JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 15, Number 3, Pages 671–714
S 0894-0347(02)00390-9
Article electronically published on February 27, 2002

SUPERSINGULAR ELLIPTIC CURVES, THETA SERIES AND WEIGHT TWO MODULAR FORMS

MATTHEW EMERTON

This paper deals with two subjects and their interaction. The first is the problem of spanning spaces of modular forms by theta series. The second is the commutative algebraic properties of Hecke modules arising in the arithmetic theory of modular forms.

Let p be a prime, and let B denote the quaternion algebra over $\mathbb{Q}$ that is ramified at p and ∞ and at no other places. If L is a left ideal in a maximal order of B, then L is a rank four $\mathbb{Z}$-module equipped in a natural way with a positive definite quadratic form [6, §1]. (We shall say that L is a rank four quadratic space, and remark that the isomorphism class of L as a quadratic space depends only on the left ideal class of L in its maximal order.) Eichler [5] proved that the theta series of L is a weight two modular form on $\Gamma_0(p)$, and that as L ranges over a collection of left ideal class representatives of all left ideals in all maximal orders of B these theta series span the vector space of weight two modular forms on $\Gamma_0(p)$ over $\mathbb{Q}$.

In this paper we strengthen this result as follows: if L is as above, then the q-expansion of its theta series $\Theta(L)$ has constant term equal to one and all other coefficients equal to even integers. Suppose that f is a modular form whose q-expansion coefficients are even integers, except perhaps for its constant term, which we require merely to be an integer. It follows from Eichler's theorem that f may be written as a linear combination of $\Theta(L)$ (with L ranging over a collection of left ideals of maximal orders of B) with rational coefficients. We show that in fact these coefficients can be taken to be integers.

Let $\mathbb{T}$ denote the $\mathbb{Z}$-algebra of Hecke operators acting on the space of weight two modular forms on $\Gamma_0(p)$. The proof that we give of our result hinges on analyzing the structure of a certain $\mathbb{T}$-module $\mathcal{X}$. We can say what $\mathcal{X}$ is: it is the free $\mathbb{Z}$-module of divisors supported on the set of singular points of the (reducible, nodal) curve $X_0(p)$ in characteristic p. The key properties of $\mathcal{X}$, which imply the above result on theta series, are that the natural map $\mathbb{T} \longrightarrow \mathrm{End}_{\mathbb{T}}(\mathcal{X})$ is an isomorphism, and that furthermore $\mathcal{X}$ is locally free of rank one in a Zariski neighbourhood of the Eisenstein ideal of $\mathbb{T}$. We remark that it is comparatively easy to prove the analogous statements after tensoring with $\mathbb{Q}$, for they then follow from the fact that $\mathcal{X}$ is a faithful $\mathbb{T}$-module. Indeed, combining this with the semi-simplicity of the $\mathbb{Q}$-algebra $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$, one deduces that $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a free $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$-module of rank one, and in particular that the map $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathrm{End}_{\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}}(\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q})$ is an isomorphism.

Received by the editors November 1, 2000 and, in revised form, September 19, 2001.
2000 *Mathematics Subject Classification.* Primary 11F11, 11F27, 11F37.

By contrast, $\mathcal{X}$ need not always be locally free of rank one as a $\mathbb{T}$-module. Indeed, we show that this is the case if and only if $\mathbb{T}$ is a Gorenstein ring, and Kilford [14] has shown that $\mathbb{T}$ can be non-Gorenstein (for example, when p equals 431 or 503).

The connection between Eichler's theorem and the $\mathbb{T}$-module $\mathcal{X}$ was observed by Ohta [18] (actually, he considered only the mod p reduction of $\mathcal{X}$), and further developed by Gross [6]. It was Gross who raised the question of studying the structure of $\mathcal{X}$ and of strengthening Eichler's result [8]. In addition to the ideas of [6], our arguments will rely heavily on the results and techniques of [15] and [20], [23], which provide powerful tools for analyzing questions related to the arithmetic of modular forms.

The contents of the paper are as follows. Section 0 presents a more detailed introduction to the paper, and states the main results. It concludes with a complete analysis of the case $p = 11$, to serve the reader as an example. Sections 1, 2, 3 and 4 develop all the inputs necessary for the proofs of the results stated in section 0. The actual proofs of these results are presented in section 5. Section 6 discusses some aspects of the situation when $\mathbb{T}$ is non-Gorenstein; in particular, it provides an interpretation of some of our results in the language of "local theta-characteristics" of one-dimensional local rings. Section 7 discusses the extension of our results to the case of non-prime level. Finally, the appendix relates the analysis of the $\mathbb{T}$-module $\mathcal{X}$ made in the main body of the paper to the p-adic analytic properties of $X_0(p)$; it is somewhat disjoint from the rest of the paper.

We close this introduction by remarking on two novel points that arise in the proof of our main results. The first is that we obtain in sections 3 and 7 a new proof that the theta series of various quadratic forms constructed from the quaternion algebra B are modular forms, which is algebro-geometric rather than analytic in nature. The second is Theorem 4.6, which yields some information about the torsion subgroup of a modular Jacobian in the absence of a Gorenstein hypothesis, by appealing instead to level lowering results. We hope that both ideas may have additional applications.

0. Statement of results

We will describe our results in more detail. We begin by introducing some notation and filling in some background. If f is a weight two modular form on $\Gamma_0(p)$, we let $a_n(f)$ denote the n^{th} q-expansion coefficient of f, so that $f = \sum_{n=0}^{\infty} a_n(f)q^n$. We let $\mathcal{M}$ denote the $\mathbb{Z}$-module of weight two modular forms f on $\Gamma_0(p)$ for which $a_n(f) \in \mathbb{Z}$ when $n \geq 1$ and $a_0(f) \in \frac{1}{2}\mathbb{Z}$.

One way of producing elements in $\mathcal{M}$ is as follows: if E_i and E_j are two supersingular elliptic curves in characteristic p, then $L_{i,j} = \mathrm{Hom}(E_i, E_j)$ is a free $\mathbb{Z}$-module of rank four equipped with a positive definite quadratic form, given by taking the degree of an isogeny (see Proposition 3.6 below for details). If $\Theta(L_{i,j})$ denotes the theta series of $L_{i,j}$, then $\frac{1}{2}\Theta(L_{i,j})$ lies in $\mathcal{M}$. (See Proposition 3.15 below, as well as the subsequent remarks, for a discussion of this point.) The quadratic spaces $L_{i,j}$ are precisely those attached to the quaternion algebra B in the manner described in the introduction (as is explained in [6, §2]).

Let $X_0(p)$ denote the curve over $\mathrm{Spec}\,\mathbb{Z}$ that is a coarse moduli space for the $\Gamma_0(p)$-moduli problem. The fibres of $X_0(p)$ are smooth curves over every point of

$\operatorname{Spec}\mathbb{Z}$ other than p. By contrast, if g denotes the (constant) arithmetic genus of the fibres of $X_0(p)$ (which we recall is approximately equal to $p/12$, as follows from Proposition 3.15 below, for example), then the geometric fibre of $X_0(p)$ in characteristic p is the union of two rational curves meeting at $g+1$ ordinary double points. Let $x_0, \ldots, x_g$ denote these singular points; they are in bijective correspondence with the isomorphism classes of supersingular curves E_i. Let $\mathcal{X}$ denote the free $\mathbb{Z}$-module of divisors supported on the x_i, and define a $\mathbb{Z}$-bilinear pairing

$$\mathcal{X} \times \mathcal{X} \longrightarrow \mathcal{M} \tag{0.1}$$

by the formula $x_i \times x_j \mapsto \frac{1}{2}\Theta(L_{i,j})$.

As above, we let $\mathbb{T}$ denote the $\mathbb{Z}$-algebra of Hecke operators acting on the space of weight two modular forms on $\Gamma_0(p)$. The $\mathbb{Z}$-module $\mathcal{M}$ is closed under the action of $\mathbb{T}$, and so $\mathcal{M}$ is naturally a faithful $\mathbb{T}$-module. The action of the Hecke correspondences on the set of x_i induces an action on $\mathcal{X}$ which factors through $\mathbb{T}$, making $\mathcal{X}$ a faithful $\mathbb{T}$-module as well (see Theorem 3.1 below). One shows (see [6] or section 3 below) that the pairing (0.1) is $\mathbb{T}$-bilinear, and so induces a map

$$\mathcal{X} \otimes_{\mathbb{T}} \mathcal{X} \longrightarrow \mathcal{M} \tag{0.2}$$

from the tensor product of $\mathcal{X}$ with itself over $\mathbb{T}$ to $\mathcal{M}$.

Theorem 0.3. *The morphism* (0.2) *is surjective. Equivalently, $\mathcal{M}$ is spanned by the half-theta series* $\frac{1}{2}\Theta(L_{i,j})$.

Recall that $\mathcal{X}$ and $\mathcal{M}$ are both free of rank $g+1$ over $\mathbb{Z}$ (where g is equal to the genus of $X_0(p)$), and so in particular (taking into account the symmetry $L_{i,j} \xrightarrow{\sim} L_{j,i}$; see Lemma 3.7) there are $(g+1)(g+2)/2$ theta series $\Theta(L_{i,j})$. Thus although Theorem 0.3 yields an explicit spanning set for $\mathcal{M}$ as a $\mathbb{Z}$-module, it does not yield a basis for $\mathcal{M}$ (except in the case when $g = 0$).

As we indicated in the introduction, Theorem 0.3 is closely connected to the following result.

Theorem 0.4. *The natural morphism $\mathbb{T} \longrightarrow \operatorname{End}_{\mathbb{T}}(\mathcal{X})$ is an isomorphism.*

The passage between the intrinsic structure of the $\mathbb{T}$-module $\mathcal{X}$ and the surjectivity of (0.2) is provided by the duality between Hecke operators and modular forms (discussed in section 1), some commutative algebra of bilinear pairings (discussed in section 2), and the existence of a natural $\mathbb{Z}$-valued $\mathbb{T}$-bilinear pairing on $\mathcal{X}$. If we let e_i denote one-half the number of automorphisms of E_i, then this pairing is defined as follows: $\langle x_i, x_j \rangle = e_i \delta_{i,j}$. The connection with (0.2) is provided by the formula $\langle x_i, x_j \rangle = a_1(\frac{1}{2}\Theta(L_{i,j}))$. (See section 3 for a more complete discussion of this pairing, and Proposition 3.11 and the surrounding text in particular for a precise statement of its connection with (0.2).)

As already mentioned in the introduction, the $\mathbb{T}$-module $\mathcal{X}$ is not always locally free of rank one. In order to state our results concerning this subject, we introduce some additional notation.

We let $\mathcal{M}^0$ denote the $\mathbb{T}$-submodule of $\mathcal{M}$ consisting of those f for which $a_0(f) = 0$ (that is, the submodule of cusp forms in $\mathcal{M}$), and let $\mathbb{T}^0$ denote that quotient of $\mathbb{T}$ that acts faithfully on $\mathcal{M}^0$. We let $\mathcal{X}^0$ denote the submodule of $\mathcal{X}$ consisting of divisors of degree zero. Then $\mathcal{X}^0$ is also a faithful $\mathbb{T}^0$-module (see Theorem 3.1 below).

For any maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ and any $\mathbb{T}$-module U we let $U_{\mathfrak{m}}$ denote the completion of U at $\mathfrak{m}$. In particular, $\mathbb{T}_{\mathfrak{m}}$ denotes the completion of $\mathbb{T}$ at $\mathfrak{m}$, and $U_{\mathfrak{m}}$ is naturally a $\mathbb{T}_{\mathfrak{m}}$-module.

Theorem 0.5. *Fix a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$. The following are equivalent:*

(i) *The $\mathbb{T}_{\mathfrak{m}}$-module $\mathcal{M}_{\mathfrak{m}}$ is free of rank one.*
(i)^0 *The $\mathbb{T}^0_{\mathfrak{m}}$-module $\mathcal{M}^0_{\mathfrak{m}}$ is free of rank one.*
(ii) *The $\mathbb{T}_{\mathfrak{m}}$-module $\mathcal{X}_{\mathfrak{m}}$ is free of rank one.*
(ii)^0 *The $\mathbb{T}^0_{\mathfrak{m}}$-module $\mathcal{X}^0_{\mathfrak{m}}$ is free of rank one.*
(iii) *The ring $\mathbb{T}_{\mathfrak{m}}$ is Gorenstein.*
(iii)^0 *The ring $\mathbb{T}^0_{\mathfrak{m}}$ is Gorenstein.*

If these equivalent conditions hold, then the morphism $\mathcal{X}_{\mathfrak{m}} \otimes_{\mathbb{T}_{\mathfrak{m}}} \mathcal{X}_{\mathfrak{m}} \longrightarrow \mathcal{M}_{\mathfrak{m}}$ induced by (0.2) *is an isomorphism.*

It seems worth remarking on the nature of the Gorenstein hypotheses that appear among the equivalent statements of Theorem 0.5. It follows from the results of [15] that $\mathbb{T}_{\mathfrak{m}}$ and $\mathbb{T}^0_{\mathfrak{m}}$ are Gorenstein in most cases (see Theorem 1.14 below for the precise statement). In particular this is the case if $\mathfrak{m}$ is Eisenstein (in the sense described in section 1 below). The proof of this result depends on the deepest results of [15], and we rely upon these same results to prove Theorem 0.5 in the Eisenstein case. In particular, in this case Theorem 0.5 should properly be regarded, both in its statement and its proof, as showing that "if $\mathfrak{m}$ is an Eisenstein maximal ideal, then the following properties hold", rather than as presenting a list of equivalent properties that may or may not hold.

In the non-Eisenstein case the situation is quite different. Interestingly, and perhaps contrary to general expectations, L. Kilford [14] has recently found examples of non-Eisenstein $\mathfrak{m}$ for which $\mathbb{T}_{\mathfrak{m}}$ is non-Gorenstein. (The results of [15] show that such $\mathfrak{m}$ are necessarily of residue characteristic two and ordinary.) Thus in this case Theorem 0.5 is genuinely a list of equivalent possibilities, that may or may not hold in any particular case. (It is mentioned in [14] that William Stein has implemented Theorem 0.5 as a means of testing whether or not $\mathbb{T}_{\mathfrak{m}}$ is Gorenstein, by taking advantage of the fact that condition (ii) is amenable to being checked by computer algebra.)

Since the modules $\mathcal{X}$ and $\mathcal{X}^0$ appear with equal status among the conditions of Theorem 0.5, one might ask whether suitable analogues of Theorems 0.3 and 0.4 hold when $\mathcal{X}$ is replaced by $\mathcal{X}^0$ and $\mathcal{M}$ by $\mathcal{M}^0$. We will state a result that answers this question, after making a definition. Let $\mathbb{T}^{\mathrm{Eis}}$ denote the quotient of $\mathbb{T}$ which acts faithfully on the weight two Eisenstein series on $\Gamma_0(p)$ (so that after forgetting the $\mathbb{T}$-algebra structure, $\mathbb{T}^{\mathrm{Eis}}$ is isomorphic to $\mathbb{Z}$). Let I denote the ideal in $\mathbb{T}$ which is the kernel of the surjection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}}$. Then the ideal $I\mathbb{T}^0$ of $\mathbb{T}^0$ has finite index in $\mathbb{T}^0$, equal to the numerator of $(p-1)/12$ (when written in lowest terms) (see Proposition 1.8, part (iii)); denote this number by n. Note that this ideal $I\mathbb{T}^0$ is the celebrated Eisenstein ideal of [15].

Theorem 0.6. (i) *The image of the morphism $\mathcal{X}^0 \otimes_{\mathbb{T}^0} \mathcal{X}^0 \longrightarrow \mathcal{M}^0$ induced by* (0.2) *is equal to $I\mathcal{M}^0$, and is of index n in $\mathcal{M}^0$.*

(ii) *The natural map $\mathbb{T}^0 \longrightarrow \mathrm{End}_{\mathbb{T}^0}(\mathcal{X}^0)$ is an isomorphism.*

As a final variant on our theme, we note that the $\mathbb{Z}$-valued pairing on $\mathcal{X}$ described above yields an embedding $\mathcal{X} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$, whose image has finite index in

$\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X},\mathbb{Z})$. Thus we may extend the pairing (0.1) to a pairing

$$\mathcal{X}\times\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X},\mathbb{Z})\longrightarrow\mathcal{M}\otimes_{\mathbb{Z}}\mathbb{Q}. \tag{0.7}$$

If $\check{x}_0,\dots,\check{x}_g$ denotes the basis of $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X},\mathbb{Z})$ dual to the basis $x_0,\dots,x_g$ of $\mathcal{X}$, then $\check{x}_j=\dfrac{x_j}{e_j}$ for $j=0,\dots,g$, and so the pairing (0.7) maps the pair $(x_i,\check{x}_j)$ to the normalized theta series $\dfrac{\Theta(L_{i,j})}{2e_j}$. Thus, if we let $\mathcal{N}$ denote the submodule of $\mathcal{M}\otimes_{\mathbb{Z}}\mathbb{Q}$ consisting of modular forms f for which $a_n(f)\in\mathbb{Z}$ if $n\geq 1$ (but with no condition on $a_0(f)$), then (0.7) takes values in $\mathcal{N}$, and induces a morphism

$$\mathcal{X}\otimes_{\mathbb{T}}\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X},\mathbb{Z})\longrightarrow\mathcal{N}. \tag{0.8}$$

There is an analogue for $\mathcal{X}^0$, yielding a morphism

$$\mathcal{X}^0\otimes_{\mathbb{T}^0}\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}^0,\mathbb{Z})\longrightarrow\mathcal{M}^0. \tag{0.9}$$

(Note that there is no distinction between cusp forms in $\mathcal{M}$ and in $\mathcal{N}$.) The following result describes the images of these morphisms.

Theorem 0.10. *The morphisms* (0.8) *and* (0.9) *are surjections of* $\mathbb{T}$*-modules.*

Note that the surjectivity of (0.8) is equivalent to the statement that $\mathcal{N}$ is spanned over $\mathbb{Z}$ by the normalized theta series $\dfrac{\Theta(L_{i,j})}{2e_j}$.

We owe the idea of studying the $\mathbb{T}$-module $\mathcal{X}$ and the map (0.2) entirely to Gross, and the preceding results answer (in a slightly refined form) questions raised by him in [8]. In these lectures Gross also pointed out that a positive answer to these questions would yield a formal analogy with a theorem of Hecke in algebraic number theory [11, thm. 177], which we now explain. Namely, it follows from Theorem 1.14 below that $\mathbb{T}$ becomes Gorenstein after inverting 2, and from Propositions 1.1 and 1.3 that there is a natural injection $\mathcal{M}\longrightarrow\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T},\mathbb{Z})$ whose cokernel has order equal to the denominator of $(p-1)/12$, which hence becomes an isomorphism after inverting 6. Theorem 0.5 thus shows that after inverting 6 the morphism (0.2) yields an isomorphism of locally free $\mathbb{T}[1/6]$-modules of rank one:

$$\mathcal{X}[1/6]\otimes_{\mathbb{T}[1/6]}\mathcal{X}[1/6]\xrightarrow{\sim}\mathcal{M}[1/6]\xrightarrow{\sim}\mathrm{Hom}_{\mathbb{Z}[1/6]}(\mathbb{T}[1/6],\mathbb{Z}[1/6]).$$

In particular, $\mathrm{Hom}_{\mathbb{Z}[1/6]}(\mathbb{T}[1/6],\mathbb{Z}[1/6])$ is a square in the Picard group of $\mathbb{T}[1/6]$. By way of comparison, Hecke's theorem states that if $\mathcal{O}$ is the ring of integers in a finite extension of $\mathbb{Q}$, then the inverse different $\mathcal{D}^{-1}$ of $\mathcal{O}$ (which by definition is isomorphic to $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{O},\mathbb{Z})$ as an $\mathcal{O}$-module) is a square in the ideal class group (that is, the Picard group) of $\mathcal{O}$.

One can ask if the analogue of Hecke's result holds without inverting 6. That is, in those cases when $\mathbb{T}$ is Gorenstein, whether the $\mathbb{T}$-module $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T},\mathbb{Z})$ is a square element in the Picard group of $\mathbb{T}$; or whether $\mathrm{Hom}_{\mathbb{Z}[1/2]}(\mathbb{T}[1/2],\mathbb{Z}[1/2])$ is a square element in the Picard group of $\mathbb{T}[1/2]$ (remembering that $\mathbb{T}[1/2]$ is always Gorenstein). We don't know the answer to either of these questions in general.

An example. We will describe our results in as concrete a fashion as possible in the case when $p=11$. In particular, we will describe $\mathbb{T}$ explicitly, identify the elements of $\mathrm{Pic}(\mathbb{T})$ corresponding to $\mathcal{M}$, $\mathcal{N}$, $\mathcal{X}$, and $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X},\mathbb{Z})$, and describe the maps (0.2) and (0.8) in terms of these elements of $\mathrm{Pic}(\mathbb{T})$.

We begin by recalling that the space of modular forms of weight two on $\Gamma_0(p)$ is two-dimensional, spanned by the Eisenstein series $E = \frac{5}{12} + q + 3q^2 + \cdots$ and the cusp form $f = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = q - 2q^2 + \cdots$. These two Hecke eigenforms are congruent modulo five, and so one sees that $\mathcal{M}$ is the free $\mathbb{Z}$-module spanned by $\frac{6(E-f)}{5}$ and f, while $\mathcal{N}$ is the free $\mathbb{Z}$-module spanned by $\frac{E-f}{5}$ and f.

We now provide an explicit description of the Hecke ring $\mathbb{T}$. Each of $\mathbb{T}^{\mathrm{Eis}}$ and $\mathbb{T}^0$ is isomorphic to $\mathbb{Z}$, and (since E and f are congruent modulo five) the image of $\mathbb{T}$ under the injection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}} \oplus \mathbb{T}^0$ is equal to $\{(m_1, m_2) | m_1 \equiv m_2 \pmod 5\}$. This ring is Gorenstein; indeed, the pairing

$$(m_1, m_2) \times (m_1', m_2') \mapsto \frac{m_1 m_1' - m_2 m_2'}{5}$$

yields an isomorphism of $\mathbb{T}$ with its $\mathbb{Z}$-dual. (Since f is supersingular at two, this is a special case of Theorem 1.14 below.) One computes that $\mathrm{Pic}(\mathbb{T})$ is isomorphic to the cokernel of the natural map $\mathbb{Z}^\times \longrightarrow (\mathbb{Z}/5)^\times$, which has order two. The module $U = \{(m_1, m_2) | 2m_1 \equiv m_2 \pmod 5\}$ (with the obvious $\mathbb{T}$-action) represents the non-trivial element of $\mathrm{Pic}(\mathbb{T})$.

Define a map of $\mathbb{T}$-modules $\mathbb{T} \longrightarrow \mathcal{M}$ via $(m_1, m_2) \mapsto m_1 \frac{6E}{5} - m_2 \frac{f}{5}$. This is evidently an isomorphism of $\mathbb{T}$-modules (given the above description of $\mathcal{M}$), and shows that $\mathcal{M}$ represents the trivial element of $\mathrm{Pic}(\mathbb{T})$. Similarly the map $(m_1, m_2) \mapsto m_1 \frac{E}{5} - m_2 \frac{f}{5}$ is an isomorphism of $\mathbb{T}$ with $\mathcal{N}$, showing that $\mathcal{N}$ also represents the trivial element of $\mathrm{Pic}(\mathbb{T})$. (This last statement also follows from part (i) of Proposition 1.3 below, together with the preceding observation that $\mathbb{T}$ is isomorphic to its $\mathbb{Z}$-dual.) With respect to these two isomorphisms, the inclusion $\mathcal{M} \subset \mathcal{N}$ corresponds to the endomorphism of $\mathbb{T}$ defined via $(m_1, m_2) \mapsto (6m_1, m_2)$.

The two supersingular j-invariants in characteristic 11 are $j = 0$ and $j = 1728$. We denote the corresponding basis elements of $\mathcal{X}$ by x_0 and x_1. Then $e_0 = 3$ and $e_1 = 2$. Write $\mathbf{x} = 2x_0 + 3x_1$. It follows from the results of section 3 below that $\mathbb{T}$ acts on $\mathbf{x}$ through $\mathbb{T}^{\mathrm{Eis}}$ and on $x_1 - x_0$ through $\mathbb{T}^0$. Define a map of $\mathbb{T}$-modules $U \longrightarrow \mathcal{X}$ via $(m_1, m_2) \mapsto m_1 \frac{\mathbf{x}}{5} + m_2 \frac{x_1 - x_0}{5}$. It is immediate that this map is an isomorphism, and so $\mathcal{X}$ represents the non-trivial element of $\mathrm{Pic}(\mathbb{T})$.

Let $\check{x}_0$ and $\check{x}_1$ denote the basis of $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$ which is dual to the basis x_0, x_1 of $\mathcal{X}$. Then the degree morphism $\deg : \mathcal{X} \longrightarrow \mathbb{Z}$ is equal to the element $\check{x}_0 + \check{x}_1$ of $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$, while the element $2\check{x}_1 - 3\check{x}_0$ annihilates $\mathbf{x}$. It follows from the results of section 3 below that $\mathbb{T}$ acts on $\deg$ through $\mathbb{T}^{\mathrm{Eis}}$ and on $2\check{x}_1 - 3\check{x}_0$ through $\mathbb{T}^0$. Thus the morphism $U \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$ defined via $(m_1, m_2) \mapsto m_1 \frac{\deg}{5} + m_2 \frac{2\check{x}_1 - 3\check{x}_0}{5}$ is an isomorphism of $\mathbb{T}$-modules, and $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$ also represents the non-trivial element of $\mathrm{Pic}(\mathbb{T})$.

With respect to the isomorphisms $U \xrightarrow{\sim} \mathcal{X}$ and $U \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$ constructed in the preceding two paragraphs, the tautological perfect pairing $\mathcal{X} \times \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z}) \longrightarrow \mathbb{Z}$ corresponds to the perfect pairing $U \times U \longrightarrow \mathbb{Z}$ defined by

$$(m_1, m_2) \times (m_1', m_2') \mapsto \frac{m_1 m_1' + m_2 m_2'}{5}.$$

The embedding $\mathcal{X} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$ induced by the $\mathbb{Z}$-valued $\mathbb{T}$-bilinear pairing on $\mathcal{X}$ of Definition 3.4 below corresponds to the endomorphism of U defined via $(m_1, m_2) \mapsto (6m_1, m_2)$.

Recall that $L_{i,j}$ denotes the quadratic space of endomorphisms from the elliptic curve E_i representing x_i to the elliptic curve E_j representing x_j. From the values of e_0 and e_1 we can determine that

$$\frac{1}{2}\Theta(L_{0,0}) = \frac{1}{2} + 3q + \cdots = \frac{6E + 9f}{5},$$

that

$$\frac{1}{2}\Theta(L_{0,1}) = \frac{1}{2} + 0q + \cdots = \frac{6(E - f)}{5},$$

and that

$$\frac{1}{2}\Theta(L_{1,1}) = \frac{1}{2} + 2q + \cdots = \frac{6E + 4f}{5}.$$

From these formulas we compute the following particular values of the map $\mathcal{X} \otimes_{\mathbb{T}} \mathcal{X} \longrightarrow \mathcal{M}$ given by (0.2):

$$\mathbf{x} \otimes \mathbf{x} \mapsto 30E,$$

$$\mathbf{x} \otimes (x_1 - x_0) \mapsto 0,$$

and

$$(x_1 - x_0) \otimes (x_1 - x_0) \mapsto 5f.$$

Since both the source and target of (0.2) are torsion free $\mathbb{Z}$-modules, these values completely determine this map. One finds that, in terms of the given isomorphisms $U \xrightarrow{\sim} \mathcal{X}$ and $\mathbb{T} \xrightarrow{\sim} \mathcal{M}$, the map (0.2) corresponds to the isomorphism $U \otimes_{\mathbb{T}} U \xrightarrow{\sim} \mathbb{T}$, given by

$$(m_1, m_2) \otimes (m_1', m_2') \mapsto (m_1 m_1', -m_2 m_2'), \tag{0.11}$$

which witnesses the fact that U yields an element of $\mathrm{Pic}(\mathbb{T})$ of order two. We also see that the induced map $\mathcal{X}^0 \otimes_{\mathbb{T}^0} \mathcal{X}^0 \longrightarrow \mathcal{M}^0 = \mathbb{Z} \cdot f$ has image equal to $5\mathbb{Z} \cdot f$. (Note that 5 is the numerator of $(11 - 1)/12 = 5/6$.)

Similarly, we compute the following values of the map $\mathcal{X} \otimes_{\mathbb{T}} \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z}) \longrightarrow \mathcal{N}$ given by (0.8):

$$\mathbf{x} \otimes \deg \mapsto 5E,$$

$$\mathbf{x} \otimes (2\check{x}_1 - 3\check{x}_0) \mapsto 0,$$

$$(x_1 - x_0) \times \deg \mapsto 0,$$

and

$$(x_1 - x_0) \times (2\check{x}_1 - 3\check{x}_0) \mapsto 5f.$$

From these values we deduce that, in terms of the given isomorphisms $U \xrightarrow{\sim} \mathcal{X}$, $U \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$, and $\mathbb{T} \xrightarrow{\sim} \mathcal{N}$, the map (0.8) also corresponds to the isomorphism $U \otimes_{\mathbb{T}} U \xrightarrow{\sim} \mathbb{T}$ given by (0.11). If we note that $\mathrm{Hom}_{\mathbb{Z}}(X^0, \mathbb{Z})$ is the free $\mathbb{Z}$-module of rank one spanned by $\dfrac{2\check{x}_1 - 3\check{x}_0}{5}$, we also deduce that the map $\mathcal{X}^0 \otimes_{\mathbb{T}^0} \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}^0, \mathbb{Z}) \longrightarrow \mathcal{M}^0$ is surjective.

Taken together, the above calculations establish all our results in the case $p = 11$.

1. The $\mathbb{T}$-module $\mathcal{M}$

As in section 0, we let $\mathcal{M}$ denote the $\mathbb{Z}$-module of modular forms f of weight two on $\Gamma_0(p)$ for which $a_n(f)$ lies in $\mathbb{Z}$ ($n \geq 1$) and $a_0(f)$ lies in $\frac{1}{2}\mathbb{Z}$, and let $\mathbb{T}$ denote the $\mathbb{Z}$-algebra of Hecke operators, which (tautologically from its construction) acts faithfully on $\mathcal{M}$. Also, $\mathcal{M}^0$ denotes the submodule of cusp forms in $\mathcal{M}$ (that is, those f for which $a_0(f) = 0$), and $\mathbb{T}^0$ denotes the quotient of $\mathbb{T}$ that acts faithfully on $\mathcal{M}^0$.

The tensor product $\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Q}$ is naturally identified with the space of weight two modular forms on $\Gamma_0(p)$ all of whose q-expansion coefficients lie in $\mathbb{Q}$. We let $\mathcal{N}$ denote the $\mathbb{T}$-submodule of $\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Q}$ consisting of those f for which $a_n(f)$ lies in $\mathbb{Z}$ when $n \geq 1$, and for notational consistency we will let $\mathcal{N}^0$ denote $\mathcal{M}^0$ when regarded as the submodule of cusp forms in $\mathcal{N}$.

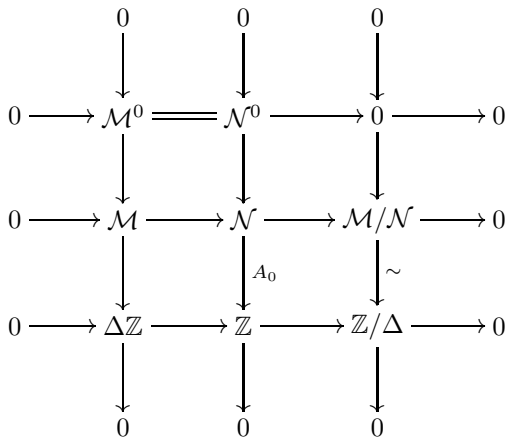
Let $E = \dfrac{p-1}{24} + \displaystyle\sum_{n=1}^{\infty} \sigma'(n) q^n$ (where $\sigma'(n) = \displaystyle\sum_{d|n,(p,d)=1} d$) denote the weight two Eisenstein series on $\Gamma_0(p)$. Then E is a $\mathbb{T}$-eigenform, and so defines a surjection $\mathbb{T} \longrightarrow \mathbb{Z}$ that sends the Hecke operator T_n to the integer $\sigma'(n)$. We let $\mathbb{T}^{\mathrm{Eis}}$ denote $\mathbb{Z}$ regarded as a quotient of $\mathbb{T}$ in this way. We denote by $\mathcal{N}^{\mathrm{Eis}}$ the $\mathbb{T}$-submodule of $\mathcal{N}$ spanned by the Eisenstein series E, and by $\mathcal{M}^{\mathrm{Eis}}$ the intersection $\mathcal{M} \cap \mathcal{N}^{\mathrm{Eis}}$. These are both free modules of rank one over $\mathbb{T}^{\mathrm{Eis}}$, and $\mathcal{M}^{\mathrm{Eis}}$ (respectively $\mathcal{N}^{\mathrm{Eis}}$) is the maximal submodule of $\mathcal{M}$ (respectively $\mathcal{N}$) on which the $\mathbb{T}$-action factors through $\mathbb{T}^{\mathrm{Eis}}$.

We define the positive integers n and Δ to be respectively the numerator and denominator of the fraction $(p-1)/12$, when reduced to lowest terms. Since $a_0(E) = (p-1)/24$, we see immediately that ΔE lies in $\mathcal{M}$, and generates $\mathcal{M}^{\mathrm{Eis}}$.

By definition $\mathcal{N}$ contains $\mathcal{M}$, and since both are finitely generated $\mathbb{Z}$-modules spanning the same $\mathbb{Q}$-vector space, $\mathcal{M}$ has finite index in $\mathcal{N}$. The following result shows that this index is exactly equal to Δ.

Proposition 1.1. *Let $A_0 : \mathcal{N} \longrightarrow \mathbb{Q}$ denote the map $f \mapsto 2\Delta a_0(f)$. Then A_0 is in fact a surjection from $\mathcal{N}$ onto $\mathbb{Z}$, which fits into the following commutative diagram, whose rows and columns are short exact:*

(1.2)



In this diagram, the action of $\mathbb{T}$ on the objects of the bottom row factors through $\mathbb{T}^{\mathrm{Eis}}$.

Proof. If $p = 2$ or 3, then $\mathcal{N} = \mathcal{N}^{\mathrm{Eis}}$ is spanned by E, and $\mathcal{M} = \mathcal{M}^{\mathrm{Eis}}$ is spanned by ΔE. Given this, the truth of the proposition in these cases is immediate. Thus we assume for the remainder of the proof that $p \geq 5$.

We first show that A_0 maps $\mathcal{N}$ into $\mathbb{Z}$. We will use the results of [15, §§ II.4, II.5], which provide a detailed study of the arithmetic of q-expansions of weight two modular forms on $\Gamma_0(p)$. Note that in this reference $B(\mathbb{Z})$ denotes the submodule of $\mathcal{N}$ consisting of modular forms all of whose q-expansion coefficients lie in $\mathbb{Z}$, while $B^0(\mathbb{Z})$ denotes the module we have called $\mathcal{N}^0$. For any ring R, $B(R) = B(\mathbb{Z}) \otimes_{\mathbb{Z}} R$ and $B^0(R) = B^0(\mathbb{Z}) \otimes_{\mathbb{Z}} R$.

Suppose that $f \in N$; write $a_0(f) = a/b$, where a and b are coprime integers. Then $b(p-1)f - 24aE$ is an element of $\mathcal{N}^0$, which is congruent to $-24a\delta \pmod{(p-1)b}$. (Here δ is the formal q-expansion introduced in [15, p. 78].) Thus $-24a\delta$ lies in $B^0(\mathbb{Z}/(p-1)b)$, and from [15, prop. II.5.12] we deduce that $(p-1)b$ divides $24an$. Writing $(p-1) = n(12/\Delta)$, we see that this is equivalent to b dividing $2\Delta a$; since a and b are coprime, we deduce that b divides 2Δ. Thus $A_0(f) = 2\Delta a/b \in \mathbb{Z}$.

The preceding paragraph shows that A_0 is a map $\mathcal{N} \longrightarrow \mathbb{Z}$. Immediately from its definition, we see that $\mathcal{N}^0$ is the kernel of A_0. In order to complete the proof that (1.2) has exact rows and columns we have to show that A_0 yields a surjection of $\mathcal{N}$ onto $\mathbb{Z}$, and restricts to yield a surjection of $\mathcal{M}$ onto $\Delta\mathbb{Z}$.

Note that the Eisenstein series E maps to the integer

$$A_0(E) = 2\Delta a_0(E) = 2\Delta \frac{p-1}{24} = n.$$

On the other hand we can find $g \in \mathcal{M}$ such that $a_0(g) = 1/2$ (via the theta series construction of section 3, for example), and so

$$A_0(g) = 2\Delta a_0(g) = \Delta.$$

Thus we see that the image of $\mathcal{M}$ does equal $\Delta\mathbb{Z}$, while the image of $\mathcal{N}$ contains g.c.d$(n, \Delta) = 1$, and so equals $\mathbb{Z}$.

Finally, we have to show that the action of $\mathbb{T}$ on the bottom row factors through $\mathbb{T}_{\mathrm{Eis}}$. This is perhaps most rapidly seen by tensoring the diagram through with $\mathbb{Q}$ over $\mathbb{Z}$, and using the isomorphism $\mathcal{N}^{\mathrm{Eis}} \otimes_{\mathbb{Z}} \mathbb{Q} \oplus \mathcal{N}^0 \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} \mathcal{N} \otimes_{\mathbb{Z}} \mathbb{Q}$. □

One point of view on the preceding result is as follows: [15, cor. II.5.11 (ii)] shows that if $p \geq 5$ and m is an integer prime to p, then 1 is the q-expansion of a modular form for $\Gamma_0(p)$ over $\mathbb{Z}/m$ if and only if m divides 12. However, this modular form may not lift to a modular form in characteristic zero. (In the terminology of [15], it is a modular form in $\omega^{\otimes 2}$, but not necessarily in $B(\mathbb{Z}/m)$.) Proposition 1.1 shows that 1 *is* the q-expansion of an element of $B(\mathbb{Z}/m)$ if and only if m divides 2Δ.

We will require the duality between modular forms and Hecke operators, which we recall in the following proposition.

Proposition 1.3. (i) *There is a natural isomorphism of* $\mathbb{T}$*-modules*

$$\mathcal{N} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z}),$$

defined by the pairing $\langle f, T \rangle = a_1(f|T)$.

(ii) *There is a natural isomorphism of* $\mathbb{T}^0$*-modules*

$$\mathcal{M}^0 = \mathcal{N}^0 \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}^0, \mathbb{Z}),$$

defined by the same pairing as that of part (i).

Proof. The assertion of (ii) is obtained by specializing [19, thm. 2.2] to the case of $\Gamma_0(p)$. A simple modification of the proof of this theorem yields (i). The key point is that a weight two modular form cannot have a constant q-expansion. □

We now digress slightly, and present a point of view on the results of [15, p. 96] which is in keeping with the arguments of this section.

Consider the injection

$$0 \longrightarrow \mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}} \oplus \mathbb{T}^0. \tag{1.4}$$

This is $\mathbb{Z}$-dual to the injection

$$0 \longrightarrow \mathcal{N}^{\mathrm{Eis}} \oplus \mathcal{N}^0 \longrightarrow \mathcal{N}. \tag{1.5}$$

We also have the short exact sequence

$$0 \longrightarrow \mathcal{N}^0 \longrightarrow \mathcal{N} \xrightarrow{A_0} \mathbb{Z} \longrightarrow 0 \tag{1.6}$$

which makes up the central column of (1.2).

The map $A_0 : \mathcal{N} \longrightarrow \mathbb{Z}$ corresponds by Proposition 1.3 to an element of $\mathbb{T}$, which we denote by t_0, characterized by the property $a_1(f|t_0) = A_0(f) = 2\Delta a_0(f)$ for any $f \in N$. Dualizing (1.6) yields the short exact sequence

$$0 \longrightarrow \mathbb{Z}t_0 \longrightarrow \mathbb{T} \longrightarrow \mathbb{T}^0 \longrightarrow 0. \tag{1.7}$$

We now prove a slightly rephrased version of [15, prop. II.9.7].

Proposition 1.8. (i) *The kernel of the surjection $\mathbb{T} \longrightarrow \mathbb{T}^0$ is principal, generated by t_0.*

(ii) *The element $t_0 - n$ of $\mathbb{T}$ lies in the kernel of the surjection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}}$.*

(iii) *The cokernel of the injection* (1.4) *is cyclic of order n.*

Proof. Claim (i) follows from the exact sequence (1.7). Claim (ii) follows from the fact that $A_0(E) = 2\Delta a_0(E) = n$, while $a_1(E) = 1$. To prove claim (iii), it suffices to prove the same statement for the cokernel of the injection (1.5). A consideration of the short exact sequence (1.6) shows that the cokernel of (1.5) is isomorphic to $A_0(\mathcal{N})/A_0(\mathcal{N}^{\mathrm{Eis}}) = \mathbb{Z}/A_0(E) = \mathbb{Z}/n$. This proves the proposition. □

The idea of using the surjectivity of A_0 to prove statement (i) of the previous proposition arose out of a suggestion of Diamond, and simplifies our original argument.

From Proposition 1.8 (iii) we see that the natural injection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}} \oplus \mathbb{T}^0$ is not an isomorphism unless $n = 1$ (in which case $p = 2$, 3, 5, 7 or 13, and so $\mathbb{T}^0 = 0$); this is the main theme of [15]. We regard $\operatorname{Spec} \mathbb{T}$ as being the union of its closed subschemes $\operatorname{Spec} \mathbb{T}^{\mathrm{Eis}}$ and $\operatorname{Spec} \mathbb{T}^0$. From this optic, the maximal ideals $\mathfrak{m}$ of $\mathbb{T}$ are seen to be of three types. The first type consists of those that lie in $\operatorname{Spec} \mathbb{T} \setminus \operatorname{Spec} \mathbb{T}^{\mathrm{Eis}}$; that is, they are the maximal ideals that induce the unit ideal of $\mathbb{T}^{\mathrm{Eis}}$, but a non-unit ideal of $\mathbb{T}^0$. The second type consists of those that lie in $\operatorname{Spec} \mathbb{T} \setminus \operatorname{Spec} \mathbb{T}^0$; that is, they are the maximal ideals that induce the unit ideal of $\mathbb{T}^0$, but a non-unit ideal of $\mathbb{T}^{\mathrm{Eis}}$. The third type consists of those that lie in the intersection of $\operatorname{Spec} \mathbb{T}^{\mathrm{Eis}}$ and $\operatorname{Spec} \mathbb{T}^0$; that is, they are the maximal ideals that induce a non-unit ideal of both $\mathbb{T}^{\mathrm{Eis}}$ and $\mathbb{T}^0$ (the primes of fusion between $\mathbb{T}^{\mathrm{Eis}}$ and $\mathbb{T}^0$ in $\mathbb{T}$). We refer to the maximal ideals of this third type as the Eisenstein maximal ideals of $\mathbb{T}$. From Proposition 1.8 (iii) we deduce that the residue characteristics of the Eisenstein primes are precisely the prime numbers that divide n. (This

calculation was first carried out in [15, p. 96].) This will be quite important in the arguments to come, as we see already in the next proposition.

Proposition 1.9. *For any maximal ideal $\mathfrak{m}$ of $\mathbb{T}$, the completion $\mathcal{M}_\mathfrak{m}$ is free of rank one as a $\mathbb{T}_\mathfrak{m}$-module if and only if the completion $\mathcal{N}_\mathfrak{m}$ is free of rank one as a $\mathbb{T}_\mathfrak{m}$-module.*

Proof. Let ℓ denote the residue characteristic of $\mathfrak{m}$. If $\mathfrak{m}$ is of the first type (that is, generates the unit ideal of $\mathbb{T}^{\mathrm{Eis}}$), then completing (1.2) at $\mathfrak{m}$ yields an isomorphism $\mathcal{M}_\mathfrak{m} \xrightarrow{\sim} \mathcal{N}_\mathfrak{m}$, and the proposition is clear in this case. If $\mathfrak{m}$ is of the second type (that is, generates the unit ideal of $\mathbb{T}^0$), then completing (1.2) at $\mathfrak{m}$ yields isomorphisms $\mathcal{M}_\mathfrak{m} \xrightarrow{\sim} \Delta\mathbb{Z}_\ell$ and $\mathcal{N}_\mathfrak{m} \xrightarrow{\sim} \mathbb{Z}_\ell$. Thus both are free $\mathbb{T}_\mathfrak{m} \xrightarrow{\sim} \mathbb{T}^{\mathrm{Eis}}_\mathfrak{m} \xrightarrow{\sim} \mathbb{Z}_\ell$-modules of rank one, so that the proposition is also clear in this case. If $\mathfrak{m}$ is an Eisenstein ideal, then ℓ divides n, and so does not divide Δ (since n and Δ are coprime by construction). Thus completing (1.2) at $\mathfrak{m}$ yields an isomorphism $\mathcal{M}_\mathfrak{m} \xrightarrow{\sim} \mathcal{N}_\mathfrak{m}$, and the proposition follows in this case as well. □

The following interpretation of the results of [15] was pointed out to the author by Gross.

Theorem 1.10. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$. Then $\mathbb{T}_\mathfrak{m}$ is Gorenstein if and only if $\mathbb{T}^0_\mathfrak{m}$ is Gorenstein.*

Proof. If $\mathfrak{m}$ is a maximal ideal of the first type, then $\mathbb{T}_\mathfrak{m} \xrightarrow{\sim} \mathbb{T}^0_\mathfrak{m}$, and so the theorem is true in this case. If $\mathfrak{m}$ is a maximal ideal of the second type, then $\mathbb{T}_\mathfrak{m} \xrightarrow{\sim} \mathbb{T}^{\mathrm{Eis}}_\mathfrak{m}$, and so $\mathbb{T}^0_\mathfrak{m} = 0$ (and hence is Gorenstein). On the other hand, if ℓ denotes the residue characteristic of $\mathfrak{m}$, then $\mathbb{T}^{\mathrm{Eis}}_\mathfrak{m} \xrightarrow{\sim} \mathbb{Z}_\ell$. Since this ring is also Gorenstein, the theorem follows in this case.

It remains to treat the case when $\mathfrak{m}$ is Eisenstein. In this case, let I denote the kernel of the map $\mathbb{T}_\mathfrak{m} \longrightarrow \mathbb{T}^{\mathrm{Eis}}_\mathfrak{m}$ and J denote the kernel of the map $\mathbb{T}_\mathfrak{m} \longrightarrow \mathbb{T}^0_\mathfrak{m} \xrightarrow{\sim} \mathbb{Z}_\ell$. Then $I \cap J = 0$, and so $\operatorname{Spec} \mathbb{T}_\mathfrak{m}$ is the scheme-theoretic union of $\operatorname{Spec} \mathbb{T}^{\mathrm{Eis}}_\mathfrak{m}$ and $\operatorname{Spec} \mathbb{T}^0_\mathfrak{m}$. The scheme-theoretic intersection of $\mathbb{T}^{\mathrm{Eis}}_\mathfrak{m}$ and $\mathbb{T}^0_\mathfrak{m}$ is certainly a Cartier divisor on $\operatorname{Spec} \mathbb{T}^{\mathrm{Eis}}_\mathfrak{m} \xrightarrow{\sim} \operatorname{Spec} \mathbb{Z}_\ell$, while [15, thm. II.18.10] implies that it is a Cartier divisor on $\operatorname{Spec} \mathbb{T}^0_\mathfrak{m}$.

It is a general result that if a scheme X is the scheme-theoretic union of two closed subschemes that meet along a common Cartier divisor, then X is Gorenstein if and only if each of these subschemes is Gorenstein. (See Lemma 1.11 below.) Applying this in the above case, we see that $\operatorname{Spec} \mathbb{T}_\mathfrak{m}$ is Gorenstein if and only if $\operatorname{Spec} \mathbb{T}^{\mathrm{Eis}}_\mathfrak{m}$ and $\operatorname{Spec} \mathbb{T}^0_\mathfrak{m}$ are Gorenstein. Since $\operatorname{Spec} \mathbb{T}^{\mathrm{Eis}} \xrightarrow{\sim} \operatorname{Spec} \mathbb{Z}_\ell$ is Gorenstein, the assertion of the theorem follows. □

The following result was explained to the author by Roth. We include a proof for the sake of completeness.

Lemma 1.11. *Let X be a finite-dimensional Noetherian scheme which admits a dualizing complex $\mathcal{F}^\bullet$. Suppose that X_1 and X_2 are two closed subschemes of X such that X is the scheme-theoretic union of X_1 and X_2, and such that the scheme-theoretic intersection $X_1 \cap X_2$ is a Cartier divisor on both X_1 and X_2. Then X is Gorenstein if and only if each of X_1 and X_2 are Gorenstein.*

Proof. Recall that a finite-dimensional connected Noetherian scheme Y with dualizing complex $\mathcal{F}^\bullet_Y$ is Gorenstein if and only if $\mathcal{F}^\bullet_Y$ is quasi-isomorphic to a locally

free $\mathcal{O}_Y$-sheaf of rank one supported in degree $-\dim(Y)$ [10, §V.9]. If Y is Gorenstein and Z is a Cartier divisor on Y, then Z is also Gorenstein (this is true of any local complete intersection in a Gorenstein scheme [10, pp. 143–144]), and $\dim(Z) = \dim(Y) - 1$ (since any Noetherian scheme admitting a dualizing complex is catenary [10, §V.10]). This has the consequence that if two connected Gorenstein subschemes of a fixed ambient scheme meet along a common Cartier divisor, they must be of the same dimension. (We will use this remark below.)

It suffices to prove the lemma after restricting our attention to a sufficiently small neighbourhood of an arbitrary point x of X. Since it is clearly true in the neighbourhood of points in the complement of $X_1 \cap X_2$ (since in such a neighbourhood X is simply the disjoint union of X_1 and X_2), we may in addition assume that x lies in $X_1 \cap X_2$. By shrinking the neighbourhood under consideration, we may and do assume that X_1, X_2 and $X_1 \cap X_2$ are connected.

Write $D = X_1 \cap X_2$. Let $i_1 : X_1 \longrightarrow X$ and $i_2 : X_2 \longrightarrow X$ denote the closed immersions of X_1 and X_2 respectively into X. Let $\mathcal{I}_1$ and $\mathcal{I}_2$ denote the ideal sheaves of $\mathcal{O}_X$ cutting out X_1 and X_2 respectively. Then $\mathcal{I}_1 \cap \mathcal{I}_2 = 0$. (This is the meaning of X being the scheme-theoretic union of X_1 and X_2.) In particular, the natural map $\mathcal{I}_1 \longrightarrow (\mathcal{I}_1 + \mathcal{I}_2)/\mathcal{I}_2$ is an isomorphism. The target of this isomorphism is the ideal of the Cartier divisor D on X_2, and so is a locally free $\mathcal{O}_{X_2}$-module of rank one. Thus $\mathcal{I}_1$ is a locally principal ideal sheaf in $\mathcal{O}_X$, with annihilator equal to $\mathcal{I}_2$. Similarly, $\mathcal{I}_2$ is a locally principal ideal sheaf in $\mathcal{O}_X$, with annihilator equal to $\mathcal{I}_1$. By restricting our attention to a smaller neighbourhood of x, if necessary, we may and do assume that both $\mathcal{I}_1$ and $\mathcal{I}_2$ are in fact principal, generated by sections a_1 and a_2 of $\mathcal{O}_X$ respectively. Thus we have a short exact sequence

$$0 \longrightarrow i_{1*}\mathcal{O}_{X_1} \xrightarrow{\cdot a_2} \mathcal{O}_X \longrightarrow i_{2*}\mathcal{O}_{X_2} \longrightarrow 0, \tag{1.12}$$

and an analogous sequence is obtained by reversing the roles of X_1 and X_2.

If we write $\mathcal{F}_1^\bullet = i_1^! \mathcal{F}^\bullet$ and $\mathcal{F}_2^\bullet = i_2^! \mathcal{F}^\bullet$, then we obtain dualizing complexes on X_1 and X_2 respectively [10, prop. V.2.4]. Applying $RHom(-, \mathcal{F})$ to (1.12) (and remembering that $RHom(j_*\mathcal{O}_Y, \mathcal{F}^\bullet) = j^! \mathcal{F}^\bullet$ for any closed immersion $j : Y \longrightarrow X$ [10, thm. III.8.7(3)]) yields the distinguished triangle

$$\cdots \longrightarrow \mathcal{F}_2^\bullet \longrightarrow \mathcal{F}^\bullet \xrightarrow{\cdot a_2} \mathcal{F}_1^\bullet \longrightarrow \cdots \tag{1.13}$$

in the derived category of coherent $\mathcal{O}_X$-modules. Again, we obtain an analogous distinguished triangle by reversing the roles of X_1 and X_2.

Let us suppose that X_1 and X_2 are Gorenstein. The remark made at the beginning of the proof implies that X_1 and X_2 are of the same dimension, say n (and so X is also of dimension n). Thus $\mathcal{F}_1^\bullet$ and $\mathcal{F}_2^\bullet$ are quasi-isomorphic to rank one locally free sheaves over $\mathcal{O}_{X_1}$ and $\mathcal{O}_{X_2}$ respectively, supported in degree $-n$. Taking the long exact sequence of cohomology corresponding to the distinguished triangle (1.13), we find that $\mathcal{F}^\bullet$ is quasi-isomorphic to a coherent $\mathcal{O}_X$-module supported in degree $-n$, and obtain the short exact sequence

$$0 \longrightarrow \mathcal{H}^{-n}(X_2, \mathcal{F}_2^\bullet) \longrightarrow \mathcal{H}^{-n}(X, \mathcal{F}^\bullet) \xrightarrow{\cdot a_2} \mathcal{H}^{-n}(X_1, \mathcal{F}_1^\bullet) \longrightarrow 0.$$

Reversing the roles of X_1 and X_2 we similarly obtain a short exact sequence

$$0 \longrightarrow \mathcal{H}^{-n}(X_1, \mathcal{F}_1^\bullet) \longrightarrow \mathcal{H}^{-n}(X, \mathcal{F}^\bullet) \xrightarrow{\cdot a_1} \mathcal{H}^{-n}(X_2, \mathcal{F}_2^\bullet) \longrightarrow 0.$$

Combining these two exact sequence, we find that the injection $\mathcal{H}^{-n}(X_1, \mathcal{F}_1^\bullet) \longrightarrow \mathcal{H}^{-n}(X, \mathcal{F}^\bullet)$ identifies $\mathcal{H}^{-n}(X_1, \mathcal{F}_1^\bullet)$ with the annihilator of a_1 in $\mathcal{H}^{-n}(X, \mathcal{F}^\bullet)$, and

also that multiplication by a_2 induces a surjection of $\mathcal{H}^{-n}(X, \mathcal{F}^\bullet)$ onto this annihilator. Again, similar remarks apply after reversing the roles of X_1 and X_2.

If we write $\mathcal{M} = \mathcal{H}^{-n}(X, \mathcal{F}^\bullet)$, then we may summarize our conclusions by observing that we have a short exact sequence $0 \longrightarrow a_2\mathcal{M} \longrightarrow \mathcal{M} \xrightarrow{\cdot a_1} a_1\mathcal{M} \longrightarrow 0$, in which $a_2\mathcal{M}$ is a locally free $\mathcal{O}_{X_1}$-module of rank one, and $a_1\mathcal{M}$ is a locally free $\mathcal{O}_{X_2}$-module of rank one. An elementary application of Nakayama's lemma now implies that $\mathcal{M}$ is locally free of rank one over $\mathcal{O}_X$, and thus that X is Gorenstein in a neighbourhood of x.

The converse implication (that X Gorenstein implies X_1 and X_2 Gorenstein) is proved by a similar consideration of the distinguished triangle (1.13). Since we do not require it in this paper, we omit the details. □

Recall that Mazur has shown that the equivalent conditions of Theorem 1.10 hold in almost all cases. In order to state his result precisely, we recall that if $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ of residue characteristic ℓ, then we say that $\mathfrak{m}$ is ordinary if T_ℓ does not lie in $\mathfrak{m}$; otherwise we say that $\mathfrak{m}$ is supersingular. We remark that if $\mathfrak{m}$ is of the second or third type (that is, induces a non-unit maximal ideal of $\mathbb{T}^{\mathrm{Eis}}$), then $T_\ell \equiv 1 + \ell \equiv 1 \pmod{\mathfrak{m}}$, and so $\mathfrak{m}$ is necessarily ordinary.

Theorem 1.14. *The Hecke algebra $\mathbb{T}^0_{\mathfrak{m}}$ is Gorenstein, except possibly in the case that $\mathfrak{m}$ is of the first type, is ordinary and has residue characteristic two.*

Proof. If $\mathfrak{m}$ is of the first type, then by [15, cor. II.15.2] we see that $\mathbb{T}^0_{\mathfrak{m}}$ is Gorenstein, except in the case excluded in the statement of the theorem. If $\mathfrak{m}$ is of the second type, then $\mathbb{T}^0_{\mathfrak{m}} = 0$ is Gorenstein. If $\mathfrak{m}$ is Eisenstein, then [15, cor. II.16.3] shows that $\mathbb{T}^0_{\mathfrak{m}}$ is Gorenstein. □

As a final result in this section, we state and prove a proposition required in the proof of Theorem 0.6.

Proposition 1.15. *Let I denote the kernel of the surjection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}}$. Then the quotient $\mathcal{M}^0/I$ is isomorphic to $\mathbb{T}^0/I$; in particular, it is of order n.*

Proof. We first note that $\mathbb{T}^0/I$ is isomorphic to the cokernel of (1.4), and so, by part (iii) of Proposition 1.8, is cyclic of order n, while the quotient $\mathcal{M}^0/I$ is isomorphic to $\mathcal{M}^0 \otimes_{\mathbb{T}^0} (\mathbb{T}^0/I)$. Thus both $\mathbb{T}^0/I$ and $\mathcal{M}^0/I$ are $\mathbb{T}^0$-modules of finite order annihilated by I, and hence to prove that they are isomorphic, it suffices to prove that their completions at all the maximal ideals $\mathfrak{m}$ of $\mathbb{T}^0$ containing $I\mathbb{T}^0$ are isomorphic. These are precisely the images in $\mathbb{T}^0$ of the Eisenstein maximal ideals of $\mathbb{T}$, and we must thus show that $\mathcal{M}^0_{\mathfrak{m}}/I$ and $\mathbb{T}^0_{\mathfrak{m}}/I$ are isomorphic as $\mathbb{T}^0_{\mathfrak{m}}$-modules for every Eisenstein maximal ideal $\mathfrak{m}$ of $\mathbb{T}$. This follows immediately from part (ii) of Proposition 1.3 together with [15, cor. II.16.3], which shows that $\mathcal{M}^0_{\mathfrak{m}}$ and $\mathbb{T}^0_{\mathfrak{m}}$ are already isomorphic as $\mathbb{T}^0_{\mathfrak{m}}$-modules. □

2. Some commutative algebra of bilinear pairings

In this section we present some simple commutative algebra that is used in the proof of the theorems of section 0.

We put ourselves in the following situation: A is a commutative ring with identity and B is a commutative A-algebra. We begin by recalling some adjointness isomorphisms involving Hom and $\otimes$.

For the first isomorphism, let U and V be B-modules, and let W be an A-module: then we have an isomorphism

$$\mathrm{Hom}_A(U \otimes_B V, W) \xrightarrow{\sim} \mathrm{Hom}_B(V, \mathrm{Hom}_A(U, W)), \tag{2.1}$$

defined by sending a morphism ϕ in the source to the morphism $v \mapsto (u \mapsto \phi(u \otimes v))$ in the target. For the second isomorphism, let W be a B-module: then we have an isomorphism

$$\mathrm{Hom}_A(W, A) \xrightarrow{\sim} \mathrm{Hom}_B(W, \mathrm{Hom}_A(B, A)), \tag{2.2}$$

defined by sending a morphism ϕ in the source to the morphism $w \mapsto (b \mapsto \phi(bw))$ in the target. (Given the preceding descriptions of these maps, it is immediate to check that both are indeed isomorphisms.)

Let us now fix a pair U,V of B-modules. We have the following diagram:

$$\begin{array}{ccc} \mathrm{Hom}_A(U \otimes_B V, A) & \xrightarrow{\quad\sim\quad} & \mathrm{Hom}_B(V, \mathrm{Hom}_A(U, A)) \\ \downarrow \sim & & \downarrow \sim \\ \mathrm{Hom}_B(U \otimes_B V, \mathrm{Hom}_A(B, A)) & \xrightarrow{\sim} & \mathrm{Hom}_B(V, \mathrm{Hom}_B(U, \mathrm{Hom}_A(B, A))) \end{array} \tag{2.3}$$

The left (respectively right) vertical arrow of this diagram is obtained from (2.2) by taking W to be $U \otimes_B V$ (respectively U). The top arrow is obtained from (2.1) by taking W to be A, and the bottom arrow is obtained from (2.1) by replacing A with B and taking W to be $\mathrm{Hom}_A(B, A)$. One easily checks that (2.3) commutes.

By the definition of tensor product, the elements of $\mathrm{Hom}_A(U \otimes_B V, A)$ correspond to B-bilinear pairings $\langle\, , \rangle : U \times V \longrightarrow A$. Suppose given such a pairing. The corresponding element $\phi_A \in \mathrm{Hom}_A(U \otimes_B V, A)$ gives rise via (2.3) to morphisms $\phi_B \in \mathrm{Hom}_B(U \otimes_B V, \mathrm{Hom}_A(B, A))$, $\chi_A \in \mathrm{Hom}_B(V, \mathrm{Hom}_A(U, A))$, and $\chi_B \in \mathrm{Hom}_B(V, \mathrm{Hom}_B(U, \mathrm{Hom}_A(B, A)))$.

For the remainder of this section we keep ourselves in the above situation, and in addition assume as a running hypothesis that B, U and V are all locally free of finite rank as A-modules. The first result that we prove will give necessary and sufficient conditions for the morphism ϕ_B to be surjective, under the assumption that the pairing $\langle\, , \rangle$ is perfect.

Lemma 2.4. *In the setting described above, suppose that the pairing $\langle\, , \rangle : U \times V \longrightarrow A$ is a perfect B-bilinear pairing of locally free A-modules of finite rank (that is, suppose that the morphism χ_A is an isomorphism of B-modules). Then the morphism $\phi_B : U \otimes_B V \longrightarrow \mathrm{Hom}_A(B, A)$ is surjective if and only if $U/\mathfrak{m}$ is a faithful $B/\mathfrak{m}$-module for each maximal ideal $\mathfrak{m}$ of A.*

Proof. Since B is finitely generated over A, the morphism ϕ_B is surjective if and only if the corresponding morphism $\phi_B/\mathfrak{m} : U/\mathfrak{m} \otimes_{B/\mathfrak{m}} V/\mathfrak{m} \longrightarrow \mathrm{Hom}_A(B, A)/\mathfrak{m}$ obtained by tensoring ϕ_B through with $A/\mathfrak{m}$ over A is surjective, for each maximal ideal $\mathfrak{m}$ of A.

Since B is locally free over A, reduction modulo $\mathfrak{m}$ yields an isomorphism

$$\mathrm{Hom}_A(B, A)/\mathfrak{m} \xrightarrow{\sim} \mathrm{Hom}_{A/\mathfrak{m}}(B/\mathfrak{m}, A/\mathfrak{m}).$$

Composing $\phi_B/\mathfrak{m}$ with this isomorphism we obtain a morphism $\phi_{B/\mathfrak{m}} : U/\mathfrak{m} \otimes_{B/\mathfrak{m}} V/\mathfrak{m} \longrightarrow \mathrm{Hom}_{A/\mathfrak{m}}(B/\mathfrak{m}, A/\mathfrak{m})$. This corresponds via the diagram (2.3) (with A replaced by $A/\mathfrak{m}$, B replaced by $B/\mathfrak{m}$, U replaced by $U/\mathfrak{m}$ and V replaced by $V/\mathfrak{m}$) to the morphism $\phi_{A/\mathfrak{m}} = \phi_A/\mathfrak{m} : U/\mathfrak{m} \otimes_{B/\mathfrak{m}} V/\mathfrak{m} \longrightarrow A/\mathfrak{m}$ obtained by

tensoring ϕ_A through with $A/\mathfrak{m}$ over A. Since U is locally free over A, there is similarly an isomorphism $\mathrm{Hom}_A(U,A)/\mathfrak{m} \xrightarrow{\sim} \mathrm{Hom}_{A/\mathfrak{m}}(U/\mathfrak{m}, A/\mathfrak{m})$, and composing this with the morphism $\chi_A/\mathfrak{m} : V/\mathfrak{m} \longrightarrow \mathrm{Hom}_A(U,A)/\mathfrak{m}$ we obtain a morphism $\chi_{A/\mathfrak{m}} : V/\mathfrak{m} \longrightarrow \mathrm{Hom}_{A/\mathfrak{m}}(U/\mathfrak{m}, A/\mathfrak{m})$, which also corresponds via (2.3) (again with A replaced by $A/\mathfrak{m}$, and so on) to the morphism $\phi_{A/\mathfrak{m}}$. Since χ_A is assumed to be an isomorphism, we see that the same is true of $\chi_{A/\mathfrak{m}}$. Putting these observations together with that of the preceding paragraph, we see that it suffices to prove the lemma with A replaced by $A/\mathfrak{m}$, B by $B/\mathfrak{m}$, U by $U/\mathfrak{m}$ and V by $V/\mathfrak{m}$. Thus for the rest of the proof we assume that A is a field.

By assumption χ_A induces an isomorphism $V \xrightarrow{\sim} \mathrm{Hom}_A(U,A)$ of B-modules, and so it suffices to prove the lemma in the case when $V = \mathrm{Hom}_A(U,A)$ and ϕ_A corresponds to the tautological pairing $U \times \mathrm{Hom}_A(U,A) \longrightarrow A$. Thus in addition to assuming that A is a field, we assume that $V = \mathrm{Hom}_A(U,A)$ from now on.

Now $\phi_B : U \otimes_B \mathrm{Hom}_A(U,A) \longrightarrow \mathrm{Hom}_A(B,A)$ is surjective if and only if the A-dual morphism $B \longrightarrow \mathrm{Hom}_A(U \otimes_B \mathrm{Hom}_A(U,A), A)$ is injective. Composing this morphism with the adjointness isomorphism (2.1) (taking V to be $\mathrm{Hom}_A(U,A)$ and W to be A), we obtain a morphism

$$B \longrightarrow \mathrm{Hom}_B(\mathrm{Hom}_A(U,A), \mathrm{Hom}_A(U,A)), \tag{2.5}$$

which is thus injective precisely when ϕ_B is surjective. One immediately checks that (2.5) is the canonical morphism describing the B-module structure on $\mathrm{Hom}_A(U,A)$, and so it is injective precisely when $\mathrm{Hom}_A(U,A)$ is a faithful B-module. Since $\mathrm{Hom}_A(U,A)$ is a faithful B-module precisely when U is a faithful B-module, this completes the proof of the lemma. □

One example of a situation in which the faithfulness condition of Lemma 2.4 holds is the case when U is a locally free B-module of finite positive rank. The following lemma analyzes the case when A is a discrete valuation ring, and U is assumed to be locally free as a B-module only over the generic point of $\mathrm{Spec}\, A$.

Lemma 2.6. *In addition to our running hypotheses, suppose that A is a discrete valuation ring with uniformizer π and field of fractions K, and that $U \otimes_A K$ is free of finite rank as a $B \otimes_A K$-module. Then U/π is a faithful B/π-module if and only if the natural map from B to the centre of the endomorphism ring $\mathrm{End}_B(U,U)$ is an isomorphism.*

Proof. We begin with some remarks concerning the structure of $\mathrm{End}_A(U,U)$ and its subring $\mathrm{End}_B(U,U)$. Since U is free of finite rank over A, the former ring is a matrix ring over A. In particular it is torsion-free and its reduction modulo π acts faithfully on the reduction U/π. More generally, if R is any A-subalgebra of $\mathrm{End}_A(U,U)$, note that R/π acts faithfully on U/π if and only if R is saturated in $\mathrm{End}_A(U,U)$.

We let Z denote the centre of $\mathrm{End}_B(U,U)$. Both Z and $\mathrm{End}_B(U,U)$ are in particular A-submodules of the matrix ring $\mathrm{End}_A(U,U)$, and so are free of finite rank as A-modules. Also, they are both saturated in $\mathrm{End}_A(U,U)$, since U is torsion-free.

The action of B on U induces a morphism $\iota : B \longrightarrow Z$ (the natural map referred to in the statement of the lemma). Tensoring ι with K over A yields the analogous morphism of $B \otimes_A K$ into the centre of $\mathrm{End}_{B \otimes_A K}(U \otimes_A K, U \otimes_A K)$. By assumption $U \otimes_A K$ is a free $B \otimes_A K$-module of finite rank, and so its endomorphism ring is a

matrix ring over B. Since the centre of such a ring is just B itself, we conclude that ι becomes an isomorphism after tensoring with K over A. Furthermore, the source and target of ι are both free A-modules of finite rank, the source by assumption and the target by the observations of the preceding paragraph. Thus we conclude that ι is an injection, with torsion cokernel.

With these preliminaries complete, it is easy to prove the lemma. The morphism ι is an isomorphism if and only if its cokernel is torsion free (since this cokernel would then be both torsion and torsion-free, and so trivial). This cokernel is torsion free if and only if $\iota(B)$ is saturated in Z. Since Z is saturated in $\mathrm{End}_A(U,U)$, we see that ι is an isomorphism if and only if $\iota(B)$ is saturated in $\mathrm{End}_A(U,U)$. The lemma follows once we recall that $\iota(B)$ is saturated in $\mathrm{End}_A(U,U)$ if and only if B/π acts faithfully on U/π. □

The rest of this section is devoted to presenting criteria for computing the cokernel of ϕ_B, in situations where it may not be surjective (for example, because the pairing giving rise to ϕ_A is not perfect).

We add to our running hypotheses the assumption that A is a complete local ring. Since B is locally free of finite rank as an A-module, this implies that B decomposes as the direct sum of completions $B_{\mathfrak{n}}$, where $\mathfrak{n}$ ranges over the (finitely many) maximal ideals of B. For any such maximal ideal $\mathfrak{n}$, we let $U_{\mathfrak{n}}$ and $V_{\mathfrak{n}}$ denote the completions of U and V at $\mathfrak{n}$. Then U and V also decompose as the direct sums of their completions.

Lemma 2.7. *Suppose, in addition to our running hypotheses, that for any maximal ideal $\mathfrak{n}$ of B at least one of the following two conditions holds:*

(i) *the morphisms $U_{\mathfrak{n}} \otimes_{B_{\mathfrak{n}}} V_{\mathfrak{n}} \longrightarrow \mathrm{Hom}_A(B_{\mathfrak{n}}, A)$ induced by ϕ_B and $V_{\mathfrak{n}} \longrightarrow \mathrm{Hom}_A(U_{\mathfrak{n}}, A)$ induced by χ_A are both surjective;*

(ii) *the $B_{\mathfrak{n}}$-module $U_{\mathfrak{n}}$ is free of rank one.*

Then the cokernel of the morphism ϕ_B is isomorphic to the cokernel of the morphism χ_A.

Proof. Writing $B \xrightarrow{\sim} \bigoplus_{\mathfrak{n}} B_{\mathfrak{n}}$, $U \xrightarrow{\sim} \bigoplus_{\mathfrak{n}} U_{\mathfrak{n}}$, and $V \xrightarrow{\sim} \bigoplus_{\mathfrak{n}} V_{\mathfrak{n}}$, we see that the cokernels of ϕ_B and χ_A also decompose as such direct sums, and so it suffices to verify the lemma after replacing B by one of the $B_{\mathfrak{n}}$ and U and V by the corresponding $U_{\mathfrak{n}}$ and $V_{\mathfrak{n}}$. Thus we may assume that either ϕ_B and χ_A are surjections, or that U is a free B-module of rank one.

In the first case, both ϕ_B and χ_A have trivial cokernels, and so the lemma holds in this case.

In the second case, note that the morphism χ_B is equal to the composition of χ_A with the isomorphism $\mathrm{Hom}_A(U, A) \xrightarrow{\sim} \mathrm{Hom}_B(U, \mathrm{Hom}_A(B, A))$. Thus the cokernel of χ_A is isomorphic to the cokernel of χ_B. In addition, the morphism χ_B can be thought of as being obtained from the morphism ϕ_B by tensoring over B with the B-dual of the B-module U (which we are assuming to be free of rank one). Thus the cokernel of ϕ_B is isomorphic to the cokernel of χ_B, and so to the cokernel of χ_A, proving the lemma in this case. □

For ease of future reference, we recall our notation and running hypotheses. We are given a complete local ring A, an A-algebra B which is free of finite rank as an A-module, and a pair of B-modules U and V which are free of finite rank as A-modules. Furthermore, there is a B-bilinear pairing $U \times V \to A$, which induces tautological maps of B-modules $\chi_A : V \to \mathrm{Hom}_A(U, A)$ and $\phi_B : U \otimes_B V \to \mathrm{Hom}_A(B, A)$.

Proposition 2.8. *Suppose, in addition to our running hypotheses, that for any maximal ideal $\mathfrak{n}$ of B at least one of the following two conditions holds:*

(i) *the pairing $U_\mathfrak{n} \times V_\mathfrak{n} \longrightarrow A$ is perfect, and $U_\mathfrak{n}/\mathfrak{m}$ is a faithful $A/\mathfrak{m}$-module (here $\mathfrak{m}$ denotes the maximal ideal of A);*

(ii) *the $B_\mathfrak{n}$-module $U_\mathfrak{n}$ is free of rank one.*

Then the cokernel of the morphism ϕ_B is isomorphic to the cokernel of the morphism χ_A.

Proof. The pairing $U_\mathfrak{n} \times V_\mathfrak{n} \longrightarrow A$ is perfect if and only if the morphism $V_\mathfrak{n} \longrightarrow \mathrm{Hom}_A(U_\mathfrak{n}, A)$ induced by χ_A is an isomorphism. Thus Lemma 2.4 (with U, V and B replaced by $U_\mathfrak{n}$, $V_\mathfrak{n}$ and $B_\mathfrak{n}$) implies that condition (i) of the present proposition implies condition (i) of Lemma 2.7. Since condition (ii) of the present proposition is identical to that of Lemma 2.7, the proposition is now seen to follow from that lemma. □

3. The $\mathbb{T}$-module $\mathcal{X}$. Constructions

Let $\mathcal{S}$ denote the set of singular points of the geometric fibre of $X_0(p)$ in characteristic p. As in section 0 we write $\mathcal{S} = \{x_0, \ldots, x_g\}$ (where g is equal to the genus of $X_0(p)$). The set $\mathcal{S}$ is in bijection with the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and for each point $x_i \in \mathcal{S}$ we let E_i denote a supersingular curve representing the isomorphism class corresponding to x_i.

Let $\mathcal{X}$ denote the free $\mathbb{Z}$-module on the set $\mathcal{S}$, let $\deg : \mathcal{X} \longrightarrow \mathbb{Z}$ denote the $\mathbb{Z}$-linear map obtained by sending each $x_i \in \mathcal{S}$ to $1 \in \mathbb{Z}$, and let $\mathcal{X}^0$ denote the kernel of deg. The Hecke correspondences on $X_0(p)$ induce endomorphisms of $\mathcal{X}$ and of $\mathcal{X}^0$. (See [20, pp. 443–445] for a detailed discussion of these correspondences.)

Theorem 3.1. (i) *The action of the Hecke correspondences on $\mathbb{Z}$, regarded as the quotient $\mathcal{X}/\mathcal{X}^0$, factors through $\mathbb{T}^{\mathrm{Eis}}$. That is, the Hecke operator T_n acts as multiplication by $\sigma'(n)$.*

(ii) *The action of the Hecke correspondences on $\mathcal{X}^0$ makes $\mathcal{X}^0$ a faithful $\mathbb{T}^0$-module.*

(iii) *The action of the Hecke correspondences on $\mathcal{X}$ makes $\mathcal{X}$ a faithful $\mathbb{T}$-module.*

Proof. Let $\mathbb{T}'$ denote the polynomial ring over $\mathbb{Z}$ on the countably many generators T_n. The action of the Hecke correspondences on $\mathcal{X}$ induces an action of $\mathbb{T}'$ on $\mathcal{X}$.

Let I' denote the kernel of the surjection of $\mathbb{T}'$ onto $\mathbb{T}^{\mathrm{Eis}}$, and let J' denote the kernel of the surjection of $\mathbb{T}'$ onto $\mathbb{T}^0$. Then $I' \cap J'$ is the kernel of the surjection $\mathbb{T}' \longrightarrow \mathbb{T}$, since the map $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}} \oplus \mathbb{T}^0$ is injective. Furthermore, since the cokernel of this map is finite of order n, we see that $n\mathbb{T}' \subset I' + J'$, and hence that $n(I' \cap J') \subset I'J'$.

If we prove (i) and (ii), then we conclude immediately that $\mathrm{Ann}_{\mathbb{T}'}(\mathcal{X}) \subset I' \cap J'$; a consideration of the exact sequence $0 \longrightarrow \mathcal{X}^0 \longrightarrow \mathcal{X} \longrightarrow \mathbb{Z} \longrightarrow 0$ shows in addition that $I'J' \subset \mathrm{Ann}_{\mathbb{T}'}(\mathcal{X})$. Taking into account the inclusion $n(I' \cap J') \subset I'J'$ and the fact that $\mathcal{X}$ is $\mathbb{Z}$-torsion free, we deduce that $I' \cap J' = \mathrm{Ann}_{\mathbb{T}'}(\mathcal{X})$. This is the claim of (iii).

For any $x_i \in \mathcal{S}$, $\deg(T_n x_i) = \sigma'(n)$. Thus the action of $\mathbb{T}'$ on $\mathbb{Z}$ (as it appears in the preceding exact sequence) kills I', and yields a faithful action of $\mathbb{T}'/I' \xrightarrow{\sim} \mathbb{T}^{\mathrm{Eis}}$ on $\mathbb{Z}$. This proves (i).

Let $T_0(p)$ denote the torus that is the connected component of the fibre in characteristic p of the Néron model of the Jacobian $J_0(p)$ of $X_0(p)$. The Hecke correspondences act on $T_0(p)$ functorially via their action on $J_0(p)$, and hence also act on the character lattice $\mathrm{Hom}(T_0(p)_{/\overline{\mathbb{F}}_p}, \mathbb{G}_{m/\overline{\mathbb{F}}_p})$ of $T_0(p)$. Furthermore (a) there is a canonical isomorphism (of Hecke modules) of $\mathcal{X}^0$ with this character lattice; (b) we can recover the Hecke action on $T_0(p)$ from the Hecke action on its character lattice; (c) the endomorphisms of $J_0(p)$ act faithfully on its toric reduction $T_0(p)$; (d) we can recover the Hecke action on cusp forms from the Hecke action on $J_0(p)$ by passing to its cotangent space. Thus the annihilator of the $\mathbb{T}'$-action on $\mathcal{X}^0$ is equal to the annihilator of the $\mathbb{T}'$-action on the space of weight two cusp forms on $\Gamma_0(p)$, which is J'. This proves (ii). (This is a particular case of [20, thm. 3.10].) □

Remark. A more natural way to prove part (iii) of this theorem, without studying separately the Eisenstein and cuspidal parts of $\mathcal{X}$, would be to observe that $\mathcal{X}$ is the character group of the connected component of the fibre in characteristic p of the Néron model of the generalized Jacobian of the non-proper curve $Y_0(p) = X_0(p) \setminus$ cusps, and that the Hecke action on this semi-abelian variety factors faithfully through $\mathbb{T}$.

Corollary 3.2. *$\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a free $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$-module of rank one.*

Proof. It follows from Theorem 3.1 that $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a faithful $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$-module. Also $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a semi-simple $\mathbb{Q}$-algebra. (This is proved by noting that $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{R}$ acts faithfully as an algebra of self-adjoint operators on a finite-dimensional vector space equipped with a positive definite inner product. One can use the vector space $M \otimes_{\mathbb{Z}} \mathbb{R}$ equipped with the Petersson inner product, as in [1], or the space $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{R}$ equipped with the inner product induced by Definition 3.4 below, as in [6, prop. 2.7 (7)].) Furthermore, $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q}$ are of the same dimension $(= g + 1)$ over $\mathbb{Q}$. These observations suffice to prove the corollary. □

For each $x_i \in \mathcal{S}$ we let e_i denote one half of the number of automorphisms of E_i. The following lemma is pointed out in [6, p. 117]. (Recall that Δ denotes the denominator of $(p-1)/12$ when this fraction is written in lowest terms.)

Lemma 3.3. *The product $\prod_{i=0}^{g} e_i$ is equal to Δ.*

Proof. This follows from the well-known explicit calculation of the e_i, which we recall. If $p = 2$ (respectively $p = 3$), then $j = 0$ is the unique supersingular j-invariant, and the corresponding elliptic curve has 24 (respectively 12) automorphisms. If $(p, 6) = 1$, then $e_i = 1$ unless $j(E_i) = 0$ (respectively $j(E_i) = 1728$), in which case $e_i = 3$ (respectively $e_i = 2$); furthermore, this j-value actually is supersingular in characteristic p if and only if $p \equiv -1 \pmod 3$ (respectively $p \equiv -1 \pmod 4$). □

Definition 3.4. We define a symmetric pairing on $\mathcal{X}$ via the formula

$$\langle x_i, x_j \rangle = e_i \delta_{i,j} = e_j \delta_{i,j} = \text{ one-half the number of isomorphisms from } E_i \text{ to } E_j.$$

If we restrict this pairing to the submodule $\mathcal{X}^0$ of $\mathcal{X}$, we obtain the Picard-Lefschetz pairing discussed in [20, §§ 2 and 3].

We now prove a series of results relating this pairing to the theta series of quadratic spaces constructed from the supersingular elliptic curves E_i. There is some

overlap with the results of [6]; in particular, Proposition 3.6, Lemmas 3.7 and 3.8, and Corollary 3.9 are essentially contained in sections 2, 4 and 5 of this reference, although the point of view is different. (In [6], the lattice $\mathcal{X}$ is considered as the Picard group of a certain curve obtained as the disjoint union of genus zero curves. Regarding notation, note that in [6] this curve is denoted by X, while the lattice we denote by $\mathcal{X}$ is denoted by $\mathrm{Pic}(X)$. It might also be useful to observe that the lattice we denote by $\mathcal{X}$ is denoted by Λ in [20], and that the lattice we denote by $\mathcal{X}^0$ is denoted by X in that reference.)

We begin by recalling a construction from [6] and [8]:

Definition 3.5. For each pair of elements x_i and x_j of $\mathcal{S}$, let $L_{i,j}$ denote the quadratic space whose underlying $\mathbb{Z}$-module is the space of isogenies from E_i to E_j, equipped with the quadratic form $\phi \mapsto \deg(\phi)$. (Here and below we adopt the usual convention that if $\phi = 0$, then $\deg(\phi) = 0$.)

Proposition 3.6. *For any two elements x_i and x_j of $\mathcal{S}$, $L_{i,j}$ is a free $\mathbb{Z}$-module of rank 4 equipped with a positive definite quadratic form.*

Proof. Since any two supersingular elliptic curves in characteristic p are isogenous, we see that the rank of $L_{i,j}$ as a $\mathbb{Z}$-module is equal to the rank of $L_{i,i}$ for any choice of i, and this rank is 4, since the endomorphisms of a supersingular elliptic curve form an order in a quaternion algebra over $\mathbb{Q}$. That taking degrees yields a definite quadratic form is immediate from the fact that an isogeny of degree zero must be the zero isogeny. □

Lemma 3.7. *For any two elements x_i and x_j of $\mathcal{S}$ there is a natural isomorphism of quadratic spaces $L_{i,j} \xrightarrow{\sim} L_{j,i}$.*

Proof. The required isomorphism is obtained by sending any isogeny from E_i to E_j, of some degree n say, to its dual isogeny, which maps from E_j to E_i, and is also of degree n. □

If n is any natural number, let $r_n(L_{i,j})$ denote the number of elements of $L_{i,j}$ of degree n.

Lemma 3.8. *If x_i and x_j are any two elements of $\mathcal{S}$, then*

$$\begin{aligned}\langle T_n x_i, x_j\rangle &= \text{ one-half the number of degree } n \text{ isogenies from } E_i \text{ to } E_j \\ &= \frac{1}{2} r_n(L_{i,j}).\end{aligned}$$

Proof. Since $T_n x_i$ is the formal sum of all curves that are the image of E_i under an n-isogeny, and since $\langle x_k, x_j\rangle$ equals one half the number of isomorphisms from E_k to E_j, for any index k, we see that $\langle T_n x_i, x_j\rangle$ does indeed equal one-half the number of degree n isogenies from E_i to E_j, as claimed. □

Corollary 3.9. *The pairing of Definition* 3.4 *is $\mathbb{T}$-bilinear. That is, for any $x, y \in \mathcal{X}$ and any $T \in \mathbb{T}$, $\langle Tx, y\rangle = \langle x, Ty\rangle$.*

Proof. It suffices to verify this when $x = x_i$ and $y = y_j$ are elements of $\mathcal{S}$ and $T = T_n$ for some natural number n. In this case Lemmas 3.7 and 3.8 show that $\langle T_n x_i, x_j\rangle = \frac{1}{2} r_n(L_{i,j}) = \frac{1}{2} r_n(L_{j,i}) = \langle T_n x_j, x_i\rangle = \langle x_i, T_n x_j\rangle$. □

Corollary 3.9 shows that we are in the situation of section 2 (taking A to be $\mathbb{Z}$, B to be $\mathbb{T}$ and $U = V$ to be $\mathcal{X}$). In particular the pairing of Definition 3.4 yields a morphism of $\mathbb{Z}$-modules $\mathcal{X} \otimes_{\mathbb{T}} \mathcal{X} \longrightarrow \mathbb{Z}$ (the morphism denoted ϕ_A in section 2) and a corresponding morphism of $\mathbb{T}$-modules

$$\mathcal{X} \otimes_{\mathbb{T}} \mathcal{X} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z}) \tag{3.10}$$

(the morphism denoted ϕ_B in section 2). Composing (3.10) with the isomorphism of Proposition 1.3 (ii) we obtain a morphism $\theta : \mathcal{X} \otimes_{\mathbb{T}} \mathcal{X} \longrightarrow \mathcal{N}$. From the definition of the pairing of Proposition 1.3 and the construction of (3.10) we see that the map θ is determined by the formula $a_n(\theta(x \otimes x')) = \langle T_n x, x' \rangle$, for $x, x' \in \mathcal{X}$ and $n \geq 1$. The following results are devoted to computing the map θ, and in particular, will explain our choice of notation for this map.

Proposition 3.11. *If x_i and x_j are any two elements of $\mathcal{S}$, then for any $n \geq 1$, we have $a_n(\theta(x_i \otimes x_j)) = \frac{1}{2} r_n(L_{i,j})$.*

Proof. Combining the above discussion with Lemma 3.8 we see that if $n \geq 1$, then $a_n(\theta(x_i \otimes x_j)) = \langle T_n x_i, x_j \rangle = \frac{1}{2} r_n(L_{i,j})$. □

Definition 3.12. Let $\mathbf{x}$ denote the element of $\mathcal{X}$ defined by $\mathbf{x} = \Delta \sum_{i=0}^{g} \frac{x_i}{e_i}$. (Note that Lemma 3.3 implies that this is an element of $\mathcal{X}$.)

This is the element denoted by e_0 in [6, (4.8)]. Observe that $\langle \mathbf{x}, x_i \rangle = \Delta$ for each element x_i of $\mathcal{S}$. Thus $\langle \mathbf{x}, x \rangle = \Delta \deg(x)$, for any $x \in \mathcal{X}$.

Let $\mathcal{X}^{\mathrm{Eis}}$ denote the maximal $\mathbb{T}$-submodule of $\mathcal{X}$ on which the action of $\mathbb{T}$ factors through $\mathbb{T}^{\mathrm{Eis}}$. The short exact sequence $0 \longrightarrow \mathcal{X}^0 \longrightarrow \mathcal{X} \longrightarrow \mathbb{Z} \longrightarrow 0$ along with parts (i) and (ii) of Theorem 3.1 shows that $\mathcal{X}^{\mathrm{Eis}}$ must be a rank one $\mathbb{Z}$-submodule of $\mathcal{X}$.

Lemma 3.13. *$\mathcal{X}^{\mathrm{Eis}}$ is the free $\mathbb{Z}$-module of rank one generated by $\mathbf{x}$.*

Proof. For any element x_j of $\mathcal{S}$, we compute that

$$\begin{aligned}\langle T_n \mathbf{x}, x_j \rangle = \langle \mathbf{x}, T_n x_j \rangle &= \Delta \sum_i \frac{\langle x_i, T_n x_j \rangle}{e_i} \\ &= \Delta \sum_i \text{ number of } n\text{-isogenies with source } E_j \text{ and target isomorphic to } E_i \\ &= \Delta \times \text{ number of } n\text{-isogenies with source } E_j = \Delta \sigma'(n).\end{aligned}$$

Thus the coefficient of x_j in $T_n \mathbf{x}$ must be $\Delta \sigma'(n)/e_j$. Since j was arbitrary, we find that $T_n \mathbf{x} = \sigma'(n) \mathbf{x}$. Thus $\mathbf{x}$ lies in $\mathcal{X}^{\mathrm{Eis}}$.

Now $\mathcal{X}^{\mathrm{Eis}}$ is free of rank one over $\mathbb{Z}$, and the coefficients Δ/e_i of the generators x_i of $\mathcal{X}$ in $\mathbf{x}$ are coprime elements of $\mathbb{Z}$ (as follows from Lemma 3.3 and the explicit values of the numbers e_i which are recalled in the course of its proof). Thus we see that $\mathbf{x}$ is not divisible by any non-unit element of $\mathbb{Z}$ in $\mathcal{X}$, and so it must generate $\mathcal{X}^{\mathrm{Eis}}$. □

Proposition 3.14. *Let x_i be any element of $\mathcal{S}$. Then $\theta(\mathbf{x} \otimes x_i)$ is equal to the modular form ΔE.*

Proof. Similarly to the proof of Proposition 3.11, we compute

$$a_n(\theta(\mathbf{x} \otimes x_i)) = \langle T_n \mathbf{x}, x_i \rangle = \langle \sigma'(n)\mathbf{x}, x_i \rangle = \Delta\sigma'(n),$$

since $\langle \mathbf{x}, x_i \rangle = \Delta$ for each generator x_i of $\mathcal{X}$. □

Proposition 3.15. *The following statements hold:*

(i) *if x_i and x_j are any two elements of $\mathcal{S}$, then $a_0(\theta(x_i \otimes x_j)) = \frac{1}{2}$;*

(ii) *for any two elements x, $y \in \mathcal{X}$, the constant term of $\theta(x \otimes y)$ is equal to $(\deg(x)\deg(y))/2$;*

(iii) *if x_i and x_j are any two elements of $\mathcal{S}$, then $\theta(x_i \otimes x_j) = \frac{1}{2}\Theta(L_{i,j})$;*

(iv) $a_0(E) = \sum_i \frac{1}{2e_i}$;

(v) $\deg \mathbf{x} = n$;

(vi) $\sum_i \frac{1}{e_i} = \frac{p-1}{12}$.

Proof. We begin by proving that the six statements are mutually equivalent. Since the formation of $a_0(\theta(x \otimes y))$ and $(\deg(x)\deg(y))/2$ are both bilinear in x and y, statements (i) and (ii) are clearly equivalent. Proposition 3.11 together with the fact that $a_0(\Theta(L_{i,j})) = 1$ shows that statements (i) and (iii) are equivalent. Since $\deg(\mathbf{x}) = \Delta \sum_i \frac{1}{e_i}$ and $a_0(E) = (p-1)/24 = n/2\Delta$, we see that statements (iv), (v) and (vi) are equivalent.

We now show that statements (i) and (iv) are equivalent. To this end, we observe that

$$a_0(\theta(x_i \otimes x_j)) = \frac{1}{\deg(\mathbf{x})}\left(a_0(\theta(\mathbf{x} \otimes x_j)) + a_0(\theta((\deg(\mathbf{x})x_i - \mathbf{x}) \otimes x_j))\right).$$

Note that $\deg(\mathbf{x})x_i - \mathbf{x}$ lies in $\mathcal{X}^0$, which implies that $\theta((\deg(\mathbf{x})x_i - \mathbf{x}) \otimes x_j)$ lies in $\mathcal{M}^0$, and so has vanishing constant term. Proposition 3.14 asserts that $\theta(\mathbf{x} \otimes x_i) = \Delta E$. Thus we find that

$$a_0(E) = \frac{\deg(\mathbf{x}) a_0(\theta(x_i \otimes x_j))}{\Delta} = a_0(\theta(x_i \otimes x_j)) \sum_i \frac{1}{e_i},$$

which makes it clear that statements (i) and (iv) are equivalent.

It remains to see that these statements actually hold. There are at least two ways to do this. For example, it is a classical theorem that the theta-series $\Theta(L_{i,j})$ are weight two modular forms on $\Gamma_0(p)$. The formula of Proposition 3.11 then shows that $\theta(x_i \otimes x_j)$ and $\frac{1}{2}\Theta(L_{i,j})$ coincide up to their constant terms, and so coincide. Thus $a_0(\theta(x_i \otimes x_j)) = \frac{1}{2}a_0(\Theta(L_{i,j})) = \frac{1}{2}$, proving part (i) of Proposition 3.15. Alternatively, one could observe that condition (vi) is precisely Eichler's mass formula [4]. □

Propositions 3.11 and 3.15 "almost" give an analysis-free proof of the modularity of the theta series $\Theta(L_{i,j})$. Indeed, the construction of the map θ is purely algebro-geometric, and Proposition 3.11 then shows that $\Theta(L_{i,j})$ is a modular form, provided we allow ourselves to modify its constant term as necessary. Proposition 3.15 shows that in fact no such modification is necessary. To what extent does the proof

of this theorem depend on analysis? Igusa [13] has given a proof of Eichler's mass formula that exploits the properties of supersingular elliptic curves and makes no reference to analytic considerations. If one appeals to this argument, then the only analytic ingredient in the proof of Proposition 3.15 is the theory of the Eisenstein series E. One can easily give a purely algebro-geometric proof that there exists a Hecke eigenform $E \in \mathcal{N}$ on which $\mathbb{T}$ acts through $\mathbb{T}^{\mathrm{Eis}}$, but one is left with the problem of determining $a_0(E)$, and the usual proof that this is equal to $(p-1)/24$ uses analysis. It would be interesting to have a purely geometric determination of this constant term, for example in the form of statement (iv) of Proposition 3.15. This would then yield a purely algebro-geometric determination of the constant term of the modular forms $\theta(x_i \otimes x_j)$. (For additional remarks on this problem, see the discussion following the proof of Proposition A.2 of the appendix.)

Lemma 3.16. (i) *The cokernel of the morphism $\mathcal{X} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$ induced by the pairing of Definition* 3.4 *is isomorphic to $\mathbb{Z}/\Delta$, regarded as a $\mathbb{T}$-module via the surjection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}}$. In particular the discriminant of this pairing is equal to Δ.*

(ii) *The cokernel of the morphism $\mathcal{X}^0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}^0, \mathbb{Z})$ induced by the restriction of the pairing of Definition* 3.4 *to $\mathcal{X}^0$ is isomorphic to $\mathbb{Z}/n$, regarded as a $\mathbb{T}$-module via the surjection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}}$. In particular the discriminant of this pairing is equal to n.*

Proof. The claim of part (i) concerning the discriminant of the pairing of Definition 3.4 follows directly from the fact that with respect to the basis $\mathcal{S}$ of $\mathcal{X}$, this pairing is given by a diagonal matrix, the product of whose diagonal entries equals Δ, by Lemma 3.3.

Since the pairing of Definition 3.4 has a non-zero discriminant, it induces an embedding $\mathcal{X} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$, which is $\mathbb{T}$-linear, by Corollary 3.9. Since $\langle \mathbf{x}, x \rangle = \Delta \deg(x)$ for all $x \in \mathcal{X}$, we see that under this map the element $\mathbf{x}$ of $\mathcal{X}$ maps to the element $\Delta \deg$ of $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z})$. Thus we obtain a commutative diagram of morphisms of $\mathbb{T}$-modules

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{X}^{\mathrm{Eis}} & \longrightarrow & \mathcal{X}^{\mathrm{Eis}} \oplus \mathcal{X}^0 & \longrightarrow & \mathcal{X}^0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle (1)} & & \downarrow{\scriptstyle (2a)} & & \downarrow{\scriptstyle (3)} & & \\
 & & & & \mathcal{X} & & & & \\
 & & & & \downarrow{\scriptstyle (2b)} & & & & \\
0 & \longrightarrow & \mathbb{Z}\deg & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}^0, \mathbb{Z}) & \longrightarrow & 0,
\end{array}
\tag{3.17}
$$

in which the top and bottom rows are exact, and in which all vertical arrows are injections.

Map (1) of (3.17) has cokernel equal to $\mathbb{Z}/\Delta$, regarded as a $\mathbb{T}$-module via the surjection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}}$ (as follows from part (i) of Theorem 3.1), (2a) has cokernel isomorphic to $\mathbb{Z}/n$, regarded as a $\mathbb{T}$-module via the surjection $\mathbb{T} \longrightarrow \mathbb{T}^{\mathrm{Eis}}$ (as follows from part (i) of Theorem 3.1 and part (v) of Proposition 3.15), and (2b) has cokernel of order Δ (as follows from the discriminant calculation made at the beginning of this proof). Since Δ and n are coprime, we deduce that the cokernel of (1) maps isomorphically to the cokernel of (2b), proving part (i), while the cokernel of (2a) maps isomorphically to the cokernel of (3), proving part (ii). □

We remark that part (ii) of Lemma 3.16 can also be proved in the following way: it follows from [9, 11.5.2b] that the cokernel of the map $\mathcal{X}^0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}^0, \mathbb{Z})$ is isomorphic to the group of connected components of the geometric fibre at p of the Néron model of $J_0(p)$, which is a cyclic group of order n on which $\mathbb{T}$ acts through its quotient $\mathbb{T}^{\mathrm{Eis}}$, by [15, thm. A.1, prop. II.11.1]. Note though that this argument also depends on calculating the discriminant of the Picard-Lefschetz pairing, which in turn depends on Eichler's mass formula (see Proposition 1.4 and section 2, as well as the remark prior to the statement of Proposition 1.2, of [15, appendix]), and so this proof is not so different from the one that we have given. As a final remark on Lemma 3.16, we also note that Theorem 3.12, Proposition 3.14 and Theorem 3.22 of [20] each imply the weaker statement that the cokernel of the map from $\mathcal{X}^0$ into $\mathrm{Hom}(\mathcal{X}^0, \mathbb{Z})$ is annihilated by the Eisenstein ideal, and so in particular by n.

Let ℓ be a prime. The tensor product $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is a direct sum of the complete local rings $\mathbb{T}_{\mathfrak{m}}$, where $\mathfrak{m}$ ranges over the maximal ideals of $\mathbb{T}$ of residue characteristic ℓ. Thus the tensor product $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ decomposes as a direct sum of its completions $\mathcal{X}_{\mathfrak{m}}$. We may tensor the pairing of Definition 3.4 by $\mathbb{Z}_\ell$ over $\mathbb{Z}$ to obtain a pairing

$$\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \times \mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathbb{Z}_\ell. \tag{3.18}$$

Since this pairing is $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-bilinear (by Corollary 3.9) we see that for distinct maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$ of residue characteristic ℓ, this pairing becomes trivial when restricted to $\mathcal{X}_{\mathfrak{m}} \times \mathcal{X}_{\mathfrak{m}'}$. Thus this pairing is the direct sum of its restrictions $\mathcal{X}_{\mathfrak{m}} \times \mathcal{X}_{\mathfrak{m}} \longrightarrow \mathbb{Z}_\ell$, as $\mathfrak{m}$ ranges over the maximal ideals of $\mathbb{T}$ having residue characteristic ℓ.

Similarly, we can restrict (3.18) to obtain the pairing

$$\mathcal{X}^0 \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \times \mathcal{X}^0 \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathbb{Z}_\ell, \tag{3.19}$$

and we similarly observe that it decomposes as the direct sum of its restrictions $\mathcal{X}^0_{\mathfrak{m}} \times \mathcal{X}^0_{\mathfrak{m}} \longrightarrow \mathbb{Z}_\ell$.

Corollary 3.20. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ of residue characteristic ℓ.*

(i) *If ℓ does not divide Δ, then the pairing $\mathcal{X}_{\mathfrak{m}} \times \mathcal{X}_{\mathfrak{m}} \longrightarrow \mathbb{Z}_\ell$ is a perfect $\mathbb{T}_{\mathfrak{m}}$-bilinear pairing of free $\mathbb{Z}_\ell$-modules.*

(ii) *If $\mathfrak{m}$ is not an Eisenstein prime, then the pairing $\mathcal{X}^0_{\mathfrak{m}} \times \mathcal{X}^0_{\mathfrak{m}} \longrightarrow \mathbb{Z}_\ell$ is a perfect $\mathbb{T}^0_{\mathfrak{m}}$-bilinear pairing of free $\mathbb{Z}_\ell$-modules.*

Proof. Part (i) follows immediately from the discriminant computation of part (i) of Lemma 3.16.

To prove part (ii), we proceed by cases. If ℓ does not divide Δ, then part (ii) follows from part (i) and the direct sum decomposition $\mathcal{X}^{\mathrm{Eis}}_{\mathfrak{m}} \oplus \mathcal{X}^0_{\mathfrak{m}} \xrightarrow{\sim} \mathcal{X}_{\mathfrak{m}}$, together with the fact that $\mathcal{X}^{\mathrm{Eis}}$ and $\mathcal{X}^0$ are orthogonal under the pairing (by $\mathbb{T}$-bilinearity). On the other hand, if ℓ does not divide n, then part (ii) follows from the discriminant calculation of Lemma 3.16 (ii). Since Δ and n are coprime by construction, we see that part (ii) is now proved. □

Let us point out that part (ii) of Corollary 3.20 may also be deduced from [20, thm. 3.12/prop. 3.14/thm. 3.22]. (Compare the related remark following the proof of Lemma 3.16.)

The final observation that we will make in this section is that the results already established suffice to recover Eichler's theorem [5] that the space of weight two modular forms on $\Gamma_0(p)$ is spanned by theta series.

Proposition 3.21. *The morphism* $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q} \otimes_{\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q}} \mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Q}$ *induced by* (0.2) *is an isomorphism. In particular, the* $\mathbb{Q}$*-vector space* $\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Q}$ *is spanned by the theta series* $\Theta(L_{i,j})$.

Proof. It follows from Lemma 3.16 (i) that the pairing of Definition 3.4 has non-zero discriminant. Thus if we take $A = \mathbb{Q}$, $B = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$, and $U = V = \mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q}$, we find that it induces a perfect pairing $U \times U \longrightarrow A$, and so we are in the situation of Lemma 2.4. It follows from that lemma, together with Corollary 3.2, that the morphism ϕ_B (in the notation of that lemma) is an isomorphism. However, ϕ_B is precisely the morphism θ tensored with $\mathbb{Q}$ over $\mathbb{Z}$ (once we use Propositions 1.1 and 1.3 to make the identifications $\mathcal{M}\otimes_{\mathbb{Z}}\mathbb{Q} \xrightarrow{\sim} \mathcal{N}\otimes_{\mathbb{Z}}\mathbb{Q} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Q}}(\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q}, \mathbb{Q})$). The proposition now follows by observing that Proposition 3.11 implies that θ tensored with $\mathbb{Q}$ over $\mathbb{Z}$ and (0.2) tensored with $\mathbb{Q}$ over $\mathbb{Z}$ are the same map. □

4. The $\mathbb{T}$-module $\mathcal{X}$. Further properties

In this section, we study in more detail the structure of the $\mathbb{T}_{\mathfrak{m}}$-modules $\mathcal{X}_{\mathfrak{m}}$ and $\mathcal{X}^0_{\mathfrak{m}}$ (as $\mathfrak{m}$ ranges over the maximal ideals of $\mathbb{T}$), and their relation to the arithmetic of the Jacobian $J_0(p)$.

We begin by studying the case when $\mathfrak{m}$ is an Eisenstein maximal ideal of $\mathbb{T}$ of residue characteristic ℓ. As in the proof of Theorem 1.10, we let I denote the kernel of the map $\mathbb{T}_{\mathfrak{m}} \longrightarrow \mathbb{T}^{\mathrm{Eis}}_{\mathfrak{m}} \xrightarrow{\sim} \mathbb{Z}_\ell$ and J denote the kernel of the map $\mathbb{T}_{\mathfrak{m}} \longrightarrow \mathbb{T}^0_{\mathfrak{m}}$. Then I and J are each principal (since their intersection is zero and each induces a Cartier divisor in the closed subscheme cut out by the other – see the proofs of Theorem 1.10 and Lemma 1.11), and so $I + J$ is generated by a pair of elements $\eta \in I$, $\gamma \in J$. Now γ is a lifting of the generator of the image of J in $\mathbb{Z}_\ell$, and so is congruent to some power ℓ^n of ℓ modulo I. Thus we have $I + J = (\eta, \ell^n)\mathbb{T}_{\mathfrak{m}}$, and $\mathbb{T}_{\mathfrak{m}}/(I + J) \xrightarrow{\sim} \mathbb{Z}_\ell/\ell^n$. We conclude that $\mathfrak{m} = (\eta, \ell)\mathbb{T}_{\mathfrak{m}}$.

Lemma 4.1. *Let* $\mathfrak{m}$ *be an Eisenstein maximal ideal of residue characteristic* ℓ.

(i) *If* N *is any finitely generated* $\mathbb{T}_{\mathfrak{m}}/\ell$*-module, then* $N[\mathfrak{m}]$ *(the* $\mathbb{T}$*-submodule of* $\mathfrak{m}$*-torsion points of* N*) and* $N/\mathfrak{m}$ *are* $\mathbb{T}/\mathfrak{m}$*-vector spaces of equal rank.*

(ii) *If* $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ *is a short exact sequence of* $\mathbb{T}_{\mathfrak{m}}/\ell$*-modules, there is an induced long exact sequence*

$$0 \longrightarrow N'[\mathfrak{m}] \longrightarrow N[\mathfrak{m}] \longrightarrow N''[\mathfrak{m}] \longrightarrow N'/\mathfrak{m} \longrightarrow N/\mathfrak{m} \longrightarrow N''/\mathfrak{m} \longrightarrow 0.$$

Proof. To prove (i), note that $N[\eta]$ and N/η are $\mathbb{T}_{\mathfrak{m}}$-modules annihilated by both ℓ and η, and hence by $\mathfrak{m}$, so that $N[\eta] = N[\mathfrak{m}]$ and $N/\eta = N/\mathfrak{m}$. That they are of equal rank as $\mathbb{T}/\mathfrak{m}$-vector spaces (equivalently, of equal length as $\mathbb{T}_{\mathfrak{m}}$-modules) follows from the exact sequence $0 \longrightarrow N[\eta] \longrightarrow N \xrightarrow{\cdot\eta} N \longrightarrow N/\eta \longrightarrow 0$ and the additivity of lengths in exact sequences.

To prove (ii), tensor the given exact sequence with the complex $\mathbb{T}_{\mathfrak{m}}/\ell \xrightarrow{\cdot\eta} \mathbb{T}_{\mathfrak{m}}/\ell$ of free $\mathbb{T}_{\mathfrak{m}}/\ell$-modules and apply the snake lemma. This yields the long exact sequence

$$0 \longrightarrow N'[\eta] \longrightarrow N[\eta] \longrightarrow N''[\eta] \longrightarrow N'/\eta \longrightarrow N/\eta \longrightarrow N''/\eta \longrightarrow 0.$$

Since ℓ and η generate the maximal ideal $\mathfrak{m}\mathbb{T}_{\mathfrak{m}}$, we can rewrite this as

$$0 \longrightarrow N'[\mathfrak{m}] \longrightarrow N[\mathfrak{m}] \longrightarrow N''[\mathfrak{m}] \longrightarrow N'/\mathfrak{m} \longrightarrow N/\mathfrak{m} \longrightarrow N''/\mathfrak{m} \longrightarrow 0,$$

as claimed in the statement of part (ii). □

Theorem 4.2. *Let $\mathfrak{m}$ be an Eisenstein maximal ideal of $\mathbb{T}$. Then $\mathcal{X}_\mathfrak{m}$ is a free $\mathbb{T}_\mathfrak{m}$-module of rank one, and $\mathcal{X}^0_\mathfrak{m}$ is a free $\mathbb{T}^0_\mathfrak{m}$-module of rank one.*

Proof. As above, we let ℓ denote the residue characteristic of $\mathfrak{m}$. From Corollary 3.2 we see that $\mathcal{X}_\mathfrak{m} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is free of rank one over $\mathbb{T}_\mathfrak{m} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, and that similarly $\mathcal{X}^0_\mathfrak{m} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is free of rank one over $\mathbb{T}^0_\mathfrak{m} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Thus to prove the theorem it suffices to show that each of the $\mathbb{T}/\mathfrak{m} \xrightarrow{\sim} \mathbb{T}^0/\mathfrak{m}$-vector spaces $\mathcal{X}/\mathfrak{m}$ and $\mathcal{X}^0/\mathfrak{m}$ are of dimension one.

We begin by proving that these two vector spaces are of the same dimension. To do this, we first tensor the short exact sequence of $\mathbb{T}$-modules

$$0 \longrightarrow \mathcal{X}^0 \longrightarrow \mathcal{X} \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

with the flat $\mathbb{T}$-module $\mathbb{T}_\mathfrak{m}$ to obtain the short exact sequence of $\mathbb{T}_\mathfrak{m}$-modules

$$0 \longrightarrow \mathcal{X}^0_\mathfrak{m} \longrightarrow \mathcal{X}_\mathfrak{m} \xrightarrow{\deg} \mathbb{Z}_\ell \longrightarrow 0.$$

This is a short exact sequence of torsion-free (equals flat) $\mathbb{Z}_\ell$-modules, and so reducing modulo ℓ yields the short exact sequence $0 \longrightarrow \mathcal{X}^0_\mathfrak{m}/\ell \longrightarrow \mathcal{X}_\mathfrak{m}/\ell \xrightarrow{\deg} \mathbb{Z}/\ell \longrightarrow 0$, giving rise, by part (ii) of Lemma 4.1, to the long exact sequence

$$\begin{aligned}(4.3)\quad 0 \longrightarrow \mathcal{X}^0_\mathfrak{m}/\ell\,[\mathfrak{m}] \longrightarrow \mathcal{X}_\mathfrak{m}/\ell\,[\mathfrak{m}] \xrightarrow{\deg} \mathbb{Z}/\ell \\ \longrightarrow \mathcal{X}^0/\mathfrak{m} \longrightarrow \mathcal{X}/\mathfrak{m} \xrightarrow{\deg} \mathbb{Z}/\ell \longrightarrow 0.\end{aligned}$$

(Note that $\mathbb{T}$ acts on the quotient $\mathbb{Z} \xrightarrow{\sim} \mathcal{X}/\mathcal{X}^0$ through $\mathbb{T}^{\mathrm{Eis}}$, so that $\mathbb{Z}/\ell\,[\mathfrak{m}] \xrightarrow{\sim} (\mathbb{Z}/\ell)/\mathfrak{m} \xrightarrow{\sim} \mathbb{Z}/\ell$.) We wish to show that $\mathcal{X}/\mathfrak{m}$ and $\mathcal{X}^0/\mathfrak{m}$ are of the same dimension over $\mathbb{T}/\mathfrak{m}$. It is equivalent to show (by Lemma 4.1, part (i)) that $\mathcal{X}/\ell\,[\mathfrak{m}]$ and $\mathcal{X}^0/\ell\,[\mathfrak{m}]$ are of the same rank. A consideration of (4.3) shows that it suffices to prove that the image of $\mathcal{X}/\ell\,[\mathfrak{m}]$ in $\mathbb{Z}/\ell$ is trivial.

Let $\bar{x} \in \mathcal{X}_\mathfrak{m}/\ell\,[\mathfrak{m}]$. We can find an element $x \in \mathcal{X}$ that reduces to $\bar{x}$ modulo ℓ. Let x_i be an element of $\mathcal{S}$. Write $f = \theta(x \otimes x_i) \in \mathcal{M}$. Then $f - a_1(f)E$ is an element of $\ell\mathcal{N}$, since x is annihilated by $\mathfrak{m}$ modulo ℓ, and so (in the notation of Proposition 1.1) $A_0(f) \equiv A_0(a_1(f)E) = a_1(f)n \mod \ell$. By Proposition 3.15 we see that $A_0(f) = 2\Delta \deg(x)/2 = \Delta \deg(x)$. Thus we conclude that $\Delta \deg(x) \equiv a_1(f)n \mod \ell$. Since $\mathfrak{m}$ is an Eisenstein prime, Proposition 1.8 shows that ℓ divides n, and so is coprime to Δ. Thus $\deg(x) \equiv 0 \mod \ell$, and so $\bar{x}$ does have trivial image in $\mathbb{Z}/\ell$. This completes the proof that $\mathcal{X}/\mathfrak{m}$ and $\mathcal{X}^0/\mathfrak{m}$ have the same dimension.

To prove the theorem, it remains to show that $\mathcal{X}^0/\mathfrak{m}$ is of dimension one over $\mathbb{T}^0/\mathfrak{m}$. We will follow the methods of [20] and [23], and we refer to the proofs of [20, thm. 6.1] and [23, thm. 2.3] and the references cited therein for a more detailed discussion of the techniques used and claims made in the argument that follows.

Let $\mathcal{J}$ denote the Néron model of the Jacobian $J_0(p)$ of $X_0(p)$, and let $T_0(p)$ denote the connected component of the characteristic p fibre of $\mathcal{J}$. Then $T_0(p)$ is a torus over $\mathbb{F}_p$. Recall that $\mathcal{X}^0$ can be naturally identified with the character lattice $\mathrm{Hom}_{\overline{\mathbb{F}}_p}(T_0(p), \mathbb{G}_m)$ of $T_0(p)$. Since $T_0(p)$ is defined over $\mathbb{F}_p$, we see that $\mathcal{X}^0$ is equipped with an action of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, and that $T_0(p)$ can in turn be recovered from $\mathcal{X}^0$ equipped with its action of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ as $\mathrm{Hom}(\mathcal{X}^0, \mathbb{G}_m)$ (at first defined over $\overline{\mathbb{F}}_p$, and then descended to $\mathbb{F}_p$ using the descent data induced by the Galois action on $\mathcal{X}^0$). By regarding the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-action on $\mathcal{X}^0$ as being an unramified action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, we see that the expression $\mathrm{Hom}(\mathcal{X}^0, \mathbb{G}_m)$ equally well defines

a torus $\mathcal{T}$ over $\mathbb{Z}_p$ that has $T_0(p)$ as its special fibre. (We are recalling the standard fact that any torus over the special fibre of a Henselian discrete valuation ring deforms uniquely to a torus over the discrete valuation ring itself.)

The formal completion of $\mathcal{T}$ along its characteristic p fibre embeds into the formal completion of $\mathcal{J}$ along its characteristic p fibre, and so the group scheme $\mathcal{T}[\ell]$ embeds as a sub-group scheme of $\mathcal{J}[\ell]$ (at first formally, but then actually, since it is finite). Passing to characteristic zero fibres shows that $\mathcal{T}[\ell]_{/\mathbb{Q}_p}$ embeds into $J_0(p)[\ell]_{/\mathbb{Q}_p}$. Now $\mathcal{T}[\ell]$ is Cartier dual to $\mathcal{X}^0/\ell$, and the cokernel of the preceding embedding is naturally identified with $\mathcal{X}^0/\ell$. We thus obtain a short exact sequence of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules

$$0 \longrightarrow \mathrm{Hom}(\mathcal{X}^0/\ell, \mu_\ell) \longrightarrow J_0(p)[\ell](\overline{\mathbb{Q}}_p) \longrightarrow \mathcal{X}^0/\ell \longrightarrow 0,$$

where $\mathrm{Hom}(\mathcal{X}^0/\ell, \mu_\ell)$ is naturally identified with $\mathcal{T}[\ell](\overline{\mathbb{Q}}_p)$. (This is the short exact sequence [23, (2.4)].)

Apply $\mathrm{Hom}_{\mathbb{T}^0}(\mathbb{T}^0/\mathfrak{m}, -)$ to this short exact sequence, to obtain the exact sequence

$$0 \longrightarrow \mathrm{Hom}(\mathcal{X}^0/\mathfrak{m}, \mu_\ell) \longrightarrow J_0(p)[\mathfrak{m}](\overline{\mathbb{Q}}_p) \longrightarrow \mathcal{X}^0/\ell\,[\mathfrak{m}],$$

where $J_0(p)[\mathfrak{m}]$ denotes the finite subgroup scheme of $J_0(p)[\ell]$ that is the simultaneous kernel of all elements of $\mathfrak{m}$. Observe that [15, p. 99 and cor. II.16.3] implies that $J_0(p)[\mathfrak{m}]$ is a two-dimensional $\mathbb{T}/\mathfrak{m}$-vector space scheme, and that $\mathcal{J}[\mathfrak{m}]$ extends it to a two-dimensional finite flat $\mathbb{T}/\mathfrak{m}$-vector space scheme over $\mathbb{Z}_p$, whose specialization to characteristic p has non-zero image in the connected component group of the special fibre of $\mathcal{J}$. On the other hand, it follows from the discussion of the preceding paragraph that the specialization to characteristic p of the points of $\mathrm{Hom}(\mathcal{X}^0/\mathfrak{m}, \mu_\ell)$ lie in $T_0(p)[\ell]$, and so have trivial image in this connected component group. Thus $\mathrm{Hom}(\mathcal{X}^0/\mathfrak{m}, \mu_\ell)$ must be only one-dimensional over $\mathbb{T}/\mathfrak{m}$. The theorem now follows. □

We now turn to an analysis of $\mathcal{X}_\mathfrak{m}$ and $\mathcal{X}^0_\mathfrak{m}$ when $\mathfrak{m}$ is of the first type (so that $\mathbb{T}_\mathfrak{m} \xrightarrow{\sim} \mathbb{T}^0_\mathfrak{m}$ and $\mathcal{X}^0_\mathfrak{m} \xrightarrow{\sim} \mathcal{X}_\mathfrak{m}$).

Lemma 4.4. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ of the first type, having residue characteristic ℓ, and let W be a finite length $\mathbb{T}^0_\mathfrak{m}/\ell$-module. Then the $\mathbb{T}^0_\mathfrak{m}/\ell$-modules $\mathcal{X}^0_\mathfrak{m}/\ell \otimes_{\mathbb{T}^0_\mathfrak{m}/\ell} W$ and $\mathrm{Hom}_{\mathbb{T}^0_\mathfrak{m}/\ell}(W, \mathcal{X}^0_\mathfrak{m}/\ell)$ are naturally $\mathbb{Z}/\ell$-dual to one another. In particular, they are of equal dimension as $\mathbb{Z}/\ell$-vector spaces.*

Proof. Since $\mathfrak{m}$ is non-Eisenstein, it follows from Corollary 3.20 (ii) that the pairing (3.19) induces a perfect $\mathbb{T}^0_\mathfrak{m}/\ell$-bilinear pairing $\mathcal{X}^0_\mathfrak{m}/\ell \times \mathcal{X}^0_\mathfrak{m}/\ell \longrightarrow \mathbb{Z}/\ell$. Using this we compute (using the adjointness between Hom and $\otimes$) that

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}/\ell}(\mathcal{X}^0_\mathfrak{m}/\ell \otimes_{\mathbb{T}^0_\mathfrak{m}/\ell} W, \mathbb{Z}/\ell) &\xrightarrow{\sim} \mathrm{Hom}_{\mathbb{T}^0_\mathfrak{m}/\ell}(W, \mathrm{Hom}_{\mathbb{Z}/\ell}(\mathcal{X}^0_\mathfrak{m}/\ell, \mathbb{Z}_\ell)) \\ &\xrightarrow{\sim} \mathrm{Hom}_{\mathbb{T}^0_\mathfrak{m}/\ell}(W, \mathcal{X}^0_\mathfrak{m}/\ell).\end{aligned}$$

Since a $\mathbb{Z}/\ell$-vector space and its dual have the same dimension, this proves the lemma. □

For the remainder of this section we fix an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ and thus obtain an embedding of Galois groups $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. (In other words, we fix a choice of a decomposition group at p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.) The following simple lemma will be required in the proof of Theorem 4.6 below. We refer to [24, p. 189] for the notion of finiteness of a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-representation.

Lemma 4.5. *Let A be a finite local ring with residue field k, let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(k)$ be an irreducible two-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over k, let U be a finite-length A-module equipped with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and let V be a finite-length A-module equipped with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Suppose that*

(i) *ρ is* not *finite at p;*

(ii) *the semi-simplification of U as an $A[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module is isomorphic to a direct sum of copies of ρ;*

(iii) *V is a finite $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module;*

(iv) *there is a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-equivariant A-linear embedding $V \to U$.*

Then $\lg(U) \geq 2\lg(V)$. (Here $\lg(-)$ denotes the length of a finite length A-module.)

Proof. Let $F^0 \supset F^1 \supset \cdots \supset F^{l-1} \supset F^l = 0$ be a decreasing filtration of U by $A[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-modules such that the successive quotients F^i/F^{i+1} are isomorphic to ρ ($i = 0, \ldots, l-1$). Let $G^i = V \cap F^i$. Then G^i/G^{i+1} embeds into F^i/F^{i+1}. Since the latter k-vector space is two-dimensional and not finite as a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module, while G^i/G^{i+1} is finite (being a subquotient of the finite representation V), we see that G^i/G^{i+1} is at most one-dimensional. Thus

$$\lg U = \sum_{i=0}^{l-1} \lg F^i/F^{i+1} \geq 2 \sum_{i=0}^{l-1} \lg G^i/G^{i+1} = 2 \lg V. \qquad \square$$

If $\mathfrak{m}$ is a maximal ideal of the first type, then attached to $\mathfrak{m}$ there is a two-dimensional irreducible representation $\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{T}^0/\mathfrak{m})$, characterized by the property that it is unramified away from p and ℓ, and that for any prime q distinct from p and ℓ, the characteristic polynomial of $\rho(\mathrm{Frob}_q)$ is equal to $X^2 - T_q X + q \pmod{\mathfrak{m}}$ [15, prop. II.14.1]. Furthermore, the $\mathbb{T}/\mathfrak{m}\,[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module $J_0[\mathfrak{m}](\overline{\mathbb{Q}})$ has a Jordan-Hölder filtration whose successive irreducible quotients are isomorphic to the representation $\rho_{\mathfrak{m}}$ [15, proof of prop. II.14.2].

Note that the set $\mathcal{S}$ that forms a basis for $\mathcal{X}$ is equipped with an action of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ (since it is a set of $\overline{\mathbb{F}}_p$-valued points of a curve defined over $\mathbb{F}_p$). Thus $\mathcal{X}$ is naturally a $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-module. We may equally well regard $\mathcal{X}$ as an unramified $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module. (This Galois action coincides with that considered in the proof of Theorem 4.2.)

Theorem 4.6. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ of the first type of characteristic ℓ. Then there is a short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}/\ell\,[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-modules*

$$0 \longrightarrow \mathrm{Hom}(\mathcal{X}^0_{\mathfrak{m}}, \mu_\ell) \longrightarrow J_0(p)[\ell](\overline{\mathbb{Q}}_p)_{\mathfrak{m}} \longrightarrow \mathcal{X}^0_{\mathfrak{m}}/\ell \longrightarrow 0,$$

which is split as a short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}/\ell$-modules.

Proof. The theorem is an extension of [23, thm. 2.3], and will follow the same lines of proof as that result. Just as in the proof of Theorem 4.2 we obtain a short exact sequence

$$0 \longrightarrow \mathrm{Hom}(\mathcal{X}^0/\ell, \mu_\ell) \longrightarrow J_0(p)[\ell](\overline{\mathbb{Q}}_p) \longrightarrow \mathcal{X}^0/\ell \longrightarrow 0$$

of $\mathbb{T}^0/\ell\,[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-modules, which we may localize at $\mathfrak{m}$ to yield the required short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}/\ell\,[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-modules

$$0 \longrightarrow \mathrm{Hom}(\mathcal{X}^0_{\mathfrak{m}}/\ell, \mu_\ell) \longrightarrow J_0(p)[\ell](\overline{\mathbb{Q}}_p)_{\mathfrak{m}} \longrightarrow \mathcal{X}^0_{\mathfrak{m}}/\ell \longrightarrow 0. \tag{4.7}$$

We will show that (4.7) remains short exact after applying $\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, -)$, for any finite length $\mathbb{T}^0_{\mathfrak{m}}/\ell$-module W. Taking $W = \mathcal{X}^0_{\mathfrak{m}}/\ell$ will then yield a $\mathbb{T}^0_{\mathfrak{m}}/\ell$-linear map $s : \mathcal{X}^0_{\mathfrak{m}}/\ell \to J_0(p)[\ell](\overline{\mathbb{Q}}_p)_{\mathfrak{m}}$ which lifts the identity map from $\mathcal{X}^0_{\mathfrak{m}}/\ell$ to itself, and so splits (4.7).

Choose a finite length $\mathbb{T}^0_{\mathfrak{m}}/\ell$-module W. Applying $\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, -)$ to (4.7) yields an exact sequence of $\mathbb{T}^0_{\mathfrak{m}}/\ell\,[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-modules

$$\begin{aligned}(4.8)\quad 0 \longrightarrow \mathrm{Hom}(\mathcal{X}^0_{\mathfrak{m}}/\ell \otimes_{\mathbb{T}^0_{\mathfrak{m}}/\ell} W, \mu_\ell) \\ \longrightarrow \mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, J_0(p)[\ell](\overline{\mathbb{Q}}_p)_{\mathfrak{m}}) \longrightarrow \mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, \mathcal{X}^0_{\mathfrak{m}}/\ell).\end{aligned}$$

(Here we regard W as being endowed with the trivial $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-action. We have also used the isomorphism

$$\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, \mathrm{Hom}(\mathcal{X}^0_{\mathfrak{m}}/\ell, \mu_\ell)) \xrightarrow{\sim} \mathrm{Hom}(\mathcal{X}^0_{\mathfrak{m}}/\ell \otimes_{\mathbb{T}^0_{\mathfrak{m}}/\ell} W, \mu_\ell)$$

provided by the adjointness between Hom and $\otimes$.) We must show that (4.8) is exact on the right. We begin by making some observations concerning the Galois-action on the first two terms of this exact sequence.

(i) The $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module $\mathrm{Hom}(\mathcal{X}^0_{\mathfrak{m}}/\ell \otimes_{\mathbb{T}^0_{\mathfrak{m}}/\ell} W, \mu_\ell)$ is finite at p. (To see this, note that if we forget the $\mathbb{T}^0_{\mathfrak{m}}/\ell$-action, then we obtain a direct sum of copies of μ_ℓ.)

(ii) Since $J_0(p)[\ell](\overline{\mathbb{Q}}_p)$ and $J_0(p)[\ell](\overline{\mathbb{Q}})$ are of course equal, the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-action on $\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, J_0(p)[\ell](\overline{\mathbb{Q}}_p)_{\mathfrak{m}}) = \mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, J_0(p)[\ell](\overline{\mathbb{Q}})_{\mathfrak{m}})$ extends to a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action, and the semi-simplification of $\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, J_0(p)[\ell](\overline{\mathbb{Q}})_{\mathfrak{m}})$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module is a direct sum of copies of $\rho_{\mathfrak{m}}$. (This follows from the fact that this $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module is a successive extension of copies of $J_0(p)[\mathfrak{m}](\overline{\mathbb{Q}})$, which itself is a successive extension of copies of $\rho_{\mathfrak{m}}$, as we observed above.)

Since $\mathfrak{m}$ is non-Eisenstein, we see by [23, prop. 2.2] that $\rho_{\mathfrak{m}}$ is not finite at p. Taking into account (i) and (ii) above we see that Lemma 4.5 implies that the dimension of $\mathrm{Hom}(\mathcal{X}^0_{\mathfrak{m}}/\ell \otimes_{\mathbb{T}^0_{\mathfrak{m}}/\ell} W, \mu_\ell)$ over $\mathbb{Z}/\ell$ is at most one-half that of $\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, J_0(p)[\ell](\overline{\mathbb{Q}}_p)_{\mathfrak{m}})$. A consideration of (4.8) together with Lemma 4.4 now shows that each of $\mathrm{Hom}(\mathcal{X}^0_{\mathfrak{m}}/\ell \otimes_{\mathbb{T}^0_{\mathfrak{m}}/\ell} W, \mu_\ell)$ and $\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, \mathcal{X}^0_{\mathfrak{m}}/\ell)$ must be of exactly one-half the dimension of $\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/\ell}(W, J_0(p)[\ell](\overline{\mathbb{Q}}_p)_{\mathfrak{m}})$ over $\mathbb{Z}/\ell$, and that (4.8) is exact on the right. This completes the proof of the theorem. □

Corollary 4.9. *If $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ of the first type, then the dimension of $J_0(p)[\mathfrak{m}]$ over $\mathbb{T}^0/\mathfrak{m}$ is equal to twice the dimension of $\mathcal{X}^0_{\mathfrak{m}}/\mathfrak{m}$ over $\mathbb{T}^0/\mathfrak{m}$.*

Proof. This follows by taking W to be $\mathbb{T}^0/\mathfrak{m}$ in the proof of Theorem 4.6. □

Corollary 4.10. *If $\mathfrak{m}$ is a maximal ideal of the first type of $\mathbb{T}$ of residue characteristic ℓ, then $\mathcal{X}^0_{\mathfrak{m}}/\ell$ is a faithful $\mathbb{T}^0_{\mathfrak{m}}/\ell$-module.*

Proof. We see by Theorem 4.6 that it suffices to show that $J_0(p)[\ell](\overline{\mathbb{Q}}_p)_{\mathfrak{m}}$ is a faithful $\mathbb{T}^0_{\mathfrak{m}}/\ell$-module. For this, it suffices to prove that $J_0(p)[\ell](\overline{\mathbb{Q}}_p)$ is a faithful $\mathbb{T}^0/\ell$-module. Suppose that $T \in \mathbb{T}^0$ annihilates $J_0(p)[\ell](\overline{\mathbb{Q}}_p)$. Then T is divisible by ℓ in $\mathrm{End}(J_0(p))$. Since $\mathbb{T}^0$ is the full ring of endomorphisms of $J_0(p)$ [15, prop. II.9.5], we see that in fact T is divisible by ℓ in $\mathbb{T}^0$. This proves that $J_0(p)[\ell](\overline{\mathbb{Q}}_p)$ is a faithful $\mathbb{T}^0/\ell$-module, and so completes the proof of the corollary. □

As a final consideration for this section, we recall the following result.

Theorem 4.11. *If $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ of the first type, then $\mathbb{T}^0_{\mathfrak{m}}$ is Gorenstein if and only if $J_0[\mathfrak{m}]$ has rank two over $\mathbb{T}^0/\mathfrak{m}$.*

Proof. We see from [15, cor. II.15.2] that the only situation in which both conditions occurring in the statement of the theorem don't automatically hold are when $\mathfrak{m}$ is ordinary of residue characteristic two. Thus we need only prove the theorem in this case. We may furthermore assume that $p > 2$ (since $X_0(2)$ has genus zero), and so coprime to the residue characteristic of $\mathfrak{m}$. The theorem then follows from [16] and [7, prop. 12.8]. Indeed the latter reference shows that the étale part of the contravariant $\mathfrak{m}$-adic Tate module of $J_0(p)$ is free of rank one over $\mathbb{T}_{\mathfrak{m}}$, and this is precisely the input required to deduce the theorem from [16]. (We remark that the reader may also refer to the proof of [7, prop. 12.10], which uses identical reasoning to the argument of [16].) □

5. Proofs of the main results

In this section we prove the results stated in section 0.

Proof of Theorem 0.3. We wish to show that the morphism $\theta : \mathcal{X} \otimes_{\mathbb{T}} \mathcal{X} \longrightarrow \mathcal{N}$ has image equal to $\mathcal{M}$. Since its image lies in $\mathcal{M}$, and $\mathcal{M}$ has index Δ in $\mathcal{N}$ by Proposition 1.1, it will suffice to show that the cokernel of θ has order Δ. Since θ is obtained by composing the morphism (3.10) induced by the pairing of Definition 3.4 with the isomorphism of part (i) of Proposition 1.3, it suffices to show that the cokernel of (3.10) has order Δ.

For this, it will suffice to show that for each prime number ℓ, the image of the morphism

$$\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \otimes_{\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Z}_\ell} \mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell, \mathbb{Z}_\ell), \tag{5.1}$$

obtained by tensoring the morphism (3.10) through by $\mathbb{Z}_\ell$ over $\mathbb{Z}$, and which is induced by the pairing (3.18), has cokernel of order equal to the maximal power of ℓ dividing Δ. Thus for the remainder of the proof we fix ℓ, and devote ourselves to proving this statement.

If we set $A = \mathbb{Z}_\ell$, $B = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $U = V = \mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, then the running hypotheses referred to in the statement of Proposition 2.8 are satisfied. We will verify that for any maximal ideal of $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, either condition (i) or condition (ii) in the statement of Proposition 2.8 is satisfied. For this, given any maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ of residue characteristic ℓ, we must show either that the pairing (3.18) becomes perfect when restricted to $\mathcal{X}_{\mathfrak{m}} \times \mathcal{X}_{\mathfrak{m}}$ and that $\mathcal{X}_{\mathfrak{m}}/\ell$ is a faithful $\mathbb{T}_{\mathfrak{m}}/\ell$-module, or that $\mathcal{X}_{\mathfrak{m}}$ is a free $\mathbb{T}_{\mathfrak{m}}$-module of rank one.

If $\mathfrak{m}$ is of the first kind, then Corollary 3.20 (ii) (and the isomorphism $\mathcal{X}^0_{\mathfrak{m}} \xrightarrow{\sim} \mathcal{X}_{\mathfrak{m}}$) shows that the pairing (3.18) is perfect when restricted to $\mathcal{X}_{\mathfrak{m}} \times \mathcal{X}_{\mathfrak{m}}$, while Corollary 4.10 shows that $\mathcal{X}^0_{\mathfrak{m}}/\ell \xrightarrow{\sim} \mathcal{X}_{\mathfrak{m}}/\ell$ is a faithful $\mathbb{T}_{\mathfrak{m}}/\ell$-module.

If $\mathfrak{m}$ is of the second kind, then $\mathcal{X}^{\mathrm{Eis}}_{\mathfrak{m}} \xrightarrow{\sim} \mathcal{X}_{\mathfrak{m}}$ is isomorphic to $\mathbb{Z}_\ell$, and so is a free $\mathbb{T}_{\mathfrak{m}} \xrightarrow{\sim} \mathbb{T}^{\mathrm{Eis}}_{\mathfrak{m}} \xrightarrow{\sim} \mathbb{Z}_\ell$-module of rank one, while if $\mathfrak{m}$ is Eisenstein, then Theorem 4.2 shows that $\mathcal{X}_{\mathfrak{m}}$ is a free $\mathbb{T}_{\mathfrak{m}}$-module of rank one.

Thus the hypotheses of Proposition 2.8 are satisfied, and we deduce that the cokernel of (5.1) is isomorphic to the cokernel of the morphism $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell, \mathbb{Z}_\ell)$ induced by the pairing (3.18). Lemma 3.16 (i) shows that

the cokernel of this morphism has order equal to the maximal power of ℓ dividing Δ. This completes the proof of Theorem 0.3. □

Proof of Theorem 0.4. We wish to prove that the morphism $\mathbb{T} \longrightarrow \mathrm{End}_{\mathbb{T}}(\mathcal{X})$ is an isomorphism. It suffices to prove this after tensoring this morphism through by $\mathbb{Z}_\ell$, for each prime number ℓ. Lemma 2.6 shows that it suffices to prove that $\mathcal{X}/\ell$ is a faithful $\mathbb{T}/\ell$-module, for each prime number ℓ. Equivalently, it suffices to show that $\mathcal{X}_{\mathfrak{m}}/\ell$ is a faithful $\mathbb{T}_{\mathfrak{m}}/\ell$-module for each maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ of residue characteristic ℓ. This was observed in the course of proving Theorem 0.3. (When $\mathfrak{m}$ is of the second type or Eisenstein, note that $\mathcal{X}_{\mathfrak{m}}/\ell$ is even a free $\mathbb{T}_{\mathfrak{m}}/\ell$-module of rank one, and so in particular is faithful.) □

Proof of Theorem 0.5. Let ℓ denote the residue characteristic of $\mathfrak{m}$. Then $\mathbb{T}_{\mathfrak{m}}$ is a free $\mathbb{Z}_\ell$-module of finite rank, and so is Gorenstein if and only $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T}_{\mathfrak{m}}, \mathbb{Z}_\ell)$ is a free $\mathbb{T}_{\mathfrak{m}}$-module of rank one. Now Proposition 1.3 (i) provides an isomorphism $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T}_{\mathfrak{m}}, \mathbb{Z}_\ell) \xrightarrow{\sim} \mathcal{N}_{\mathfrak{m}}$, and so we see that $\mathbb{T}_{\mathfrak{m}}$ is Gorenstein if and only if $\mathcal{N}_{\mathfrak{m}}$ is free of rank one. Proposition 1.9 shows that $\mathcal{N}_{\mathfrak{m}}$ is free of rank one if and only if $\mathcal{M}_{\mathfrak{m}}$ is free of rank one. Putting these results together yields the equivalence of (i) and (iii).

The equivalence of $(\mathrm{i})^0$ and $(\mathrm{iii})^0$ is proved similarly (and is even more direct, since $\mathcal{N}^0 = \mathcal{M}^0$), while the equivalence of (iii) and $(\mathrm{iii})^0$ is simply a restatement of Theorem 1.10.

If $\mathfrak{m}$ is of the first type, then the equivalence of (ii) and $(\mathrm{ii})^0$ is tautological, while the equivalence of $(\mathrm{ii})^0$ and $(\mathrm{iii})^0$ is given by Corollary 4.9 and Theorem 4.11. If $\mathfrak{m}$ is of the second type, then $\mathbb{T}_{\mathfrak{m}} \xrightarrow{\sim} \mathbb{T}_{\mathfrak{m}}^{\mathrm{Eis}} \xrightarrow{\sim} \mathbb{Z}_\ell$, while $\mathbb{T}_{\mathfrak{m}}^0 = 0$, and similarly $\mathcal{X}_{\mathfrak{m}} \xrightarrow{\sim} \mathcal{X}_{\mathfrak{m}}^{\mathrm{Eis}} \xrightarrow{\sim} \mathbb{Z}_\ell$, while $\mathcal{X}_{\mathfrak{m}}^0 = 0$. Thus in this case the conditions (ii), $(\mathrm{ii})^0$, (iii) and $(\mathrm{iii})^0$ are all trivially satisfied. If $\mathfrak{m}$ is Eisenstein, then (ii) and $(\mathrm{ii})^0$ both hold, by Theorem 4.2, while $(\mathrm{iii})^0$ holds, by [15, cor. II.16.3].

The results proved suffice to establish all the equivalences claimed in the statement of the theorem. The final claim of the theorem follows from Theorem 0.3 and the fact that a surjective morphism between $\mathbb{T}_{\mathfrak{m}}$-modules which are both free of rank one is necessarily an isomorphism. □

Proof of Theorem 0.6. We begin by proving part (i). As usual, we let n denote the numerator of $(p-1)/12$, expressed in lowest terms. We first note that $\mathcal{M}^0/I$ is of order n, by Proposition 1.15. Thus in order to prove the theorem, we must show that the morphism

$$\mathcal{X}^0 \otimes_{\mathbb{T}^0} \mathcal{X}^0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z}), \tag{5.2}$$

induced by the restriction of the pairing of Definition 3.4 to $\mathcal{X}^0$, has a cokernel which is annihilated by I and is of order equal to n. (Note that the morphism appearing in the statement of Theorem 0.6 is obtained by composing (5.2) with the isomorphism of Proposition 1.3 (ii).) For this it suffices to show, for each prime ℓ, that the morphism

$$\mathcal{X}^0 \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \otimes_{\mathbb{T}^0 \otimes_{\mathbb{Z}} \mathbb{Z}_\ell} \mathcal{X}^0 \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell, \mathbb{Z}_\ell)$$

obtained by tensoring (5.2) through with $\mathbb{Z}_\ell$ over $\mathbb{Z}$, which is induced by the pairing (3.19), has cokernel annihilated by I and of order equal to the maximal power of ℓ dividing n.

The proof will be similar to that of Theorem 0.3. Namely, we fix ℓ, and apply Proposition 2.8, taking $A = \mathbb{Z}_\ell$, $B = \mathbb{T}^0 \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, and $U = V = \mathcal{X}^0 \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. That the hypotheses of Proposition 2.8 are satisfied follows from Corollaries 4.10 and 3.20 (ii), and Theorem 4.2 (just as in the proof of Theorem 0.3). The desired conclusion then follows from Lemma 3.16 (ii).

As for the proof of part (ii), it follows by similar observations to those made in the proof of Theorem 0.4. Indeed, to prove that $\mathbb{T}^0 \longrightarrow \mathrm{End}_{\mathbb{T}^0}(\mathcal{X}^0)$ is an isomorphism, it suffices to prove that we obtain an isomorphism after tensoring this morphism through by $\mathbb{Z}_\ell$, for each prime number ℓ. Lemma 2.6 shows that it suffices to prove that $\mathcal{X}^0/\ell$ is a faithful $\mathbb{T}^0/\ell$-module, for each prime number ℓ. Equivalently, it suffices to show that $\mathcal{X}^0_{\mathfrak{m}}/\ell$ is a faithful $\mathbb{T}^0_{\mathfrak{m}}/\ell$-module for each maximal ideal of $\mathbb{T}^0$ of residue characteristic ℓ. That this is the case was observed in the course of verifying the hypotheses of Proposition 2.8 in the proof of part (i). □

Proof of Theorem 0.10. Both claims of Theorem 0.10 follow from Lemma 2.4, the properties of the $\mathbb{T}$-module $\mathcal{X}$ and the $\mathbb{T}^0$-module $\mathcal{X}^0$ shown in the proofs of Theorems 0.3 and 0.6, and the isomorphisms of Proposition 1.3, once one notes that the pairings $\mathcal{X} \times \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}, \mathbb{Z}) \longrightarrow \mathbb{Z}$ and $\mathcal{X}^0 \times \mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}^0, \mathbb{Z}) \longrightarrow \mathbb{Z}$ are perfect by definition. □

6. Some remarks on the case when $\mathbb{T}_{\mathfrak{m}}$ is non-Gorenstein

We begin this section by discussing a general commutative algebra framework within which our results can be interpreted.

Definition 6.1. Let A be a reduced Noetherian complete one-dimensional local ring, and let Ω denote a dualizing module for A.

(i) We say that an A-module U is a weak local theta-characteristic for A if it is locally free of rank one when localized away from the maximal ideal of A, and if there is an isomorphism of A-modules $U \xrightarrow{\sim} \mathrm{Hom}_A(U, \Omega)$.

(ii) We say that U is a strong local theta-characteristic for A if it is a weak local theta-characteristic, and if the natural map $A \to \mathrm{End}_A(U)$ is an isomorphism.

If A is Gorenstein, then we can take $\Omega = A$, and so A itself is a strong local theta-characteristic. If A is arbitrary, and we let $\tilde{A}$ denote the normalization of A, then $\mathrm{Hom}_A(\tilde{A}, \Omega)$ is a dualizing sheaf for the regular ring $\tilde{A}$, and so is isomorphic to $\tilde{A}$. Since $\tilde{A}$ is isomorphic to A when localized away from the maximal ideal of A, we see that $\tilde{A}$ is a weak local theta-characteristic for A. (This example was explained to the author by Kovács.) However, since $\tilde{A}$ acts on itself through multiplication via A-linear endomorphisms, we see that $\tilde{A}$ is not a strong local theta-characteristic for A unless $A = \tilde{A}$; that is, unless A itself is normal.

If $\mathfrak{m}$ is any maximal ideal of the first type in $\mathbb{T}$, then the perfect pairing of Corollary 3.20 (ii) and the adjointness isomorphism (2.2) give rise to an isomorphism $\mathcal{X}^0_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}}(\mathcal{X}^0_{\mathfrak{m}}, \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T}^0_{\mathfrak{m}}, \mathbb{Z}_\ell))$. Since $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T}^0_{\mathfrak{m}}, \mathbb{Z}_\ell)$ is a dualizing module for the one-dimensional local ring $\mathbb{T}^0_{\mathfrak{m}}$, this isomorphism together with Theorem 0.4 shows that $\mathcal{X}^0_{\mathfrak{m}}$ is a strong local theta-characteristic for $\mathbb{T}^0_{\mathfrak{m}}$; in particular, the ring $\mathbb{T}^0_{\mathfrak{m}}$ does admit a strong local theta-characteristic. The preceding discussion shows that this is a weaker commutative algebra condition than being Gorenstein. In order to understand how much weaker, it is natural to ask the following question: does any reduced Noetherian complete one-dimensional local ring admit a strong local theta-characteristic? I don't know the answer.

We next apply the results of the preceding sections to draw some conclusions about the structure of the $\mathfrak{m}$-adic Tate module of $J_0(p)$ when $\mathbb{T}_{\mathfrak{m}}$ is non-Gorenstein.

Let us suppose that $\mathfrak{m}$ is an ordinary maximal ideal of $\mathbb{T}$ of the first type, of residue characteristic $\ell \neq p$. Then the proof of [7, 12.10] and the discussion of [16] show that the $\mathfrak{m}$-adic Tate module $T_{\mathfrak{m}}J_0(p)$ of $J_0(p)$ (that is, the localization at $\mathfrak{m}$ of the ℓ-adic Tate module of $J_0(p)$) sits in a short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}[\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)]$-modules

$$0 \longrightarrow T_{\mathfrak{m}}J_0(p)^0 \longrightarrow T_{\mathfrak{m}}J_0(p) \longrightarrow T_{\mathfrak{m}}J_0(p)^e \longrightarrow 0, \tag{6.2}$$

induced by the connected-étale short exact sequence of the ℓ-divisible group of the Néron model of $J_0(p)$ over $\mathbb{Z}_\ell$. Furthermore, $T_{\mathfrak{m}}J_0(p)^0$ is isomorphic to $\mathbb{T}^0_{\mathfrak{m}}$ as a $\mathbb{T}^0_{\mathfrak{m}}$-module, while $T_{\mathfrak{m}}J_0(p)^e$ is isomorphic to $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T}^0_{\mathfrak{m}}, \mathbb{Z}_\ell)$.

Proposition 6.3. *The short exact sequence* (6.2) *splits as a short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}$-modules if and only if $\mathbb{T}^0_{\mathfrak{m}}$ is Gorenstein.*

Proof. If $\mathbb{T}^0_{\mathfrak{m}}$ is Gorenstein, then $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathbb{T}^0_{\mathfrak{m}}, \mathbb{Z}_\ell)$ is isomorphic to $\mathbb{T}^0_{\mathfrak{m}}$, and so (6.2) is an extension of free $\mathbb{T}^0_{\mathfrak{m}}$-modules, and hence splits. Thus to complete the proof of the proposition, it remains to show that (6.2) is non-split if $\mathbb{T}^0_{\mathfrak{m}}$ is not Gorenstein.

Consider the short exact sequence

$$0 \longrightarrow J_0(p)[\ell]^0_{\mathfrak{m}} \longrightarrow J_0(p)[\ell]_{\mathfrak{m}} \longrightarrow J_0(p)[\ell]^e_{\mathfrak{m}} \longrightarrow 0 \tag{6.4}$$

obtained by tensoring (6.2) through by $\mathbb{Z}/\ell$ over $\mathbb{Z}_\ell$. We will show that (6.4) is non-split as a short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}/\ell$-modules.

Recall from Theorem 4.6 that $J_0(p)[\ell]_{\mathfrak{m}}$ is isomorphic to $\mathcal{X}^0_{\mathfrak{m}}/\ell \oplus \mathcal{X}^0_{\mathfrak{m}}/\ell$ as a $\mathbb{T}^0_{\mathfrak{m}}/\ell$-module. Thus (6.4) is isomorphic (as a short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}/\ell$-modules) to a short exact sequence of the form

$$0 \longrightarrow \mathbb{T}^0_{\mathfrak{m}}/\ell \longrightarrow \mathcal{X}^0_{\mathfrak{m}}/\ell \oplus \mathcal{X}^0_{\mathfrak{m}}/\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}/\ell}(\mathbb{T}^0_{\mathfrak{m}}/\ell, \mathbb{Z}/\ell) \longrightarrow 0.$$

It follows from the following lemma that there are no injective morphisms of $\mathbb{T}^0_{\mathfrak{m}}/\ell$-modules from $\mathrm{Hom}_{\mathbb{Z}/\ell}(\mathbb{T}^0_{\mathfrak{m}}/\ell, \mathbb{Z}/\ell)$ to $\mathcal{X}^0_{\mathfrak{m}}/\ell \oplus \mathcal{X}^0_{\mathfrak{m}}/\ell$, and so such a short exact sequence is necessarily non-split. □

Before proving the next lemma, we note that if $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ of residue characteristic ℓ, then the surjection $\mathbb{T}^0_{\mathfrak{m}}/\ell \longrightarrow \mathbb{T}^0_{\mathfrak{m}}/\mathfrak{m}$ allows us to regard $\mathrm{Hom}_{\mathbb{Z}/\ell}(\mathbb{T}^0_{\mathfrak{m}}/\mathfrak{m}, \mathbb{Z}/\ell)$ as a submodule of $\mathrm{Hom}_{\mathbb{Z}/\ell}(\mathbb{T}^0_{\mathfrak{m}}/\ell, \mathbb{Z}/\ell)$.

Lemma 6.5. *If $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ of residue characteristic ℓ for which $\mathbb{T}^0_{\mathfrak{m}}$ is not Gorenstein, then any morphism from $\mathrm{Hom}_{\mathbb{Z}/\ell}(\mathbb{T}^0_{\mathfrak{m}}/\ell, \mathbb{Z}/\ell)$ to $\mathcal{X}^0_{\mathfrak{m}}/\ell$ contains $\mathrm{Hom}_{\mathbb{Z}/\ell}(\mathbb{T}^0/\mathfrak{m}, \mathbb{Z}/\ell)$ in its kernel.*

Proof. Note that since $\mathbb{T}^0_{\mathfrak{m}}$ is assumed to be non-Gorenstein, Theorem 1.14 shows that the maximal ideal $\mathfrak{m}$ is necessarily of the first type. We will write $A = \mathbb{Z}/\ell$, $B = \mathbb{T}^0_{\mathfrak{m}}/\ell$, and $U = \mathcal{X}^0_{\mathfrak{m}}/\ell$. Then A is a field, B is a non-Gorenstein Artinian local A-algebra, and U is a B-module which is of the same dimension as B as an A-vector space, and which is isomorphic to its A-dual $\mathrm{Hom}_A(U, A)$ as a B-module. (This follows from Corollary 3.20 (ii), since $\mathfrak{m}$ is of the first type.)

Let $\mathfrak{n}$ denote the maximal ideal of B. We will show that if A, B and U satisfy the conditions laid out in the preceding paragraph, then any morphism of B-modules $\phi : \mathrm{Hom}_A(B, A) \longrightarrow U$ necessarily contains $\mathrm{Hom}_A(B/\mathfrak{n}, A)$ in its kernel. Since $\mathrm{Hom}_A(B/\mathfrak{n}, A)$ is a one-dimensional $B/\mathfrak{n}$ vector space, if it is not in the kernel of ϕ then ϕ induces an injection $\mathrm{Hom}_A(B/\mathfrak{n}, A) \longrightarrow U$. Dualizing ϕ over A, we obtain a

morphism $\psi : \mathrm{Hom}_A(U, A) \longrightarrow B$ which induces a surjection $\mathrm{Hom}_A(U, A) \longrightarrow B/\mathfrak{n}$. Thus ψ is itself a surjection, and since its source and target are of the same dimension over A, ψ is an isomorphism. But this is impossible, since $\mathrm{Hom}_A(U, A) \xrightarrow{\sim} U$ is an A-self-dual B-module, while B is not, being non-Gorenstein by assumption. We conclude that $\mathrm{Hom}_A(B/\mathfrak{n}, A)$ is in the kernel of ϕ, as claimed. □

Proposition 6.3 should be contrasted with the fact that $T_{\mathfrak{m}} J_0(p)$ sits in a short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-modules

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{X}^0_{\mathfrak{m}}, \mathbb{Z}_\ell(1)) \longrightarrow T_{\mathfrak{m}} J_0(p) \longrightarrow \mathcal{X}^0_{\mathfrak{m}} \longrightarrow 0,$$

which *is* split as a short exact sequence of $\mathbb{T}^0_{\mathfrak{m}}$-modules (as is proved by an obvious extension of the argument that proves Theorem 4.6). (Of course, the proof of Proposition 6.3 makes it clear that it is precisely because this latter exact sequence splits that the exact sequence (6.2) does not split when $\mathbb{T}^0_{\mathfrak{m}}$ is non-Gorenstein.)

We close this section by describing concretely the $\mathbb{T}^0_{\mathfrak{m}}/2$-module $\mathcal{X}^0_{\mathfrak{m}}/2$ in the particular case when $\mathfrak{m}$ is a non-Gorenstein maximal ideal of residue characteristic 2 for which $\mathbb{T}^0_{\mathfrak{m}}/2$ has length four. Writing $k = \mathbb{T}^0_{\mathfrak{m}}/\mathfrak{m}$, we note that $\mathbb{T}^0_{\mathfrak{m}}/2$ is then isomorphic to $k[x, y, z]/(x^2, y^2, z^2, xy, xz, yz)$. (One checks that this is the unique non-Gorenstein local ring of length four of characteristic 2 having residue field k.) When $p = 431$ or 503, $\mathbb{T}$ has a maximal ideal $\mathfrak{m}$ for which the completion $\mathbb{T}^0_{\mathfrak{m}}$ is non-Gorenstein and of rank four over $\mathbb{Z}_2$ [14], and so our description applies in particular to these cases.

Lemma 6.6. *If $\mathbb{T}^0_{\mathfrak{m}}$ is non-Gorenstein and $\mathbb{T}^0_{\mathfrak{m}}/2$ is of length four, then $\mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]$ has rank two over $\mathbb{Z}/2$, and is equal to $\mathfrak{m}\mathcal{X}^0_{\mathfrak{m}}/2$.*

Proof. Write d for the dimension of $\mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]$ over k. Applying Lemma 4.4 with $W = \mathbb{T}^0_{\mathfrak{m}}/\mathfrak{m}$ shows that $\mathcal{X}^0_{\mathfrak{m}}/\mathfrak{m}$ also has dimension d. The short exact sequence

$$0 \longrightarrow \mathfrak{m}\mathcal{X}^0_{\mathfrak{m}}/2 \longrightarrow \mathcal{X}^0_{\mathfrak{m}}/2 \longrightarrow \mathcal{X}^0_{\mathfrak{m}}/\mathfrak{m} \longrightarrow 0$$

then shows that $\mathfrak{m}\mathcal{X}^0_{\mathfrak{m}}/2$ has dimension $4 - d$. Since $\mathfrak{m}^2\mathbb{T}^0_{\mathfrak{m}}/2 = 0$, we see that $\mathfrak{m}\mathcal{X}^0_{\mathfrak{m}}/2 \subset \mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]$, and so $\mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]$ has dimension at least $4 - d$. Thus we see that $d \geq 2$.

Since Corollary 4.10 shows that $\mathcal{X}^0_{\mathfrak{m}}/2$ is a faithful $\mathbb{T}^0_{\mathfrak{m}}/2$-module, we see that the natural map $\mathfrak{m}\mathbb{T}^0_{\mathfrak{m}}/2 \to \mathrm{End}_{\mathbb{T}^0_{\mathfrak{m}}/2}(\mathcal{X}^0_{\mathfrak{m}}/2)$ is injective. The image of this map lies in

$$\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/2}((\mathcal{X}^0_{\mathfrak{m}}/2)/(\mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]), \mathfrak{m}\mathcal{X}^0_{\mathfrak{m}}/2).$$

Since $\mathfrak{m}\mathbb{T}^0_{\mathfrak{m}}/2$ has dimension three, while $\mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/2}((\mathcal{X}^0_{\mathfrak{m}}/2)/(\mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]), \mathfrak{m}\mathcal{X}^0_{\mathfrak{m}}/2)$ has dimension $(4 - d)^2$, we see that $d \leq 2$. Combining this calculation with that of the preceding paragraph, we see that $d = 4 - d = 2$, and so deduce the lemma. □

The $\mathbb{T}^0_{\mathfrak{m}}/2$-action on $\mathcal{X}^0_{\mathfrak{m}}/2$ is determined by the action of the maximal ideal $\mathfrak{m}\mathbb{T}^0_{\mathfrak{m}}/2$ on $\mathcal{X}^0_{\mathfrak{m}}/2$. This action in turn is determined by the composite

$$\begin{aligned} \mathfrak{m}\mathbb{T}^0_{\mathfrak{m}}/2 &\longrightarrow \mathrm{Hom}_{\mathbb{T}^0_{\mathfrak{m}}/2}((\mathcal{X}^0_{\mathfrak{m}}/2)/(\mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]), \mathfrak{m}\mathcal{X}^0_{\mathfrak{m}}/2) \\ &= \mathrm{Hom}_k(\mathcal{X}^0_{\mathfrak{m}}/\mathfrak{m}, \mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]) \xrightarrow{\sim} \mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}] \otimes_k \mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]. \end{aligned} \tag{6.7}$$

The final isomorphism holds because Lemma 4.4 shows that the pairing $\mathcal{X}^0_{\mathfrak{m}}/2 \times \mathcal{X}^0_{\mathfrak{m}}/2 \longrightarrow \mathbb{Z}/2$ given by Corollary 3.20 (ii) induces a duality between the k-vector spaces $\mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}]$ and $\mathcal{X}^0_{\mathfrak{m}}/\mathfrak{m}$. Since the pairing of Corollary 3.20 (ii) is symmetric, the map (6.7) has image lying in the subspace $\mathrm{Sym}^2_k(\mathcal{X}^0_{\mathfrak{m}}/2[\mathfrak{m}])$ of symmetric tensors.

It is also injective (as was observed in the proof of Lemma 6.6) and so is an isomorphism, since $\mathfrak{m}\mathbb{T}^0_{\mathfrak{m}}/2$ and $\mathrm{Sym}^2_k(\mathcal{X}^0_{\mathfrak{m}}/2\,[\mathfrak{m}])$ both have dimension three over $\mathbb{T}^0/\mathfrak{m}$. Thus the $\mathbb{T}^0_{\mathfrak{m}}/2$-module structure on $\mathcal{X}^0_{\mathfrak{m}}/2$ is entirely determined by choosing an isomorphism of three-dimensional k-vector spaces $\mathfrak{m}\mathbb{T}^0_{\mathfrak{m}}/2 \xrightarrow{\sim} \mathrm{Sym}^2_{\mathbb{T}^0/\mathfrak{m}}(\mathcal{X}^0_{\mathfrak{m}}/2\,[\mathfrak{m}])$. This gives a complete description of the structure of $\mathcal{X}^0_{\mathfrak{m}}/2$ as a $\mathbb{T}^0_{\mathfrak{m}}/2$-module in the case when $\mathbb{T}^0_{\mathfrak{m}}/2$ is non-Gorenstein of length four.

7. The case of non-prime level

In this section, we will discuss the extension of our results to the case of non-prime level. Unfortunately, the lack of control over Eisenstein primes in this situation, as well as the possibility of primes of fusion between old and new forms, means that our results are weaker than in the case of prime level. This is the primary reason for relegating them to this final section of the paper.

We begin by generalizing the notation introduced in sections 1 and 3. If N is a positive integer we write $\mathcal{N}(N)$ for the space of weight two modular forms $f = \sum_{n=0}^{\infty} a_n q^n$ on $\Gamma_0(N)$ for which $a_n \in \mathbb{Z}$ $(n \geq 1)$, $\mathcal{N}(N)^0$ for the submodule of $\mathcal{N}(N)$ consisting of cusp forms, and $\mathcal{N}(N)^{\mathrm{Eis}}$ for the submodule of $\mathcal{N}(N)$ spanned by Eisenstein series.

We let $\mathbb{T}$ denote the finite $\mathbb{Z}$-algebra of Hecke operators acting on $\mathcal{N}(N)$, $\mathbb{T}^0$ the quotient of $\mathbb{T}$ that acts faithfully on $\mathcal{N}(N)^0$, and $\mathbb{T}^{\mathrm{Eis}}$ the quotient of $\mathbb{T}$ that acts faithfully on $\mathcal{N}(N)^{\mathrm{Eis}}$.

We have the following generalization of Proposition 1.3 (whose proof can be found in the same reference given for the proof of that proposition).

Proposition 7.1. (i) *There is a natural isomorphism of* $\mathbb{T}$*-modules* $\mathcal{N}(N) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z})$, *defined by the pairing* $\langle f, T\rangle = a_1(f|T)$.

(ii) *There is a natural isomorphism of* $\mathbb{T}^0$*-modules* $\mathcal{N}(N)^0 \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}^0, \mathbb{Z})$, *defined by the same pairing as that of part* (i).

Now suppose that $N = Mp$, where p is a prime which does not divide M. We let V_p denote the "degeneracy operator" $f(q) \mapsto f(q^p)$, which yields a morphism $\mathcal{N}(M) \longrightarrow \mathcal{N}(Mp)$. The $\mathbb{Z}$-submodule $\mathcal{N}(M) + \mathcal{N}(M)|V_p$ of $\mathcal{N}(N)$ is stable under $\mathbb{T}$, and we let $\mathbb{T}_{\mathrm{old}}$ denote the quotient of $\mathbb{T}$ that acts faithfully on it. We let $\mathcal{N}(N)_{\mathrm{old}}$ denote the maximal $\mathbb{T}$-submodule of $\mathcal{N}(N)$ on which the $\mathbb{T}$-action factors through $\mathbb{T}_{\mathrm{old}}$. Then $\mathcal{N}(N)_{\mathrm{old}}$ is the saturation of $\mathcal{N}(M) + \mathcal{N}(M)|V_p$ in $\mathcal{N}(N)$, and so it contains $\mathcal{N}(M) + \mathcal{N}(M)|V_p$ with finite index. Similarly, we write $\mathcal{N}(N)^0_{\mathrm{old}} = \mathcal{N}(N)^0 \cap \mathcal{N}(N)_{\mathrm{old}}$ and $\mathcal{N}(N)^{\mathrm{Eis}}_{\mathrm{old}} = \mathcal{N}(N)^{\mathrm{Eis}} \cap \mathcal{N}(N)_{\mathrm{old}}$. (Here the subscript "old" stands for "old at p".)

The quotient of $\mathcal{N}(N)^{\mathrm{Eis}}$ by $\mathcal{N}(N)^{\mathrm{Eis}}_{\mathrm{old}}$ is a free $\mathbb{Z}$-module of rank one. Let E denote the weight two Eisenstein series on $\Gamma_0(p)$, let $\Sigma = \{\ell_1, \ell_2, \ldots, \ell_t\}$ denote the set of primes dividing M, and set

$$E_{\mathrm{new}} = E(q) - \sum_{\ell \in \Sigma} E(q^\ell) + \sum_{\substack{\ell_\alpha, \ell_\beta \in \Sigma \\ 1 \leq \alpha < \beta \leq t}} E(q^{\ell_\alpha \ell_\beta}) - \cdots + (-1)^t E(q^{\ell_1 \cdots \ell_t}).$$

(Here and below, the subscript "new" stands for "new at p".) Then E_{new} is a normalized $\mathbb{T}$-eigenform characterized by the conditions

$$E_{\mathrm{new}}|T_\ell = \begin{cases} (1+\ell)E_{\mathrm{new}} \text{ if } \ell \text{ does not divide } N, \\ \ell E_{\mathrm{new}} \text{ if } \ell \text{ divides } M, \\ E_{\mathrm{new}} \text{ if } \ell = p, \end{cases}$$

as ℓ ranges over all primes. One easily sees that E_{new} does not lie in $\mathcal{N}(N)^{\mathrm{Eis}}_{\mathrm{old}}$, and so its image generates the quotient $\mathcal{N}(N)^{\mathrm{Eis}}/\mathcal{N}(N)^{\mathrm{Eis}}_{\mathrm{old}}$.

We let $\mathbb{T}^{\mathrm{Eis}}_{\mathrm{new}}$ denote the quotient of $\mathbb{T}^{\mathrm{Eis}}$ which acts faithfully on E_{new}. As a ring, $\mathbb{T}^{\mathrm{Eis}}_{\mathrm{new}}$ is isomorphic to $\mathbb{Z}$. We let $\mathcal{N}(N)^0_{\mathrm{new}}$ denote the maximal $\mathbb{Z}$-submodule of $\mathcal{N}(N)^0$ orthogonal to $\mathcal{N}(N)^0_{\mathrm{old}}$ under the Petersson inner product, and write $\mathbb{T}^0_{\mathrm{new}}$ for the quotient of $\mathbb{T}^0$ which acts faithfully on $\mathcal{N}(N)^0_{\mathrm{new}}$. We also write $\mathbb{T}_{\mathrm{new}}$ for the image of $\mathbb{T}$ in $\mathbb{T}^{\mathrm{Eis}}_{\mathrm{new}} \oplus \mathbb{T}^0_{\mathrm{new}}$, and write $\mathcal{N}(N)_{\mathrm{new}}$ for the maximal $\mathbb{T}$-submodule of $\mathcal{N}(N)$ on which the $\mathbb{T}$-action factors through $\mathbb{T}_{\mathrm{new}}$ (so that $\mathcal{N}(N)_{\mathrm{new}}$ is the saturation in $\mathcal{N}(N)$ of the submodule spanned by $\mathcal{N}(N)^0_{\mathrm{new}}$ and E_{new}). We have defined $\mathcal{N}(N)_{\mathrm{new}}$ in such a way that the natural map $\mathcal{N}(N)_{\mathrm{new}} \oplus \mathcal{N}(N)_{\mathrm{old}} \to \mathcal{N}(N)$ is an injection of $\mathbb{T}$-modules whose cokernel is finite.

The modular curve $X_0(N)$ (regarded as a scheme over $\mathbb{Z}_p$) has semi-stable reduction modulo p. Its geometric fibre in characteristic p consists of two irreducible components. The specializations of the cusps 0 and ∞ of $X_0(N)$ lie on different components; let us label the two components $\mathcal{C}_0$ and $\mathcal{C}_\infty$, according to which of these two specializations they contain. Each of these components is naturally isomorphic to $X_0(M)_{/\overline{\mathbb{F}}_p}$ (which is a smooth curve, because p does not divide M). The two components meet transversally at the points corresponding to supersingular elliptic curves. More precisely, if the point x on $\mathcal{C}_\infty$ corresponds to the pair (E, C) consisting of a supersingular elliptic curve E and a cyclic subgroup of E of order M, then x is identified with the point on $\mathcal{C}_0$ obtained by taking the Frobenius twist of the pair (E, C). Let $\mathcal{S} = \{x_0, \ldots, x_s\}$ denote the collection of singular points on $X_0(N)_{/\overline{\mathbb{F}}_p}$. By regarding each x_i as a point on $\mathcal{C}_\infty$, we may regard it as corresponding to a pair (E_i, C_i) as above, well determined up to isomorphism.

We let $\mathcal{X}$ denote the $\mathbb{Z}$-module of divisors supported on the set $\mathcal{S}$, and let $\mathcal{X}^0$ denote the submodule of $\mathcal{X}$ consisting of divisors of degree zero. There is a natural action of $\mathbb{T}$ on $\mathcal{X}$ and $\mathcal{X}^0$, which makes $\mathcal{X}$ a faithful $\mathbb{T}_{\mathrm{new}}$-module, and makes $\mathcal{X}^0$ a faithful $\mathbb{T}^0_{\mathrm{new}}$-module.

Let $J_0(N)$ denote the Jacobian of $X_0(N)_{/\mathbb{Q}}$. It is an abelian variety over $\mathbb{Q}$, the special fibre of whose Néron model over $\mathbb{Z}_p$ has a semi-abelian connected component (that is, is the extension of an abelian variety by a torus). We let $T_0(N)$ denote the maximal torus of this semi-abelian variety. There is a natural identification of $\mathcal{X}^0$ with the character lattice of $T_0(N)$.

There is a monodromy pairing $\langle\, , \rangle : \mathcal{X} \times \mathcal{X} \longrightarrow \mathbb{Z}$, defined by the formula $\langle x_i, x_j \rangle = \dfrac{1}{2}\delta_{i,j} \# \operatorname{Aut}((E_i, C_i))$. This morphism is not $\mathbb{T}$-bilinear if $M > 1$. However, it is easily modified to be so. As usual, let w_M denote the Atkin-Lehner involution on $X_0(M)$, and define $[\, , \,] : \mathcal{X} \times \mathcal{X} \longrightarrow \mathbb{Z}$ by the formula $[x, y] = \langle x, w_M y \rangle$. The morphism $[\, , \,]$ *is* $\mathbb{T}$-bilinear, and so induces a morphism of $\mathbb{T}$-modules

$$\mathcal{X} \longrightarrow \operatorname{Hom}(\mathcal{X}, \mathbb{Z}), \tag{7.2}$$

which is injective (and hence has finite cokernel). (For the assertions of the last several paragraphs concerning the geometry of $X_0(N)$, we refer to sections 2 and 3 of [20], and the references cited therein.)

The discussion of section 2 (in particular the adjointness isomorphism (2.2)) together with Proposition 7.1 shows that (7.2) induces a $\mathbb{T}$-linear morphism

$$\theta : \mathcal{X} \otimes_{\mathbb{T}} \mathcal{X} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z}) \xrightarrow{\sim} \mathcal{N}(N).$$

In fact, since $\mathcal{X}$ is a $\mathbb{T}_{\mathrm{new}}$-module, the image of θ lies in $\mathcal{N}(N)_{\mathrm{new}}$. Similarly to the case when $M = 1$, this morphism is closely related to the construction of certain theta series from quaternion algebras. However, the details are more complicated when $M > 1$.

If x_i and x_j are two elements of $\mathcal{S}$, corresponding to the pairs (E_i, C_i) and (E_j, C_j) of supersingular elliptic curves and cyclic subgroups of order M, then we define $L_{i,j} = \mathrm{Hom}((E_i, C_i), (E_j, C_j))$ to be the $\mathbb{Z}$-submodule of $\mathrm{Hom}(E_i, E_j)$ consisting of those homomorphisms $\phi : E_i \longrightarrow E_j$ for which $\phi(C_i) \subset C_j$, equipped with the positive definite quadratic form given by taking the degree of an isogeny. The quadratic space $L_{i,j}$ is rank four of level $N = Mp$. (In other words, if $L_{i,j}^*$ denotes the dual lattice to $L_{i,j}$, the cokernel of the injection $L_{i,j} \to L_{i,j}^*$ induced by the quadratic form on $L_{i,j}$ has exponent Mp.)

If d is a divisor of M, then for any cyclic subgroup C of order M, we let $C[d]$ denote the unique subgroup of C of order d. Then, given x_i and x_j as in the preceding paragraph, define the quadratic space $L_{i,j}^{(d)}$ to be

$$L_{i,j}^{(d)} = \mathrm{Hom}((E_i/C_i[d], C_i/C_i[d]), (E_j, C_j[M/d])),$$

regarded as the quadratic subspace of $L_{i,j}$ consisting of homomorphisms containing $C_i[d]$ in their kernel.

As above, let $\Sigma = \{\ell_1, \cdots, \ell_t\}$ be the collection of prime factors of M.

Proposition 7.3. *If x_i and x_j are any two elements of $\mathcal{S}$, then*

$$\theta(x_i \otimes w_M x_j) = \frac{1}{2}\Theta(L_{i,j}) - \sum_{\ell \in Q} \frac{1}{2}\Theta(L_{i,j}^{(\ell)}) + \sum_{\substack{\ell_\alpha, \ell_\beta \in Q \\ 1 \le \alpha < \beta \le t}} \frac{1}{2}\Theta(L_{i,j}^{(\ell_\alpha \ell_\beta)}) - \cdots + (-1)^t \frac{1}{2}\Theta(L_{i,j}^{(\ell_1 \cdots \ell_t)}).$$

Proof. If n is a positive integer, then

$$\begin{aligned} a_n(\theta(x_i \otimes w_M x_j)) &= a_1(\theta(x_i \otimes w_M x_j)|T_n) = a_1(\theta(T_n x_i \otimes w_M x_j)) = [T_n x_i, w_M x_j] \\ &= \langle T_n x_i, x_j \rangle = \frac{1}{2} \text{ the number of cyclic } n\text{-isogenies } \phi : E_i \longrightarrow E_j \text{ for which} \\ &\qquad \ker(\phi) \cap C_i \text{ is trivial and } \phi(C_i) \text{ equals } C_j \\ &\qquad = \frac{1}{2} \text{ the number of } \phi \in L_{i,j} \text{ for which } \ker(\phi) \cap C_i \text{ is trivial.} \end{aligned}$$

If ϕ is an element of $L_{i,j}$ for which $\ker(\phi) \cap C_i \neq 0$, then $\ker(\phi) \supset C_i[q]$ for some prime q dividing M, and so $\phi \in L_{i,j}^{(q)}$. The formula of the proposition now follows directly by inclusion-exclusion counting. □

We remark that, analogously to Propositions 3.11 and 3.15, this result gives an algebro-geometric proof that certain linear combinations of theta series are modular

forms. In fact, if $M > 1$, then the modular forms in $\mathcal{N}(N)_{\text{new}}$ have vanishing constant term, and so in contrast to the situation of Proposition 3.15, the question of finding an algebro-geometric determination of the constant term of a theta-series does not arise.

It is natural to ask for a description of the image of θ. Proposition 7.3 shows that answering this question is closely related to describing the $\mathbb{Z}$-submodule of $\mathcal{N}(N)$ spanned by theta series. We begin by observing that it is easy to answer the question after tensoring through by $\mathbb{Q}$ over $\mathbb{Z}$.

Proposition 7.4. *The morphism*

$$\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q} \otimes_{\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}} \mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathcal{N}(N)_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$$

induced by θ is an isomorphism of free $\mathbb{T}_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$-modules of rank one.

Similarly, the morphism

$$\mathcal{X}^0 \otimes_{\mathbb{Z}} \mathbb{Q} \otimes_{\mathbb{T}^0 \otimes_{\mathbb{Z}} \mathbb{Q}} \mathcal{X}^0 \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathcal{N}(N)^0_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$$

induced by θ is an isomorphism of free $\mathbb{T}^0_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$-modules of rank one.

Proof. The ring $\mathbb{T}_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a reduced $\mathbb{Q}$-algebra (as follows from the results of [1]), and both $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathcal{N}(N)_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$ are faithful $\mathbb{T}_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$-modules of the same dimension over $\mathbb{Q}$ as $\mathbb{T}_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$. Thus they are free $\mathbb{T}_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$-modules of rank one. Since the pairing $\mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q} \times \mathcal{X} \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathbb{Q}$ induced by $[\,,\,]$ is perfect, Lemma 2.4 yields the first claim of the proposition. The second can be proved in a similar fashion, or by localizing the isomorphism just proved at the direct summand $\mathbb{T}^0_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$ of $\mathbb{T}_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Q}$. □

This result has the following corollary, originally due to Hijikata and Saito [12].

Corollary 7.5. *The $\mathbb{Q}$-vector space $\mathcal{N}(N) \otimes_{\mathbb{Z}} \mathbb{Q}$ is spanned by $\mathcal{N}(N)_{\text{old}} \otimes_{\mathbb{Z}} \mathbb{Q}$ together with the theta series $\Theta(L_{i,j}^{(d)})$, as x_i and x_j range over the basis $\mathcal{S}$ of $\mathcal{X}$, and d ranges over all products of primes from the set Q.*

Proof. This follows from Propositions 7.3 and 7.4 and the fact that the natural morphism $\mathcal{N}(N)_{\text{old}} \oplus \mathcal{N}(N)_{\text{new}} \longrightarrow \mathcal{N}(N)$ becomes an isomorphism after tensoring through with $\mathbb{Q}$ over $\mathbb{Z}$. □

As for describing the image of θ in the $\mathbb{Z}$-module $\mathcal{N}(N)$, when $M > 1$ we are not as successful as in the case when $M = 1$. Just as in that case, we would like to proceed by analyzing the morphism induced by θ after completing at all the maximal ideals $\mathfrak{m}$ of $\mathbb{T}$. If $\mathfrak{m}$ is such a maximal ideal of residue characteristic ℓ, then there is a semi-simple Galois representation $\rho_{\mathfrak{m}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(\mathbb{T}/\mathfrak{m})$ attached in a canonical fashion to $\mathfrak{m}$, characterized by the fact that for any prime q not dividing $N\ell$, the representation $\rho_{\mathfrak{m}}$ is unramified at q, and the characteristic polynomial of $\rho_{\mathfrak{m}}(\text{Frob}_q)$ is equal to $X^2 - T_q X + q$. Unfortunately we do not have control over the completion $\mathcal{X}_{\mathfrak{m}}$ without making some restrictive hypotheses on both $\mathfrak{m}$ and $\rho_{\mathfrak{m}}$, and these same hypotheses are then required to draw inferences concerning the image of the map induced by θ.

Theorem 7.6. *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ which is p-new and for which $\rho_{\mathfrak{m}}$ is irreducible. Suppose in addition that*

(i) *the residue characteristic ℓ of $\mathfrak{m}$ is odd, and ℓ^2 does not divide N;*

(ii) *$\mathfrak{m}$ is not a prime of fusion between ℓ-old and ℓ-new forms in $\mathcal{N}(N)^0$ (this is automatic if ℓ does not divide N, since then $\mathcal{N}(N)^0$ contains no ℓ-new forms);*

(iii) *if* $\mathfrak{m}$ *is a prime of fusion between* p*-old and* p*-new forms in* $\mathcal{N}(N)^0$*, then at least one of the following holds:* (a) ℓ *does not divide* $p-1$*, or* (b) $\rho_{\mathfrak{m}}(\mathrm{Frob}_p)$ *does not act as a scalar.*

Then the morphism $\mathcal{X}_{\mathfrak{m}} \otimes_{\mathbb{T}_m} \mathcal{X}_{\mathfrak{m}} \longrightarrow (\mathcal{N}(N)_{\mathrm{new}})_{\mathfrak{m}}$ *induced by* θ *is an isomorphism of free* $(\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}}$*-modules of rank one.*

Proof. We first note that since $\rho_{\mathfrak{m}}$ is irreducible, the natural maps $\mathbb{T}_{\mathfrak{m}} \longrightarrow \mathbb{T}^0_{\mathfrak{m}}$, $(\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}} \longrightarrow (\mathbb{T}^0_{\mathrm{new}})_{\mathfrak{m}}$, and $\mathcal{X}^0_{\mathfrak{m}} \longrightarrow \mathcal{X}_{\mathfrak{m}}$ are isomorphisms. We next observe that $\mathcal{X}_{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Q}$ is free of rank one over $(\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Q}$, by Proposition 7.4. Suppose we can prove that $\mathcal{X}/\mathfrak{m}$ is one-dimensional over $\mathbb{T}/\mathfrak{m} = \mathbb{T}_{\mathrm{new}}/\mathfrak{m}$; then since $(\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}}$ is reduced (by the results of [1]) we conclude that $\mathcal{X}_{\mathfrak{m}}$ is a free $(\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}}$-module of rank one. From [20, thm. 3.12/prop. 3.14/thm. 3.22] we deduce that the pairing $\mathcal{X}_{\mathfrak{m}} \times \mathcal{X}_{\mathfrak{m}} \longrightarrow \mathbb{Z}_\ell$ induced by $[\,,\,]$ is perfect. Lemma 2.4 now shows that the morphism $\mathcal{X}_{\mathfrak{m}} \otimes_{\mathbb{T}_{\mathfrak{m}}} \mathcal{X}_{\mathfrak{m}} \longrightarrow (\mathcal{N}(N)_{\mathrm{new}})_{\mathfrak{m}}$ is surjective. Since it becomes an isomorphism after tensoring with $\mathbb{Q}$ over $\mathbb{Z}$, by Proposition 7.4, and since its source is a free $(\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}}$-module of rank one, it must be an isomorphism between its source and target. This proves the theorem.

It remains to be shown that $\mathcal{X}/\mathfrak{m}$ is one-dimensional over $\mathbb{T}/\mathfrak{m}$. If ℓ is prime to N, this follows from [21, prop. 1] and hypothesis (iii) in the statement of the theorem. (As already noted, when ℓ is prime to N, hypothesis (ii) is superfluous.) Now suppose that ℓ exactly divides N. Hypothesis (ii) and the discussion of [22, p. 180] shows that $\rho_{\mathfrak{m}}$ appears with multiplicity one in $J_0(N)[\mathfrak{m}](\overline{\mathbb{Q}})$. If $\rho_{\mathfrak{m}}$ is not p-old, then the main theorem of [20] (which applies to our situation even though ℓ divides N, since we have the requisite statement regarding multiplicity one) shows that $\rho_{\mathfrak{m}}$ is not finite at p, and the same argument as used to prove [23, thm. 2.3] shows that $\mathcal{X}/\mathfrak{m}$ is one-dimensional over $\mathbb{T}/\mathfrak{m}$. If, on the other hand, $\rho_{\mathfrak{m}}$ is p-old, then by assumption (ii) $\ell \neq p$, and the proof of [21, prop. 1] then extends to again show that $\mathcal{X}/\mathfrak{m}$ is one-dimensional over $\mathbb{T}/\mathfrak{m}$ (the point as usual being that we have the requisite multiplicity one statement for $J_0(N)[\mathfrak{m}](\overline{\mathbb{Q}})$). □

Let S denote the following set of primes:

$$\begin{aligned} S = &\{\ell \,|\, \ell^2 \text{ divides } 4N\} \\ &\cup \{\ell \,|\, \ell \text{ is a congruence prime between } \mathcal{N}(N)^{\mathrm{Eis}} \text{ and } \mathcal{N}(N)^0\} \\ &\cup \{\ell \,|\, \ell \text{ is a congruence prime between } \ell\text{-old and } \ell\text{-new forms in } \mathcal{N}(N)^0\} \\ &\cup \{\ell \,|\, \ell \text{ is a congruence prime between } p\text{-old and } p\text{-new forms in } \mathcal{N}(N)^0\}. \end{aligned}$$

Corollary 7.7. *The* $\mathbb{Z}$*-module spanned by* $\mathcal{N}(N)^0_{\mathrm{old}}$*, together with the image of the map* $\mathcal{X}^0 \otimes_{\mathbb{T}^0} \mathcal{X}^0 \longrightarrow \mathcal{N}(N)^0_{\mathrm{new}}$ *induced by* θ*, has index in* $\mathcal{N}(N)^0$ *divisible only by primes in* S*.*

Proof. The set S contains all primes which occur as the residue characteristics of maximal ideals $\mathfrak{m}$ of $\mathbb{T}_{\mathrm{new}}$ which do not satisfy the hypotheses of Theorem 7.6, and so that theorem shows that the cokernel of the morphism $\mathcal{X}^0 \otimes_{\mathbb{T}^0} \mathcal{X}^0 \longrightarrow \mathcal{N}(N)^0_{\mathrm{new}}$ has order divisible only by primes in S. Furthermore, the index of $\mathcal{N}(N)^0_{\mathrm{new}} + \mathcal{N}(N)^0_{\mathrm{old}}$ in $\mathcal{N}(N)^0$ is divisible precisely by the primes of congruence between $\mathcal{N}(N)^0_{\mathrm{new}}$ and $\mathcal{N}(N)^0_{\mathrm{old}}$, and these are also contained in S. The theorem follows from these observations. □

Condition (ii) of Theorem 7.6, and hence the conclusion of the previous corollary, can be improved slightly by appealing to [22, thm. 2]. For example, suppose that

$p = 11$ and $M = 3$, so that $N = 33$. In this case there are no 11-old cusp forms, and so $\mathcal{N}(33)^0_{\text{new}} = \mathcal{N}(33)^0$ and $\mathbb{T}^0_{\text{new}} = \mathbb{T}^0$. The set S consists of the primes two, five (these are the congruence primes between $\mathcal{N}(N)^{\text{Eis}}$ and $\mathcal{N}(N)^0$) and three (which is a congruence prime between the 3-old and 3-new forms in $\mathcal{N}(33)^0$). However, since the 3-new quotient of $J_0(33)$ is an elliptic curve, [22, cor. to thm. 2] shows that any maximal ideal of residue characteristic three satisfies multiplicity one, and so the proof of Theorem 7.6 extends to cover these maximal ideals. We conclude that the set S in Corollary 7.7 can be replaced by the smaller set $S' = \{2, 5\}$. An explicit calculation shows in fact that the image of the map $\mathcal{X}^0 \otimes_{\mathbb{T}^0} \mathcal{X}^0 \longrightarrow \mathcal{N}(33)^0$ is of index ten in $\mathcal{N}(33)^0$.

Appendix. Supersingular points and p-adic periods of weight two modular forms

In this appendix we continue with the notation of section 7. In particular, we work in level $N = Mp$, with p not dividing M. We also assume that if $M = 1$, then $p \geq 5$ (so that p is then prime to 2Δ, where as before Δ denotes the denominator of $(p-1)/12$). Let $\Omega(\text{cusps})$ denote the dualizing sheaf of $X_0(N)$ over $\mathbb{Z}_p$, twisted by the invertible sheaf corresponding to the relative divisor of cusps in $X_0(N)$ over $\mathbb{Z}_p$. The Hecke correspondences act naturally on $H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\text{cusps}))$ (see [15, §II.6] for a discussion in the case when $M = 1$) and this action serves to make $H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\text{cusps}))$ a $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_p$-module. In fact, one has the more precise statement given by the following result.

Proposition A.1. *The $\mathbb{Z}_p$-module $H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\text{cusps}))$ is naturally a $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_p$-submodule of $\mathcal{N}(N) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ containing $\mathcal{N}(N)_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.*

Proof. We refer to [7, §8] for a discussion of the dualizing sheaf Ω of $X_1(N)$ over $\mathbb{Z}_p[\zeta]$ (where ζ is a primitive p^{th} root of unity) and its relation to weight-two cusp forms on $\Gamma_1(N)$. (Note that our N is Gross's Np.) In particular, [7, prop 8.4] shows that $H^0(X_1(N)_{/\mathbb{Z}_p[\zeta]}, \Omega)$ is a $\mathbb{Z}_p[\zeta]$-lattice inside the space of weight two cusp forms on $\Gamma_1(N)$ defined over $\mathbb{Q}_p(\zeta)$, which consists precisely of those cusp forms f such that both f and $f|w_\zeta$ have q-expansion coefficients lying in $\mathbb{Z}_p[\zeta]$.

An identical argument to the one that proves this result applies in our situation to show that $H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\text{cusps}))$ is a $\mathbb{Z}_p$-lattice inside $\mathcal{N}(N) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, consisting precisely of those modular forms for which both f and $f|w_p$ have q-expansion coefficients lying in $\mathbb{Z}_p$. (Here as usual w_p denotes the Atkin-Lehner involution at p on $\mathcal{N}(N) \otimes_{\mathbb{Z}} \mathbb{Q}_p = \mathcal{N}(Mp) \otimes_{\mathbb{Z}} \mathbb{Q}_p$.) Consequently, $H^0(X_0(N), \Omega(\text{cusps}))$ is contained in $\mathcal{N}(N)$, and the action of the Hecke correspondences on $H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\text{cusps}))$ is obtained by restricting the $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_p$-action on $\mathcal{N}(N) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. We thus conclude that $H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\text{cusps}))$ is a $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_p$-submodule of $\mathcal{N}(N) \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

To show that $H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\text{cusps}))$ contains $\mathcal{N}(N)_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$, it suffices to show that if $f \in \mathcal{N}(N)_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$, then both f and $f|w_p$ have q-expansion coefficients lying in $\mathbb{Z}_p$. By definition of $\mathcal{N}(N)$, all q-expansion coefficients of f lie in $\mathbb{Z}_p$, except perhaps the zeroth; that is to say, the constant term of f. However this constant term vanishes if $M > 1$, while if $M = 1$, then we have assumed that p does not divide 2Δ, and so this constant term lies in $\mathbb{Z}_p$ in this case as well, by virtue of Proposition 1.1. To see that all q-expansion coefficients of $f|w_p$ also lie in $\mathbb{Z}_p$, we note that $f|w_p = -f|T_p$ if $f \in \mathcal{N}(N)_{\text{new}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ (by an obvious modification of [1, lem. 7] or [20, prop. 3.7], each of which proves this in the cuspidal case). □

Recall that $\mathcal{S} = \{x_0, \dots, x_s\}$ denotes the set of singular points on the special fibre of $X_0(N)$, that $\mathcal{X}$ denotes the free $\mathbb{Z}$-module spanned by $\mathcal{S}$, and that each point $x_i \in \mathcal{S}$ corresponds to a supersingular elliptic curve E_i over $\overline{\mathbb{F}}_p$ together with a cyclic subgroup C_i of E_i of order M. We write $e_i = \frac{1}{2}\#\operatorname{Aut}((E_i, C_i))$.

Let W denote the Witt ring of $\overline{\mathbb{F}}_p$. After base-changing from $\mathbb{Z}$ to W, one finds (see the discussion of [20, p. 439]) that the formal completion of $X_0(N)$ at the point x_i in its special fibre is isomorphic to the formal spectrum of

$$W[[x,y]]/(xy - p^{e_i}) = W[[x, \frac{p^{e_i}}{x}]].$$

Denote this ring by A_i. By writing the ring A_i in terms of x rather than y, we are implicitly making a choice of orientation of the annulus obtained after passing to the rigid analytic fibre over $K = W \otimes_{\mathbb{Z}} \mathbb{Q}$ of $\operatorname{Spf} A_i$ (this annulus is the tube of the point x_i in the rigid analytic space underlying $X_0(N)_{/K}$). As explained in [2, §7], there is a canonical choice of orientation of this annulus, so that the "outer edge" is closer to the cusp ∞, while the "inner edge" is closer to the cusp 0. We may and do assume that the variables are labelled so that the differential dx/x yields this canonical orientation. The global sections of the dualizing sheaf of $\operatorname{Spf} A_i$ are a free $W[[x, \frac{p^{e_i}}{x}]]$-module of rank one spanned by dx/x, which we denote $\Omega(A_i)$, and we have a map $\operatorname{res}_i : \Omega(A_i) \longrightarrow W$ obtained by taking the residue of a section.

Proposition A.2. *The morphism*

$$H^0(X_0(N)_{/W}, \Omega(\text{cusps})) \longrightarrow \mathcal{X} \otimes_{\mathbb{Z}} W, \tag{A.3}$$

given by the formula $\omega \mapsto \sum_i \operatorname{res}_i(\omega_{|\operatorname{Spf} A_i})x_i$, *induces an isomorphism of* $\mathbb{T}^{\mathrm{new}}$*-modules*

$$H^0(X_0(N)_{/W}, \Omega(\text{cusps}))/(H^0(X_0(N)_{/W}, \Omega(\text{cusps})) \cap \mathcal{N}(N)_{\mathrm{old}} \otimes_{\mathbb{Z}} W) \xrightarrow{\sim} \mathcal{X} \otimes_{\mathbb{Z}} W.$$

Proof. That the map (A.3) is a morphism of $\mathbb{T}$-modules follows from the compatibility of the action of pulling-back or pushing-forward a differential via a map with the taking of residues of this differential. The elements of $H^0(X_0(N)_{/W}, \Omega(\text{cusps})) \cap \mathcal{N}(N)_{\mathrm{old}} \otimes_{\mathbb{Z}} W$ are rational multiples of pull-backs of differentials from $X_0(M)$, a curve with good reduction modulo p, and so have trivial residues along the supersingular annuli of $X_0(N)$. Thus (A.3) does induce a map

$$H^0(X_0(N)_{/W}, \Omega(\text{cusps}))/(H^0(X_0(N)_{/W}, \Omega(\text{cusps})) \cap \mathcal{N}(N)_{\mathrm{old}} \otimes_{\mathbb{Z}} W) \longrightarrow \mathcal{X} \otimes_{\mathbb{Z}} W.$$

The $\mathbb{T}$-actions on both the source and target of this map factor through $\mathbb{T}_{\mathrm{new}}$, and the source and target are both free W-modules of equal (finite) rank. Thus to show that this map is an isomorphism of $\mathbb{T}_{\mathrm{new}}$-modules, it suffices to prove that the map obtained by reducing (A.3) modulo p is surjective.

As remarked by Gross in [7, §8], the arguments of [15, §II.3] prove that the natural map $H^0(X_0(N)_{/W}, \Omega(\text{cusps})) \otimes_W k \longrightarrow H^0(X_0(N)_{/k}, \Omega(\text{cusps}))$ is an isomorphism. Let C_∞ and C_0 denote the components of $X_0(N)_{/k}$ containing the cusps ∞ and 0 respectively; they are both isomorphic to $X_0(M)_{/k}$. A section ω of $H^0(X_0(N)_{/k}, \Omega(\text{cusps}))$ is determined by giving a pair of differentials of the third kind $(\omega_\infty, \omega_0)$, one on each of C_∞ and C_0, regular away from the points x_i and the

cusps, and such that the residues of each differential at each of the points x_i are negative to one another.

The reduction modulo p of the map (A.3) is given by

$$(\omega_\infty, \omega_0) \mapsto \sum_i \mathrm{res}_{x_i}(\omega_\infty) x_i \in \mathcal{X} \otimes_{\mathbb{Z}} k.$$

Since the set of cusps of both C_∞ and C_0 are non-empty, the residue theorem shows that this map is surjective, as required. □

Note that when $M = 1$, there are no p-old forms in $\mathcal{N}(N) = \mathcal{N}(p)$, and so Proposition A.2 yields an isomorphism $\mathcal{N}(p) \otimes_{\mathbb{Z}} W \xrightarrow{\sim} \mathcal{X} \otimes_{\mathbb{Z}} W$. The argument used to prove this result makes it clear that it provides a kind of p-adic lift of the mod p situation considered by Ohta in [18, §2]. This result also provides a new proof of Theorem 3.1, and (following [18]) can be used to give an alternative proof that $\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is spanned by the theta series $\Theta(L_{i,j})$. (A result stronger than Eichler's theorem, but weaker than our Theorem 0.3.)

Continuing to consider the case $M = 1$, note that if we consider the particular element $E \in \mathcal{N}(p) \otimes_{\mathbb{Z}} W$, then Lemma 3.13 shows that the image of E under the isomorphism of Proposition A.2 must be equal to $w\mathbf{x}$, for some element $w \in W$. Let C denote the open subset of the irreducible component C_∞ of $X_0(p)_{/k}$ obtained by removing the cusp ∞ together with the supersingular points, and let X denote the open affinoid contained in $X_0(p)_{/K}$ which is the preimage of C under specialization. Thus X is isomorphic to the complement of the supersingular residue class disks in the affine j-line over K. If we restrict E to X we may regard it as a differential on X. The residue theorem shows that the sum of its residues around the punctures of X is equal to zero, and so we find that $a_0(E) + w \deg(\mathbf{x}) = 0$. Proposition 3.15 implies that $w = -1/2\Delta$, and hence that the residue of E around the tube of x_i is equal to $-1/2e_i$. This result (or to be precise, its analogue when $X_0(p)$ is replaced by the curve that classifies p-isogenies of elliptic curves equipped with full level-two structure) was first obtained by Stevens [25, prop. 1]. Both Steven's argument and ours rely on the residue theorem together with a knowledge of the constant term of the Eisenstein series. As observed in the remarks following the proof of Proposition 3.15, it would be interesting to have a purely algebro-geometric determination of the constant w that appears above.

Proposition A.2 is closely related to Coleman's p-adic Shimura isomorphism. Indeed, if we tensor the isomorphism of Proposition A.2 with the fraction field K of W and restrict to cusp forms on the left-hand side, and hence to $\mathcal{X}^0$ on the right-hand side, we obtain an isomorphism $\mathcal{N}(N)^0_{\mathrm{new}} \otimes_{\mathbb{Z}} K \xrightarrow{\sim} \mathcal{X}^0 \otimes_{\mathbb{Z}} K$, which is precisely the isomorphism obtained by taking $k = 2$ in [2, thm. 9.1] (up to the harmless replacement of Coleman's $\Gamma_1(M) \cap \Gamma_0(p)$ level-structure by our $\Gamma_0(Mp)$-level structure). In some sense this is a p-adic analogue of the Riemann relations: it shows that the p-new differentials on $X_0(N)_{/K}$ are uniquely determined by their periods along the supersingular annuli.

We note that Proposition A.2 yields a variant of the main theorem of [17].

Corollary A.4. *If $\mathfrak{m}$ is a maximal ideal of residue characteristic p in $\mathbb{T}$ for which $(\mathbb{T}_{\mathrm{old}})_{\mathfrak{m}} = 0$, and either $p \geq 5$ or the Galois representation $\rho_{\mathfrak{m}}$ is irreducible, then there is a natural isomorphism of $\mathbb{T}_{\mathfrak{m}}$-modules $\mathcal{N}(N)_{\mathfrak{m}} \xrightarrow{\sim} \mathcal{X}_{\mathfrak{m}}$. Consequently both are free $\mathbb{T}_{\mathfrak{m}}$-modules of rank one, and so $\mathbb{T}_{\mathfrak{m}}$ is Gorenstein.*

Proof. Since $(\mathbb{T}_{\mathrm{old}})_{\mathfrak{m}} = 0$ by assumption, each of the morphisms $\mathbb{T}_{\mathfrak{m}} \longrightarrow (\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}}$, $(\mathcal{N}(N)_{\mathrm{new}})_{\mathfrak{m}} \longrightarrow \mathcal{N}(N)_{\mathfrak{m}}$, and

$$H^0(X_0(N)_{/W}, \Omega(\mathrm{cusps}))_{\mathfrak{m}} \longrightarrow \\ H^0(X_0(N), \Omega(\mathrm{cusps}))_{\mathfrak{m}}/(H^0(X_0(N)_{/W}, \Omega(\mathrm{cusps}))_{\mathfrak{m}} \cap (\mathcal{N}(N)_{\mathrm{old}})_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} W)$$

are isomorphisms. Thus Propositions A.1 and A.2, combined with the flat base-change isomorphism $H^0(X_0(N)_{/\mathbb{Z}_p}, \Omega(\mathrm{cusps})) \otimes_{\mathbb{Z}_p} W \xrightarrow{\sim} H^0(X_0(N)_{/W}, \Omega(\mathrm{cusps}))$, yield an isomorphism of $\mathbb{T}_{\mathfrak{m}}$-modules

$$(\mathcal{N}(N)_{\mathrm{new}})_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} W \xrightarrow{\sim} \mathcal{X}_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} W. \tag{A.5}$$

Now the isomorphism of Proposition 7.1 induces an isomorphism

$$(\mathcal{N}(N)_{\mathrm{new}})_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} W \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p}((\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}}, W) \\ \xrightarrow{\sim} \mathrm{Hom}_W((\mathbb{T}_{\mathrm{new}})_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} W, W). \tag{A.6}$$

Furthermore, the morphism (7.2) induces an isomorphism

$$X_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p}(X_{\mathfrak{m}}, \mathbb{Z}_p). \tag{A.7}$$

Indeed, if $p \geq 5$, then this follows from the fact that the cokernel of the map (7.2) has exponent dividing twelve, while if $\rho_{\mathfrak{m}}$ is irreducible, we observed in the proof of Theorem 7.6 that it is implied by [20, thm. 3.12/prop. 3.14/thm. 3.22].

Tensoring the isomorphism (A.7) by W over $\mathbb{Z}_p$, and combining it with the isomorphisms (A.5) and (A.6), we find that $\mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}_p} W$ is a Gorenstein ring, and hence that the same is true of $\mathbb{T}_{\mathfrak{m}}$. □

We make one final remark in this appendix, again restricting ourselves to the case when $M = 1$. If we combine Proposition A.2 with Theorem 0.5 (noting, as has just been proved, that $\mathbb{T} \otimes_{\mathbb{Z}} W$ is Gorenstein) we obtain an isomorphism of free $\mathbb{T} \otimes_{\mathbb{Z}} W$-modules of rank one

$$(\mathcal{N}(p) \otimes_{\mathbb{Z}} W) \otimes_{\mathbb{T} \otimes_{\mathbb{Z}} W} (\mathcal{N}(p) \otimes_{\mathbb{Z}} W) \xrightarrow{\sim} \mathcal{N}(p) \otimes_{\mathbb{Z}} W, \tag{A.8}$$

or equivalently, an isomorphism $\mathbb{T} \otimes_{\mathbb{Z}} W \xrightarrow{\sim} \mathcal{N}(p) \otimes_{\mathbb{Z}} W$. Thus we see that $\mathcal{N}(p) \otimes_{\mathbb{Z}} W$ is a free $\mathbb{T} \otimes_{\mathbb{Z}} W$-module of rank one, equipped with a canonical generator, which we denote by P.

The isomorphism (A.8) determines (and is determined by) a non-degenerate $\mathbb{T}$-bilinear W-valued pairing on $\mathcal{N}(p) \otimes_{\mathbb{Z}} W$. Explicitly,

$$\langle \omega, \nu \rangle = \sum_i e_i \, \mathrm{res}_{x_i}(\omega_{|\,\mathrm{Spf}\, A_i}) \, \mathrm{res}_{x_i}(\nu_{|\,\mathrm{Spf}\, A_i}).$$

It is interesting to compare this pairing with that of [3], which is defined precisely on those forms on $\Gamma_1(p)$ whose traces to $\Gamma_0(p)$ vanish.

The generator P is characterized in terms of this pairing by the condition $\langle \omega, P \rangle = a_1(\omega)$ for any element ω of $\mathcal{N}(p) \otimes_{\mathbb{Z}} W$. Thus P could be thought of as a p-adic analogue of a Poincaré series.

Acknowledgments

The author would like to thank Benedict Gross for explaining the problem discussed in this paper to him in the Spring of 1996, and Shuzo Takahashi for reminding him of the problem in the Fall of 1999. He would also like to thank Robert Coleman for interesting conversations on related topics during the Summer of 1999, Fred Diamond for a suggestion which simplified the proof of Proposition 1.8 (i), Lloyd Kilford for communicating the examples of non-Gorenstein local Hecke rings, Sándor Kovács for providing the example involving normalization that follows Definition 6.1, Ken Ribet for encouraging him to treat fully the situation at two and three and to state a result for cusp forms, and Mike Roth for numerous enlightening conversations and computations. Finally, thanks go to Kevin Buzzard, Benedict Gross, Barry Mazur, Ken Ribet, Mike Roth, Shuzo Takahashi and the anonymous referee for their helpful comments on various preliminary versions of this paper, which helped to improve both the mathematics and the exposition.

References

1. Atkin, A.O.L., Lehner, J., *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160. MR **42:**3022
2. Coleman, R.F., *A p-adic Shimura isomorphism and p-adic periods of modular forms*, Contemp. Math. **165** (1994), 21–51. MR **96a:**11050
3. Coleman, R.F., *A p-adic inner product on elliptic modular forms*, Barsotti symposium in algebraic geometry, Academic Press, 1994, pp. 125–151. MR **95k:**11078
4. Eichler, M., *Über die Idealklassenzahl total definiter Quaternionenalgebren*, Math. Z. **43** (1938), 102–109.
5. Eichler, M., *Über die Darstellbarkeit von Modulformen durch Thetareihen*, J. Reine Angew. Math. **195** (1955), 156–171. MR **18:**297d
6. Gross, B.H., *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc. , 1987, pp. 115–187. MR **89c:**11082
7. Gross, B.H., *On a tameness criterion for Galois representations associated to modular forms* (mod p), Duke Math. J. **61** (1990), 445–517. MR **91i:**11060
8. Gross, B.H., Course at Harvard University, Spring, 1996.
9. Grothendieck, A., SGA VII, Exposé IX, SLN, vol. 288, 1972, pp. 313–523. MR **50:**7134
10. Hartshorne, R., *Residues and Duality*, SLN **20** (1966). MR **36:**5145
11. Hecke, E., *Lectures on the theory of algebraic numbers*, Springer-Verlag, 1981. MR **83m:**12001
12. Hijikata, H., Saito, H., *On the representability of modular forms by theta series*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, pp. 13–21. MR **50:**9800
13. Igusa, J.-I., *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. USA **44** (1958), 312–314. MR **20:**5183
14. Kilford, L., *Some examples of non-Gorenstein Hecke algebras associated to modular forms*, preprint, available at `http://www.ma.ic.ac.uk/~ljpk/maths/maths.html`.
15. Mazur, B., *Modular curves and the Eisenstein ideal*, Publ. Math., Inst. Hautes Etud. Sci. **47** (1977), 33–186. MR **80c:**14015
16. Mazur, B., letter to K. Ribet and J. Tilouine, in "Hecke algebras and the Gorenstein property", by J. Tilouine, Modular forms and Fermat's last theorem (G. Cornell, J.H. Silverman, G. Stevens, eds.), Springer-Verlag, 1997. MR **99k:**11004
17. Mazur, B., Ribet, K.A., *Two-dimensional representations in the arithmetic of modular curves*, Astérisque **196–197** (1991), 215–255. MR **93d:**11056
18. Ohta, M., *Theta series mod p*, J. Fac. Sci. Tokyo **28** (1981), 679–686. MR **83h:**10058
19. Ribet, K.A., *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), 193–205. MR **84j:**10040
20. Ribet, K.A., *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476. MR **91g:**11066

21. Ribet, K.A., *Multiplicities of Galois representations in Jacobians of Shimura curves*, Israel Math. Conf. Proc. **3** (1990), 221–236. MR **93c:**11043
22. Ribet, K.A., *Multiplicities of p-finite mod p Galois representations in $J_0(Np)$*, Bol. Soc. Brasil. Mat. (N. S.) **21** (1991), 177–188. MR **93b:**11078
23. Ribet, K.A., *Torsion points on $J_0(N)$ and Galois representations*, Arithmetic Theory of Elliptic Curves (J. Coates, ed.), SLN, vol. 1716, 1999. MR **2001b:**11054
24. Serre, J.-P., *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230. MR **88g:**11022
25. Stevens, G., *Coleman's $\mathcal{L}$-invariant and families of modular forms*, preprint (1996).

Department of Mathematics, Northwestern University, 2033 Sheridan Rd., Evanston, Illinois 60208-2730

E-mail address: emerton@math.northwestern.edu