(u : v)$ and $_{c,d}z_{r,s}(u : v)$ is likewise analogous to the relationship between the symbols $(u : v)$ and the symbols $_{c,d}(u : v]$ defined below in (3.1).

Remark 3.2.4. We have the following norm compatibilities among zeta elements.

i. For a fixed $s \geq 0$, the elements $_{c,d}z_{r,s}(p^{r-1}u : v)$ with $r \geq 1$ are compatible with the norm maps induced by quotients of modular curves. (This is seen through the observation that $_{c,d}z_{r+1,s}(p^r u : v)$ arises from a norm of a cup product of two Siegel units, the first of which is already a unit on $Y(p^s, N_{r+s})_{/\mathbb{Z}[\frac{1}{N}]}$.)

ii. For a fixed $r \geq 1$, the elements $_{c,d}z_{r,s}(u : v)$ are compatible for $s \geq 1$ under corestriction maps for the ring extensions, while the corestriction from $\mathbb{Z}_s[\frac{1}{N}]$ to $\mathbb{Z}[\frac{1}{N}]$ takes $_{c,d}z_{r,s}(u : v)$ to $(1 - U_p)_{c,d}z_{r,0}(u : v)$ (see [FK, Prop. 2.4.4]).

Let us use $_{c,d}z_{r,s}(u : v)_\theta$ to denote the projection of $_{c,d}z_{r,s}(u : v)$ to $H^1(\mathbb{Z}_s[\frac{1}{N}], \tilde{\mathscr{T}}_r^{(\theta)}(1))$. We will use the same notation to denote its image in the Eisenstein component $H^1(\mathbb{Z}_s[\frac{1}{N}], (\tilde{\mathscr{T}}_r)_\mathfrak{m}(1))$.

Definition 3.2.5. For $c, d > 1$ with $(c, d, 6N) = 1$ and $u, v \in \mathbb{Z}$ with $(u, v, M) = 1$ and $p \nmid v$, we set
$$_{c,d}z(u : v)_\theta = (_{c,d}z_{r,s}(p^{r-1}u : v)_\theta)_{r,s \geq 1} \in H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\frac{1}{N}], \tilde{\mathscr{T}}^{(\theta)}(1)).$$

If $u \not\equiv 0 \bmod N$, we also set
$$_{c,d}z^\sharp(u : v)_\theta = (_{c,d}z_{r,0}(p^{r-1}u : v)_\theta)_{r \geq 1} \in H^1(\mathbb{Z}[\frac{1}{N}], \tilde{\mathscr{T}}^{(\theta)}(1)).$$

Remark 3.2.6. The corestriction of $_{c,d}z(u : v)_\theta$ to $H^1(\mathbb{Z}[\frac{1}{N}], \tilde{\mathscr{T}}^{(\theta)}(1))$ is $(1 - U_p)z^\sharp(u : v)_\theta$ for $u \not\equiv 0 \bmod N$.

In what follows, Λ should typically be thought of as an Iwasawa algebra of elements of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, while Λ_θ should be considered as an algebra of inverses of diamond operators. Let $Q(O)$ denote the quotient field of an integral domain O.

Remark 3.2.7. In [FK, Prop. 3.1.3], the Λ-module $H^1_{\mathrm{Iw}}(\mathbb{Z}[\mu_{p^\infty}, \frac{1}{N}], H^1(X_1(N_r)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p)(2))$ is shown to be torsion-free. The proof of the following lemma yields the analogue on ordinary parts in the inverse limit over r, which is to say that $H^1_{\mathrm{Iw}}(\mathbb{Z}[\mu_{p^\infty}, \frac{1}{N}], \mathscr{T}^{(\theta)}(1))$ is $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \Lambda_\theta$-torsion free, without assumption on θ. However, we work with the cohomology of $\mathbb{Z}_\infty[\frac{1}{N}]$, as opposed to $\mathbb{Z}[\mu_{p^\infty}, \frac{1}{N}]$, in order to obtain torsion-freeness with coefficients in the larger module $\tilde{\mathscr{T}}^{(\theta)}(1)$.

In the proofs of the results that follow, though not the statements, we will omit superscripts "$^{(\theta)}$" denoting eigenspaces and subscripts "$_\mathfrak{m}$" denoting Eisenstein parts to lessen notation.

Lemma 3.2.8. *The $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \Lambda_\theta$-module $H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\frac{1}{N}], \tilde{\mathscr{T}}^{(\theta)}(1))$ is torsion-free.*

Proof. Note first that $H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\frac{1}{N}], \mathscr{T}(1))$ has no nonzero Λ_θ-torsion as zeroth Iwasawa cohomology groups are trivial. We modify the argument of [FK, Prop. 3.1.3(1)] in order to see that

$H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\frac{1}{N}], \mathscr{T}(1))$ has no $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \Lambda_\theta$-torsion. Let Λ^ι denote Λ with the inverse action of elements of the absolute Galois group $G_\mathbb{Q}$, and set $U = \Lambda^\iota \hat{\otimes}_{\mathbb{Z}_p} \mathscr{T}(1)$. Take a nonzero $v \in \Lambda \hat{\otimes}_{\mathbb{Z}_p} \Lambda_\theta$. Any v-torsion in the Λ_θ-torsion free

$$H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \mathscr{T}(1)) \cong H^1(\mathbb{Z}[\tfrac{1}{N}], U)$$

lies in $H^0(\mathbb{Z}[\frac{1}{N}], U/vU) \otimes_{\Lambda_\theta} Q(\Lambda_\theta)$. We set $\mathscr{Q} = \Lambda^\iota(1) \hat{\otimes}_{\mathbb{Z}_p} Q(\Lambda_\theta)$ for brevity, and we let V^* denote the $Q(\Lambda_\theta)$-dual of a $Q(\Lambda_\theta)[\![G_\mathbb{Q}]\!]$-module V. We then have

$$\begin{aligned}
H^0(\mathbb{Z}[\tfrac{1}{N}], U/vU) \otimes_{\Lambda_\theta} Q(\Lambda_\theta) &\cong \mathrm{Hom}_{Q(\Lambda_\theta)[\![G_\mathbb{Q}]\!]}(Q(\Lambda_\theta), U/vU \otimes_{\Lambda_\theta} Q(\Lambda_\theta)) \\
&\cong \mathrm{Hom}_{Q(\Lambda_\theta)[\![G_\mathbb{Q}]\!]}(Q(\Lambda_\theta), \mathscr{T} \otimes_{\Lambda_\theta} \mathscr{Q}/v\mathscr{Q}) \\
&\cong \mathrm{Hom}_{Q(\Lambda_\theta)[\![G_\mathbb{Q}]\!]}((\mathscr{T} \otimes_{\Lambda_\theta} Q(\Lambda_\theta))^*, \mathscr{Q}/v\mathscr{Q}),
\end{aligned}$$

noting that $\mathscr{T} \otimes_{\Lambda_\theta} Q(\Lambda_\theta)$ is a finite-dimensional $Q(\Lambda_\theta)$-vector space in the final step. It follows from the work of Hida [Hi] that the rank two $\mathfrak{h} \otimes_{\Lambda_\theta} Q(\Lambda_\theta)$-module $\mathscr{T} \otimes_{\Lambda_\theta} Q(\Lambda_\theta)$ is a direct sum of irreducible two-dimensional representations over finite extensions of $Q(\Lambda_\theta)$ that are attached to ordinary Λ_θ-adic eigenforms for the Hecke operators T_ℓ with $\ell \nmid N$ and U_p. Since $G_\mathbb{Q}$ acts on $\mathscr{Q}/v\mathscr{Q}$ through its maximal abelian quotient, any $Q(\Lambda_\theta)[\![G_\mathbb{Q}]\!]$-homomorphism

$$(\mathscr{T} \otimes_{\Lambda_\theta} Q(\Lambda_\theta))^* \to \mathscr{Q}/v\mathscr{Q}$$

is trivial. Thus, the $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \Lambda_\theta$-module $H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\frac{1}{N}], \mathscr{T}(1))$ has no torsion.

It remains only to show that the rightmost group in the exact sequence

$$0 \to H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \mathscr{T}(1)) \to H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \tilde{\mathscr{T}}(1)) \to H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], (\tilde{\mathscr{T}}/\mathscr{T})(1)).$$

has no $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \Lambda_\theta$-torsion. Taking $\bar{U} = \Lambda^\iota \hat{\otimes}_{\mathbb{Z}_p} (\tilde{\mathscr{T}}/\mathscr{T})(1)$, this reduces to showing that the $G_\mathbb{Q}$-invariant group $(\bar{U}/v\bar{U})^{G_\mathbb{Q}}$ is trivial for v as before. But, $G_{\mathbb{Q}(\mu_M)}$ acts trivially on $\tilde{\mathscr{T}}/\mathscr{T}$ by [FK, Prop. 3.2.4], so $(\bar{U}/v\bar{U})^{G_{\mathbb{Q}(\mu_M)}}$ is killed by $\omega(a) - 1$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, which of course means it is trivial. □

We next prove our first result on the integrality of the zeta maps of the first two authors. We consider the following symbols in the completed tensor product $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \tilde{\mathscr{H}}$:

$$_{c,d}[u:v] = c^2 d^2 \otimes (u:v) - d^2 \kappa(c) \otimes (cu:v) - c^2 \kappa(d) \otimes (u:dv) + \kappa(cd) \otimes (cu:dv), \quad (3.1)$$

where $\kappa \colon \mathbb{Z}_p^\times \to \Lambda$ sends a unit to the group element of its projection to $1 + p\mathbb{Z}_p$ (see [FK, 2.4.6]).

Theorem 3.2.9. *If $f = N$ (resp., $M \mid f$ and $f > 1$), then there exists a unique $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \mathfrak{H}$-linear map*

$$z \colon \Lambda \hat{\otimes}_{\mathbb{Z}_p} \tilde{\mathcal{H}} \to H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \tilde{\mathcal{T}}^{(\theta)}(1)) \quad (\textit{resp.}, \; z \colon \Lambda \hat{\otimes}_{\mathbb{Z}_p} \tilde{\mathcal{H}} \to H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \tilde{\mathcal{T}}_{\mathrm{m}}(1)))$$

such that $z(_{c,d}(u : v]) = {}_{c,d} z(u, v)_\theta$ for all c, d, u, and v.

Proof. We let $\Omega = \Lambda \hat{\otimes}_{\mathbb{Z}_p} \Lambda_\theta$. In [FK, Theorem 3.2.3], it is shown (via a regulator computation) that there exists a well-defined map

$$z \colon \Lambda \hat{\otimes}_{\mathbb{Z}_p} \tilde{\mathcal{H}} \to H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \tilde{\mathcal{T}}(1)) \otimes_\Omega Q(\Omega)$$

with the stated property. Each $_{c,d} z(u : v)_\theta$ lies in $H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \tilde{\mathcal{T}}(1))$, and $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \tilde{\mathcal{H}}$ is generated by the $_{c,d}(u : v]$ as an Ω-module by Propositions 3.1.5 and 3.1.6 and Nakayama's lemma. Therefore, the image of z is contained in the image of the map

$$H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \tilde{\mathcal{T}}(1)) \to H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \tilde{\mathcal{T}}(1)) \otimes_\Omega Q(\Omega)$$

Lemma 3.2.8 tells us that the latter map is injective, hence the result. $\square$

Lemma 3.2.10. *If $p \mid f$, then the Λ_θ-module $H^1(\mathbb{Z}[\tfrac{1}{N}], \tilde{\mathcal{T}}^{(\theta)}(1))$ is torsion-free. If $M \mid f$ and $f > 1$, then $H^1(\mathbb{Z}[\tfrac{1}{N}], \tilde{\mathcal{T}}_{\mathrm{m}}(1))$ is Λ_θ-torsion free.*

Proof. The first statement is [FK, Prop. 3.3.6(2)], which implies the second statement for $f = N$. The second statement is proven (in particular) in the case $f = M > 1$ in [Sh2]. $\square$

Let $\mathrm{Cor} \colon H^1_{\mathrm{Iw}}(\mathbb{Z}_\infty[\tfrac{1}{N}], \tilde{\mathcal{T}}^{(\theta)}(1)) \to H^1(\mathbb{Z}[\tfrac{1}{N}], \tilde{\mathcal{T}}^{(\theta)}(1))$ denote corestriction. Then $\mathrm{Cor} \circ z$ factors through the quotient $\mathcal{H}$ of $\Lambda \hat{\otimes}_{\mathbb{Z}_p} \tilde{\mathcal{H}}$.

Theorem 3.2.11. *If $f = N$ (resp., $M \mid f$ and $f > 1$), then there exists a unique $\mathfrak{H}$-linear map*

$$z^\sharp \colon \mathcal{H} \to H^1(\mathbb{Z}[\tfrac{1}{N}], \tilde{\mathcal{T}}^{(\theta)}(1)) \quad (\textit{resp.}, \; z^\sharp \colon \mathcal{H} \to H^1(\mathbb{Z}[\tfrac{1}{N}], \tilde{\mathcal{T}}_{\mathrm{m}}(1)))$$

such that $(1 - U_p) z^\sharp = \mathrm{Cor} \circ z$ on $\mathcal{H}$ and

$$z^\sharp(_{c,d}(u : v)) = {}_{c,d} z^\sharp(u : v)_\theta$$

for all c, d, u, and v.

Proof. In [FK, Theorem 3.3.9], it was shown that there exists a map

$$z^\sharp \colon \mathcal{H} \to H^1(\mathbb{Z}[\tfrac{1}{N}], \tilde{\mathcal{T}}(1)) \otimes_{\Lambda_\theta} Q(\Lambda_\theta)$$

with the stated properties, equalities taking place in this group. Moreover, the elements $_{c,d}z^\sharp(u:v)_\theta$ are all in $H^1(\mathbb{Z}[\frac{1}{N}], \tilde{\mathscr{T}}(1))$ itself, and $\mathscr{H}$ is generated by the $_{c,d}(u:v)$ (with $N \nmid u$) as a Λ_θ-module by Propositions 3.1.5 and 3.1.6. Therefore, the image of $z^\sharp$ is contained in the image of the map

$$H^1(\mathbb{Z}[\tfrac{1}{N}], \tilde{\mathscr{T}}(1)) \to H^1(\mathbb{Z}[\tfrac{1}{N}], \tilde{\mathscr{T}}(1)) \otimes_{\Lambda_\theta} Q(\Lambda_\theta),$$

which is injective by Lemma 3.2.10. The equalities then also take place in $H^1(\mathbb{Z}[\frac{1}{N}], \tilde{\mathscr{T}}(1))$. □

Remark 3.2.12. Let $X_1^0(N_r)_{/\mathbb{Z}[\frac{1}{N}]}$ denote the scheme-theoretic complement in $X_1(N_r)_{/\mathbb{Z}[\frac{1}{N}]}$ of the closed $\mathbb{Z}[\frac{1}{N}]$-subscheme of zero cusps, and set

$$\mathscr{T}^0 = \varprojlim_r H^1(X_1^0(N_r)_{/\overline{\mathbb{Q}}}, \mathbb{Z}_p(1))^{\mathrm{ord}}.$$

It follows from [FK, Prop. 3.2.4] that the map $H^1(\mathbb{Z}[\frac{1}{N}], \mathscr{T}^0(1)) \to H^1(\mathbb{Z}[\frac{1}{N}], \tilde{\mathscr{T}}(1))$ is injective. By [FK, Theorem 3.3.9(iii)], the map $z^\sharp$ then actually takes values in (the θ-eigenspace, or Eisenstein part, of) $H^1(\mathbb{Z}[\frac{1}{N}], \mathscr{T}^0(1))$ inside $H^1(\mathbb{Z}[\frac{1}{N}], \tilde{\mathscr{T}}(1))$.

References

[Br]   F. Brunault, Beilinson-Kato elements in K_2 of modular curves, *Acta Arith.* **134** (2008), 283-298.

[Bu]   C. Busuioc, The Steinberg symbol and special values of L-functions, *Trans. Amer. Math. Soc.* **360** (2008), 5999–6015.

[FK]   T. Fukaya and K. Kato, On conjectures of Sharifi, preprint, 121 pages.

[FKS] T. Fukaya, K. Kato, R. Sharifi, Modular symbols in Iwasawa theory, *Iwasawa Theory 2012 - State of the Art and Recent Advances*, Contrib. Math. Comput. Sci. **7**, Springer, 2014, 177-219.

[Hi]   H. Hida, Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[\![X]\!])$ attached to ordinary cusp forms, *Invent. Math.* **85** (1986), 545–613.

[Ma]   J. Manin, Parabolic points and zeta-functions of modular curves, *Math. USSR Izvsetija* **6** (1972), 19–64.

[Me]   L. Merel, Universal Fourier expansions of modular forms, *On Artin's conjecture for odd 2-dimensional representations*, Lecture Notes in Math., 1585, Springer, Berlin, 1994, 59–94.

[Oh1] M. Ohta, On the p-adic Eichler-Shimura isomorphism for Λ-adic cusp forms, *J. reine angew. Math.* **463** (1995), 49–98.

[Oh2] M. Ohta, Ordinary étale cohomology groups attached to towers of elliptic modular curves. II, *Math. Ann.* **318** (2000), 557–583.

[Sh1] R. Sharifi, A reciprocity map and the two variable p-adic L-function, *Ann. of Math.* **173** (2011), 251–300.

[Sh2] R. Sharifi, An extension of the method of Fukaya and Kato, in preparation.

[Wi] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math.* **131** (1990), 493–540.