Endomorphisms of Jacobians of Modular Curves

E. Kani

Department of Mathematics and Statistics,
Queen's University, Kingston, Ontario, Canada, K7L 3N6
Email: Kani@mast.queensu.ca

1 Introduction

Let $X_\Gamma = \Gamma\backslash\mathfrak{H}^*$ be the modular curve associated to a congruence subgroup Γ of level N with $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$. Then X_Γ has a canonical model $X = X_{\Gamma,\mathbb{Q}}$ defined over $\mathbb{Q}$, and its Jacobian variety J_X is also defined over $\mathbb{Q}$. Let $\mathbf{E} = \mathrm{End}^0_{\mathbb{Q}}(J_X)$ denote the $\mathbb{Q}$-algebra of $\mathbb{Q}$-endomorphisms of J_X. It is well-known that $\mathbf{E}$ contains the Hecke algebra $\mathbb{T}'_{\mathbb{Q}}$ generated (as a $\mathbb{Q}$-algebra) by the Hecke operators T_p with $p \nmid N$.

If N is prime, then $\mathbf{E} = \mathbb{T}'_{\mathbb{Q}}$ (cf. Ribet[6]), but for composite N's this is no longer true in general. One reason for this is that for each pair (M, d) with $dM|N$ there is a "degeneracy morphism" (cf. Mazur[4]) $B_{M,d} : X \to X_M$, where X_M is the corresponding curve of level M, and that these morphisms give rise to extra endomorphisms (called "degeneracy operators") $D_{M,d} = B^*_{M,1} \circ (B_{M,d})_*$ and ${}^tD_{M,d} = B^*_{M,d} \circ (B_{M,1})_*$ of J_X.

The purpose of this paper is to prove the following basic result which does not seem to have been recorded in the literature (but is well-known to the experts):

Theorem 1. $\mathrm{End}^0_{\mathbb{Q}}(J_X)$ *is generated as a* $\mathbb{Q}$*-algebra by the Hecke algebra* $\mathbb{T}'_{\mathbb{Q}}$ *and the degeneracy operators* $D_{M,d}$, ${}^tD_{M,d}$, *for* $dM|N$.

In particular, we see that the $\mathbb{Q}$-algebra $\mathbb{E} := \langle \mathbb{T}'_{\mathbb{Q}}, D_{M,d}, {}^tD_{M,d} : dM|N\rangle_{\mathbb{Q}}$ contains the full Hecke algebra $\mathbb{T}_{\mathbb{Q}} = \langle T_n : n \geq 1\rangle_{\mathbb{Q}}$ as a subalgebra; we will thus refer to $\mathbb{E}$ as the *extended Hecke algebra*. Note that for special curves (such as $X_0(p^2)$ and $X(p)$) we can use the methods below to obtain other generators of $\mathbb{E}$; cf. Example 19 below.

It is immediate that the algebra $\mathbb{E}$ is contained in the $\mathbb{Q}$-algebra $\mathbb{M}$ of all *modular endomorphisms*, i.e. $\mathbb{M}$ is the $\mathbb{Q}$-linear span of those endomorphisms of J_X which are defined by a double coset $\Gamma g \Gamma$ with $g \in \mathrm{GL}_2^+(\mathbb{Q})$, as in [8]. We thus obtain:

Corollary 2. *Every endomorphism* $f \in \mathrm{End}^0_{\mathbb{Q}}(J_X)$ *is* modular*, i.e.* f *is a* $\mathbb{Q}$*-linear combination of endomorphisms defined by double cosets.*

Note that the analogue of this statement is no longer true for endomorphisms which are not $\mathbb{Q}$-rational: the presence of (non-rational) CM-elliptic curves in J_X gives rise to endomorphisms which are not modular, as is easy to see.

Another interesting consequence of Theorem 1 is the following result which generalizes a statement proved in Mazur[4], p. 139.

Corollary 3. *The centre of* $\mathrm{End}^0_{\mathbb{Q}}(J_X)$ *is* $\mathbb{T}'_{\mathbb{Q}}$, *i.e.* $Z(\mathbf{E}) = \mathbb{T}'_{\mathbb{Q}}$.

In fact, the proof of Theorem 1 shows that a certain refinement of this corollary is also true. Let $\Omega^1(J_X) := H^0(J_X, \Omega^1_{J_X})$ denote the space of holomorphic 1-forms on J_X, which is naturally isomorphic to the space $S_2(\Gamma, \mathbb{Q})$ of weight 2 cusp forms with rational Fourier expansions. Then the above proof shows that centralizer of $\mathbf{E} = \mathbb{E}$ in $\mathrm{End}_{\mathbb{Q}}(\Omega^1(J_X))$ is $\mathbb{T}'_{\mathbb{Q}}$, i.e. $\mathrm{End}_{\mathbf{E}}(\Omega^1(J_X)) = \mathbb{T}'_{\mathbb{Q}}$. Thus, by the "dictionary" of [3], we obtain the following generalization of the Shimura construction:

Corollary 4. *We have* $\mathrm{End}_{\mathbf{E}}(\Omega^1(J_X)) = \mathbb{T}'_{\mathbb{Q}}$. *Thus, the map* $(A, p) \mapsto p^*\Omega^1(A) \subset \Omega^1(J_X) \simeq S_2(\Gamma, \mathbb{Q})$ *induces a bijection between the set of (equivalence classes) of abelian quotients* $p : J_X \to A$ *of* $J_X/\mathbb{Q}$ *and the set of* $\mathbb{T}'_{\mathbb{Q}}$*-submodules of* $S_2(\Gamma, \mathbb{Q})$.

The first step in the proof of Theorem 1 is the following classification of the irreducible $\mathbb{E}_{\mathbb{C}}$-modules, where $\mathbb{E}_{\mathbb{C}} = \mathbb{E} \otimes \mathbb{C}$. To state the result, recall that $\mathbb{E}_{\mathbb{C}}$ acts faithfully on the space $S = S_2(\Gamma)$ of weight 2 cusp forms on Γ, and that S has (by Atkin-Lehner theory) a $\mathbb{T}'_{\mathbb{C}}$-module decomposition $S = \bigoplus_{f \in \mathcal{N}(\Gamma)} S_f$, where $\mathcal{N}(\Gamma)$ denotes the set of all normalized newforms of weight 2 (of all levels) on Γ and S_f denotes the χ_f-eigenspace with respect to the character $\chi_f : \mathbb{T}'_{\mathbb{C}} = \mathbb{T}'_{\mathbb{Q}} \otimes \mathbb{C} \to \mathbb{C}$ defined by $f \in \mathcal{N}(\Gamma)$. We then have:

Theorem 5. *Each* S_f *is an irreducible* $\mathbb{E}_{\mathbb{C}}$*-module, and every irreducible* $\mathbb{E}_{\mathbb{C}}$*-module is isomorphic to some* S_f. *Thus* $\mathbb{E}_{\mathbb{C}}$ *is (isomorphic to) the centralizer* $C_S(\mathbb{T}'_{\mathbb{Q}})$ *of* $\mathbb{T}'_{\mathbb{Q}}$ *in* $\mathrm{End}_{\mathbb{C}}(S)$, *and* $Z(\mathbb{E}_{\mathbb{C}}) = \mathbb{T}'_{\mathbb{Q}} \otimes \mathbb{C}$.

Since this theorem is of independent interest and has a natural analogue for cusp forms of arbitrary weight, we shall prove a more general version below; cf. Theorem 11.

In view of Theorem 5, Theorem 1 follows readily once the structure of $\mathbf{E}$ is known. For this, let $n_f = \dim S_f$ and let $K_f = \mathbb{Q}(\{a_n\})$ be the field generated by the Fourier coefficients of $f = \sum a_n q^n$. Then we have the following theorem which is a consequence of the fundamental results of Ribet[7].

Theorem 6 (Ribet). $\mathrm{End}^0_{\mathbb{Q}}(J_X) \simeq \prod_{f \in \mathcal{N}(\Gamma)/G_{\mathbb{Q}}} M_{n_f}(K_f)$.

Actually, Ribet's results give *a priori* only a slightly weaker result; cf. equation (14) below. As a result, the order of the proofs of the above theorems has to be partially reversed. Indeed, after proving Theorem 5 and (14), we first deduce Corollary 3 and then Theorem 1. Finally, we use these results to prove the full version of Theorem 6.

2 The Degeneracy Operators

Throughout, we shall fix a congruence subgroup Γ with $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$, so

$$\Gamma = \Gamma_H(N) := \{g \in \mathrm{SL}_2(\mathbb{Z}) : g \equiv \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \pmod{N}, a \in H\},$$

for some subgroup $H \leq (\mathbb{Z}/N\mathbb{Z})^\times \simeq \Gamma_0(N)/\Gamma_1(N)$. Then for any divisor $M|N$ we have a corresponding subgroup $\Gamma_H(M) := \Gamma_{\overline{H}}(M)$, where $\overline{H} \leq (\mathbb{Z}/M\mathbb{Z})^\times$ is the image of H under the reduction map $r_{N,M} : (\mathbb{Z}/NZ)^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$.

For any positive integer d, let $\alpha_d = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ and $\beta_d = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) = d\alpha_d^{-1}$. Since $\beta_d \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \beta_d^{-1} = \left(\begin{smallmatrix} x & yd \\ z/d & w \end{smallmatrix}\right)$, we see that if $d|N$, then

(1) $$\beta_d\Gamma_H(N)\beta_d^{-1} = \Gamma_H(\tfrac{N}{d}, d) := \{\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : r_N(x) \in H, d|y, \tfrac{N}{d}|z\},$$

where $r_N : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ denotes the reduction (mod N) map.

In order to study the degeneracy operators mentioned in the introduction, we shall first define them as "abstract operators" via double cosets, and then (as in Shimura[8]) consider their actions on the spaces of cusp forms $S_k(\Gamma)$. Thus, fix divisors d, M of N with $dM|N$ and consider the double cosets

$$\beta_{M,d} = \Gamma_H(M)\beta_d\Gamma_H(N) \quad \text{and} \quad {}^t\beta_{M,d} = \Gamma_H(N)\alpha_d\Gamma_H(M).$$

Since $\alpha_d^{-1}\Gamma_H(N)\alpha_d = \Gamma_H(\frac{N}{d}, d) \leq \Gamma_H(M)$, we see that the degree of these double cosets (as defined in [8], p. 51) is given by

(2) $$\deg(\beta_{M,d}) = 1 \quad \text{and} \quad \deg({}^t\beta_{M,d}) = [\Gamma_H(M) : \Gamma_H(\tfrac{N}{d}, d)].$$

The (abstract) *degeneracy operators* are defined as the products

$$D_{M,d} = {}^t\beta_{M,1} \cdot \beta_{M,d} \quad \text{and} \quad {}^tD_{M,d} = {}^t\beta_{M,d} \cdot \beta_{M,1}.$$

From the definition of the product of double cosets (cf. [8], p. 52) together with the fact that $\beta_d\Gamma_H(N)\beta_d^{-1} = \Gamma_H(\frac{N}{d}, d) \leq \Gamma_H(M)$ one sees easily that

(3) $$D_{M,d} = \sum_{\gamma\in R_d} \Gamma_H(N)\gamma\beta_d\Gamma_H(N) \quad \text{and} \quad {}^tD_{M,d} = \sum_{\gamma\in R_d} \Gamma_H(N)\alpha_d\gamma^{-1}\Gamma_H(N),$$

where R_d is a system of representatives of the set of double cosets (double coset space) $\Gamma_H(N)\backslash\Gamma_H(M)/\Gamma_H(\frac{N}{d}, d)$. Note that the above formula (together with [8], p. 70) shows that the Hecke operator $T_d = \Gamma_H(N)\alpha_d\Gamma_H(N)$ is a component of ${}^tD_{M,d}$.

Remark 7. As the notation indicates, ${}^tD_{M,d}$ is the *Rosati adjoint* of $D_{M,d}$; cf. [8], p. 72 and p. 171. Similarly ${}^t\beta_{M,d}$ is the adjoint of $\beta_{M,d}$.

We next want to show that the degeneracy operators commute with the Hecke operators $T_n = T_n^N$ for $(n, N) = 1$. (Note that the T_n's generate the algebra $R(\Gamma_H(N), \Delta'_N) \otimes \mathbb{Q}$ in the notation of [8], p. 67.) To this end we show more generally

Proposition 8. *If $dM|N$, then for any integer $n \geq 1$ with $(n, N) = 1$ we have*

(4) $$T_n^M \cdot \beta_{M,d} = \beta_{M,d} \cdot T_n^N \quad \textit{and} \quad T_n^N \cdot {}^t\beta_{M,d} = {}^t\beta_{M,d} \cdot T_n^M.$$

The proof of this proposition is based on the following simple fact.

Lemma 9. *Let* Γ_1, Γ_2 *be commensurable subgroups of* $G = \mathrm{GL}_2^+(\mathbb{Q})$*, and suppose that* $\alpha \in G$ *satisfies* $\alpha\Gamma_2\alpha^{-1} \le \Gamma_1$*. Then for any* $\beta \in G$ *we have*

$$(5) \qquad (\Gamma_1\alpha\Gamma_2)(\Gamma_2\beta\Gamma_2) = c_\beta\Gamma_1\alpha\beta\Gamma_2, \quad \text{with } c_\beta = \deg(\Gamma_2\beta\Gamma_2)/\deg(\Gamma_1\alpha\beta\Gamma_2).$$

If, in addition, there exists a subset $S \subset \Gamma_2\beta\Gamma_2$ *such that* $\Gamma_1\beta\Gamma_1 = \Gamma_1\alpha S\alpha^{-1}$*, then*

$$(6) \qquad (\Gamma_1\beta\Gamma_1)(\Gamma_1\alpha\Gamma_2) = c'_\beta\Gamma_1\alpha\beta\Gamma_2, \quad \text{with } c'_\beta = \deg(\Gamma_1\beta\Gamma_1)/\deg(\Gamma_1\alpha\beta\Gamma_2),$$

and so $(\Gamma_1\alpha\Gamma_2)(\Gamma_2\beta\Gamma_2) = c''_\beta(\Gamma_1\beta\Gamma_1)(\Gamma_1\alpha\Gamma_2)$*, where* $c''_\beta = \deg(\Gamma_2\beta\Gamma_2)/\deg(\Gamma_1\beta\Gamma_1)$.

Proof. The hypothesis on α implies that $\Gamma_1\alpha\Gamma_2\beta\Gamma_2 = \Gamma_1(\alpha\Gamma_2\alpha^{-1})\alpha\beta\Gamma_2 = \Gamma_1\alpha\beta\Gamma_2$, and so (5) holds for some integer c_β. By taking degrees of both sides and observing that $\deg(\Gamma_1\alpha\Gamma_2) = 1$ by hypothesis, the given formula for c_β follows.

The hypotheses on S show that $\Gamma_1\beta\Gamma_1\alpha\Gamma_2 = (\Gamma_1\alpha S\alpha^{-1})\alpha\Gamma_2 \subset \Gamma_1\alpha\Gamma_2\beta\Gamma_2 = \Gamma_1\alpha\beta\Gamma_2$, where the last equality follows from (5). Thus, $\Gamma_1\beta\Gamma_1\alpha\Gamma_2 \subset \Gamma_1\alpha\beta\Gamma_2$, and so we must have equality since $\Gamma_1\beta\Gamma_1\alpha\Gamma_2$ is a union of (Γ_1, Γ_2)-double cosets (and since double cosets are either disjoint or equal). Thus, $\Gamma_1\beta\Gamma_1\alpha\Gamma_2 = \Gamma_1\alpha\beta\Gamma_2$, and so we see that (6) holds for some c'_β. By the same argument as for (5) we see that c'_β has the asserted value.

The last assertion follows immediately from (5) and (6) since $c''_\beta = c_\beta/c'_\beta$.

Proof of Proposition 8. Apply Lemma 9 to $\Gamma_1 = \Gamma_H(M)$, $\Gamma_2 = \Gamma_H(N)$, $\alpha = \beta_d$ and $\beta = \alpha_p$, where $p \nmid N$ is a prime. Thus, $\Gamma_1\alpha\Gamma_2 = \beta_{M,d}$, $\Gamma_1\beta\Gamma_1 = T_p^M$ and $\Gamma_2\beta\Gamma_2 = T_p^N$; cf. [8], p. 71.

Since $\alpha\Gamma_2\alpha^{-1} = \Gamma_H(\frac{N}{d}, d) \le \Gamma_1$, we see that the first hypothesis of the lemma holds. Moreover, take $S = \left\{\left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right)\right\}_{0 \le b < p} \cup \{\sigma_p\beta_p\}$, where $\sigma_p \equiv \begin{pmatrix} p^{-1} & 0 \\ 0 & p \end{pmatrix} \pmod{N}$. Since $\beta_d \left(\begin{smallmatrix} 1 & b \\ 0 & p \end{smallmatrix}\right) \beta_d^{-1} = \left(\begin{smallmatrix} 1 & bd \\ 0 & p \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b' \\ 0 & p \end{smallmatrix}\right)$, where $b' + kp = bd$, $0 \le b' < p$, and since $\beta_d\sigma_p\beta_d^{-1} \equiv \begin{pmatrix} p^{-1} & 0 \\ 0 & p \end{pmatrix} \pmod{\frac{N}{d}}$ (and since $M | \frac{N}{d}$), we see that $\Gamma_1\beta_d S\beta_d^{-1} = \Gamma_1 S = \Gamma_1\beta\Gamma_1 = T_p^M$, where the second last equality follows from [8], p. 72. Similarly, we have $S \subset \Gamma_2\beta\Gamma_2 = T_p^N$. Thus, S satisfies the hypotheses of the lemma, and so we conclude from the lemma (together with the fact that $c''_\beta = 1$ because $\deg(T_p^M) = \deg(T_p^M) = p + 1$) that the first equation of (4) holds for all primes $p \nmid N$.

Since we have $T(n,n)\beta_{M,d} = \beta_{M,d}T(n,n)$ (use [8], Prop. 3.7 on p. 54), the recursion relations of the T_n's (cf. [8], p. 71) show that the first formula of (4) holds for all n with $(n, N) = 1$.

From this it follows that we also have the formula

$$(7) \qquad {}^tT_n^M \cdot \beta_{M,d} = \beta_{M,d} \cdot {}^tT_n^N, \quad \text{for all } (n, N) = 1.$$

Indeed, since ${}^tT_n = \sigma_n T_n = T_n\sigma_n$ (cf. [8], p. 72), and since $\sigma_n\beta_{M,d} = \beta_{M,d}\sigma_n$, we see that (7) follows from the first equation of (4).

Finally, taking the Rosati adjoints of (7) yields the second equation of (4), which concludes the proof of Proposition 8.

Notation. Let $\tilde{\mathbb{T}}' = R(\Gamma_H(N), \Delta'_N)$ denote the Hecke ring generated by the (abstract) Hecke operators T_n with $(n, N) = 1$, and let $\tilde{\mathbb{E}} = \langle T_n, D_{M,d}, {}^tD_{M,d} : (n, N) = 1, dM|N\rangle \subset \tilde{\mathbb{M}} := R(\Gamma_H(N), \Delta)$ denote the Hecke ring generated by the T_n's and the degeneracy operators $D_{M,d}$ and ${}^tD_{M,d}$.

Corollary 10. *$\tilde{\mathbb{T}}'$ is a subring of the centre of $\tilde{\mathbb{E}}$, i.e. $\tilde{\mathbb{T}}' \subset Z(\tilde{\mathbb{E}})$.*

Proof. By (4) we have $T_nD_{M,d} = {}^t\beta_{M,1}T_n^M\beta_{M,d} = D_{M,d}T_n$, for any d, M with $dM|N$ and any n with $(n, N) = 1$, and similarly T_n and ${}^tD_{m,d}$ commute. Thus, since $\tilde{\mathbb{T}}' = \langle T_n\rangle$ is commutative, we see that $\tilde{\mathbb{T}}' \subset Z(\tilde{\mathbb{E}})$.

3 The Structure of the Extended Hecke Algebra $\mathbb{E}_{k,\mathbb{C}}$

We now fix an integer k and consider the space $S = S_k(\Gamma_H(N))$ of cusp forms of weight k on $\Gamma_H(N)$. By [8], p. 73, each double coset in $\tilde{\mathbb{M}} = R(\Gamma_H(N), \Delta)$ induces a natural $\mathbb{C}$-linear operator on S, and S is a *right* $\tilde{\mathbb{M}} \otimes \mathbb{C}$-module. In particular, since $\tilde{\mathbb{E}} \subset \tilde{\mathbb{M}}$, S is also a $\tilde{\mathbb{E}}\otimes\mathbb{C}$-module; we let $\mathbb{E}_{k,\mathbb{C}}$ denote the image of $\tilde{\mathbb{E}}\otimes\mathbb{C}$ in $\mathrm{End}_{\mathbb{C}}(S)^{op}$.

Thus, by definition, $\mathbb{E}_{k,\mathbb{C}}$ is the subalgebra of $\mathrm{End}_{\mathbb{C}}(S)^{op}$ generated by the Hecke operators $[T_p]_k$, for $p \nmid N$ and the degeneracy operators $[D_{M,d}]_k$, $[{}^tD_{M,d}]_k$, for $dM|N$. Note that the action of $[D_{M,d}]_k$ on S is given by the formula

$$f|[D_{M,d}]_k(z) = d^{k-1}\,\mathrm{tr}_M(f)(dz), \quad \text{for } f \in S, \tag{8}$$

where $\mathrm{tr}_M = \mathrm{tr}_{\Gamma_H(N)/\Gamma_H(M)} : S_k(\Gamma_H(N)) \to S_k(\Gamma_H(M))$ is the usual trace map. Indeed, since $\mathrm{tr}_M = [{}^t\beta_{M,1}]_k$ by definition, this follows immediately from the fact that $f|[D_{M,d}]_k = f|[{}^t\beta_{M,1}]_k[\beta_{M,d}]_k$ together with the formula

$$f|[\beta_{M,d}]_k(z) = d^{k/2-1}f|_k\beta_d(z) = d^{k-1}f(dz), \quad \text{for } f \in S_k(\Gamma_H(M)). \tag{9}$$

A similar formula holds for the operator $[{}^tD_{M,d}]_k$, which by [8], p. 76, is just the adjoint of $[D_{M,d}]_k$ with respect to the Petersson product on S.

Let $\mathbb{T}'_{k,\mathbb{C}}$ be the $\mathbb{C}$-subalgebra of $\mathbb{E}_{k,\mathbb{C}}$ generated by the Hecke operators $[T_p]_k$, for $p \nmid N$. Since $\mathbb{T}'_{k,\mathbb{C}}$ is a commutative semi-simple algebra, S has a decomposition into $\mathbb{T}'_{k,\mathbb{C}}$-eigenspaces S_χ. By Atkin-Lehner theory, each such character is of the form $\chi = \chi_f$, for a unique normalized newform f of some level $N_f|N$, and so we have the Atkin-Lehner decomposition

$$S = \bigoplus_{f\in\mathcal{N}(\Gamma)} S_f, \tag{10}$$

where $S_f = S_{\chi_f}$ and $\mathcal{N}(\Gamma) = \mathcal{N}_k(\Gamma)$ denotes the set of all normalized newforms of weight k of level $N_f|N$ on $\Gamma = \Gamma_H(N)$; cf. [2], p. 28 and/or [5], §4.6). In particular, we see that $\dim \mathbb{T}'_{k,\mathbb{C}} = \#\mathcal{N}(\Gamma)$.

We now prove:

Theorem 11. *Each S_f is an irreducible $\mathbb{E}_{k,\mathbb{C}}$-module, and every irreducible $\mathbb{E}_{k,\mathbb{C}}$-module is isomorphic to some S_f. Thus $\mathbb{E}_{k,\mathbb{C}}$ is isomorphic to the centralizer $C_S(\mathbb{T}'_{k,\mathbb{C}})$ of $\mathbb{T}'_{k,\mathbb{C}}$ in $\mathrm{End}_{\mathbb{C}}(S)$, and its centre is $Z(\mathbb{E}_{k,\mathbb{C}}) = \mathbb{T}'_{k,\mathbb{C}}$.*

Proof. First note that since $\mathbb{T}'_{k,\mathbb{C}}$ is closed under the Petersson adjoints, the same is true for $\mathbb{E}_{k,\mathbb{C}}$ and hence both algebras are semi-simple (cf. [8], p. 83.) Moreover, from Corollary 10 it follows that $\mathbb{T}'_{k,\mathbb{C}} \subset Z(\mathbb{E}_{k,\mathbb{C}})$. Thus, the operators in $\mathbb{E}_{k,\mathbb{C}}$ preserve the $\mathbb{T}'_{k,\mathbb{C}}$-eigenspaces in S, and so each S_f is a $\mathbb{E}_{k,\mathbb{C}}$-module.

Suppose S_f were reducible. Then $S_f = V_1 \oplus V_2$, where each V_i is a non-zero $\mathbb{E}_{k,\mathbb{C}}$-module because $\mathbb{E}_{k,\mathbb{C}}$ is semi-simple. Consider the map $\mathrm{tr} = \mathrm{tr}_{N_f} : S_f \to S_k(\Gamma_H(N_f)) \cap S_f = \mathbb{C}f$, where the last equality follows from the multiplicity 1 theorem of Atkin-Lehner theory. Now tr is non-zero because $\mathrm{tr}(f) = nf$, for some $n > 0$. Thus, $\mathrm{tr}(V_1) \neq 0$ or $\mathrm{tr}(V_2) \neq 0$, and so there exists (wlog) $g \in V_1$ such that $\mathrm{tr}(g) = cf$, for some $c \neq 0$. Then, by (8) we see that for each $d|N/N_f$, $cd^{k/2-1} f|_k\beta_d = g|[D_{N_f,d}]_k \in V_1$, and so $S_f \subset V_1$ since $\{f|\beta_d\}_{d|N/N_f}$ is a basis of S_f (cf. [5], Cor. 4.6.20). Thus $S_f = V_1$, which means that S_f is irreducible.

Since S is a faithful $\mathbb{E}_{k,\mathbb{C}}$-module (by construction), we see by Wedderburn that every irreducible $\mathbb{E}_{k,\mathbb{C}}$-module is a submodule of S (and thus is isomorphic to some S_f) and that hence $\mathbb{E}_{k,\mathbb{C}} \simeq \prod_{f\in\mathcal{N}(\Gamma)} M_{n_f}(\mathbb{C})$, where $n_f = \dim S_f$ $(= \sigma_0(N/N_f))$. (Note that the S_f's are pairwise non-isomorphic as $\mathbb{E}_{k,\mathbb{C}}$-modules because they are already non-isomorphic as $\mathbb{T}'_{k,\mathbb{C}}$-modules.) Thus $\dim Z(\mathbb{E}_{k,\mathbb{C}}) = \#\mathcal{N}(\Gamma) = \dim \mathbb{T}'_{k,\mathbb{C}}$, and so $Z(\mathbb{E}_{k,\mathbb{C}}) = \mathbb{T}'_{k,\mathbb{C}}$.

Finally, since S has multiplicity one as a $\mathbb{E}_{k,\mathbb{C}}$-module, it follows easily that $\mathbb{E}_{k,\mathbb{C}} \simeq C_S(\mathbb{T}'_{k,\mathbb{C}})$. To see this, note first that

$$\mathbb{E}_{k,\mathbb{C}} \;\simeq\; \mathbb{S} := \{\varphi \in \mathrm{End}_{\mathbb{C}}(S)^{op} : S_f|\varphi \subset S_f, \forall f \in \mathcal{N}(\Gamma)\}$$

because by construction $\mathbb{E}_{k,\mathbb{C}}$ is isomorphic to a subring of $\mathbb{S}$ and because $\dim \mathbb{E}_{k,\mathbb{C}} = \sum_{f\in\mathcal{N}(\Gamma)} n_f^2 = \dim \mathbb{S}$. Since clearly $\mathbb{S} = C_S(Z(\mathbb{S}))$, it follows that $\mathbb{E}_{k,\mathbb{C}} \simeq C_S(\mathbb{T}'_{k,\mathbb{C}})$.

Corollary 12. *Suppose $\mathbb{E}' \subset \mathbb{E}_{k,\mathbb{C}}$ is a semi-simple $\mathbb{C}$-algebra which contains $\mathbb{T}'_{k,\mathbb{C}}$, the operators $[D_{M,1}]_k$ for $M|N$, and for each $d|N/M$ an operator $\tilde{D}_{M,d}$ with the property that $S_k(\Gamma_H(M))|\beta_d \subset \mathrm{Im}([D_{M,1}]_k\tilde{D}_{M,d})$. Then $\mathbb{E}' = \mathbb{E}_{k,\mathbb{C}}$.*

Proof. It is enough to show that each S_f is an irreducible $\mathbb{E}'$-module, for then by the above argument we have $\mathbb{E}' \simeq \mathbb{E}_{k,\mathbb{C}}$ and hence $\mathbb{E}' = \mathbb{E}_{k,\mathbb{C}}$.

Now if S_f were reducible, then as in the proof of Theorem 11 we would have $S_f = V_1 \oplus V_2$ where (wlog) $f \in V_1$. Let $d|N/N_f$. Then by hypothesis $\exists g \in S$

such that $g|[D_{N_f,1}]\tilde{D}_{N_f,d} = f|_k\beta_d$. By replacing g by $g|\varepsilon_f$, where $\varepsilon_f \in \mathbb{T}'_{k,\mathbb{C}}$ is the idempotent such that $S_f = S|\varepsilon_f$, we may assume that $g \in S_f$. Then $g|[D_{N_f,1}]_k = cf$, for some $c \in \mathbb{C}$ (cf. proof of Theorem 11), and so $f|_k\beta_d = (cf)\tilde{D}_{N_f,d} \in V_1$. Thus as before $V_1 = S_f$, and so S_f is irreducible.

Remark 13. (a) If $\mathbb{E}_{k,\mathbb{Q}}$ denotes the $\mathbb{Q}$-algebra generated by the operators $[T_p]_k$ ($p \nmid N$), $[D_{M,d}]_k$ and $[{}^tD_{M,d}]_k$ (for $dM|N$), then we have $\mathbb{E}_{k,\mathbb{C}} = \mathbb{E}_{k,\mathbb{Q}} \otimes \mathbb{C}$, provided that $k \geq 2$. Indeed, by (3) we see easily that $\mathbb{E} \subset \mathcal{B} \subset R(\Gamma_H(N), \Delta)$, where $\mathcal{B}$ is as defined on p. 83 of [8], and so the assertion follows from [8], Th. 3.48.

(b) By conjugation, the above results also hold for the groups $\Gamma := \Gamma_H(N', t) = \beta_t\Gamma_H(tN')\beta_t^{-1}$, where $H \leq (\mathbb{Z}/N't\mathbb{Z})^\times$; in particular, they hold for the groups Γ' considered by Shimura[8], p. 67ff. More precisely, the map $\Gamma_H(N't)\alpha\Gamma_H(N't) \mapsto \Gamma\beta_t\alpha\beta_t^{-1}\Gamma$ defines a ring isomorphism $\rho_t : R(\Gamma_H(N't), \Delta) \xrightarrow{\sim} R(\Gamma, \beta_t\Delta\beta_t^{-1})$ which identifies the Hecke algebra of $\Gamma_H(N't)$ with that of Γ. Furthermore, the map $f \mapsto f|_k\beta_t$ defines an isomorphism $S_k(\Gamma) \simeq S_k(\Gamma_H(N't))$ which is compatible with the isomorphism ρ_t. Thus, the Atkin-Lehner theory for $\Gamma_H(N't)$ can be transported back to Γ, and thus the analogous results hold for Γ (in place of $\Gamma_H(N't)$).

(c) In classical Atkin-Lehner theory (cf. Miyake[5], §4.6) one often considers submodules of $S = S_k(\Gamma)$ with respect to the algebra $\mathbb{A}_k := \langle \mathbb{T}, {}^t\mathbb{T}\rangle \subset \mathrm{End}_{\mathbb{C}}(S_k(\Gamma))$, where $\mathbb{T}$ is the full Hecke algebra (and ${}^t\mathbb{T}$ is its (Rosati) adjoint); for example, one shows that S_f is an $\mathbb{A}_k$-submodule. Now it follows from the above Theorem 11 that we have the inclusion $\mathbb{A}_k \subset \mathbb{E}_{k,\mathbb{C}}$ (which is not obvious from the definitions). Indeed, since $C_S(\mathbb{E}_{k,\mathbb{C}}) = \mathbb{T}' \subset C_S(\mathbb{A}_k)$, the double centralizer theorem shows that $\mathbb{A}_k \subset \mathbb{E}_{k,\mathbb{C}}$.

4 Application to $\mathrm{End}^0_{\mathbb{Q}}(J_X)$

As in the introduction, let $X = X_H(N)/\mathbb{Q}$ denote the canonical model (in the sense of [8], p. 152) of $X_\Gamma = \Gamma\backslash\mathfrak{H}^*$, where $\Gamma = \Gamma_H(N)$. Thus, X is the unique smooth, projective curve over $\mathbb{Q}$ such that its function field $\kappa(X)$ is isomorphic to $A_0(\Gamma_H(N), \mathbb{Q})$, the field of modular functions (of weight 0) on $\Gamma_H(N)$ whose q-expansions have coefficients in $\mathbb{Q}$ (cf. [8], Prop. 6.9(2), p.140). Note that since H and $\pm H = \langle H, -1\rangle$ define the same curve $X_H(N)$, we may assume without loss of generality that $-1 \in H$, and we shall do so in the sequel.

Now for any two divisors d, M of N with $dM|N$, the map $f(z) \mapsto f(dz) = f|_0\beta_d$ clearly defines an injection of fields $\beta_d^* : A_0(\Gamma_H(M), \mathbb{Q}) \hookrightarrow A_0(\Gamma_H(N), \mathbb{Q})$ because $\beta_d^{-1}\Gamma_H(M)\beta_d \geq \beta_d^{-1}\Gamma_H(N/d, d)\beta_d = \Gamma_H(N)$. We thus have a corresponding surjective morphism of curves $B_{M,d} : X_H(N) \to X_H(M)$ such that its induced pullback map on the function fields is β_d^*. Note that the graph $\Gamma_{B_{M,d}} \subset X_H(N) \times X_H(M)$ of this morphism is precisely the correspondence $X(\beta_{M,d})$ defined by the double coset $\beta_{M,d} = \Gamma_H(M)\beta_d\Gamma_H(N)$; cf. [8], p. 170. In particular, since the degree of the morphism

$B_{M,d}$ is the degree of the Rosati adjoint ${}^t\beta_{M,d}$, we see by [8], p. 171 and (2) that $\deg(B_{M,d}) = \deg({}^t\beta_{M,d}) = [\Gamma_H(M) : \Gamma_H(N/d,d)]$.

Let $J_X = J_H(N)/\mathbb{Q}$ be the Jacobian variety of $X_H(N)/\mathbb{Q}$. Then by functoriality and autoduality of the Jacobian we have induced homomorphisms

$$B^*_{M,d} : J_H(M) \to J_H(N) \quad \text{and} \quad (B_{M,d})_* : J_H(N) \to J_H(M).$$

As is explained in [8], p. 169-171, these maps are the same as the homomorphisms $\xi({}^t\beta_{M,d}) \in \mathrm{Hom}(J_H(M), J_H(N))$ and $\xi(\beta_{M,d}) \in \mathrm{Hom}(J_H(N), J_H(M))$ defined by the double cosets ${}^t\beta_{M,d}$ and $\beta_{M,d}$, respectively. Thus, by [8], Prop. 7.1, we have

$$\xi(D_{M,d}) = \xi({}^t\beta_{M,1}) \circ \xi(\beta_{M,d}) = B^*_{M,1} \circ (B_{M,d})_* \in \mathrm{End}_{\mathbb{Q}}(J_H(N)),$$

and similarly, $\xi({}^tD_{M,d}) = B^*_{M,d} \circ (B_{M,1})_* \in \mathrm{End}_{\mathbb{Q}}(J_H(N))$. Moreover, we also have the $\mathbb{Q}$-endomorphisms $\xi(T_n) \in \mathrm{End}_{\mathbb{Q}}(J_H(N))$ defined by the Hecke operators T_n; cf. [8], p. 175. As in the introduction, we let $\mathbb{T}'_{\mathbb{Q}} \subset \mathrm{End}^0_{\mathbb{Q}}(J_H(N)) = \mathrm{End}_{\mathbb{Q}}(J_H(N)) \otimes \mathbb{Q}$ denote the $\mathbb{Q}$-algebra generated by the $\xi(T_p)$'s, for $p \nmid N$.

Proposition 14. *Let $\mathbb{E} \subset \mathrm{End}^0_{\mathbb{Q}}(J_H(N))$ denote the $\mathbb{Q}$-algebra generated by $\mathbb{T}'_{\mathbb{Q}}$ and the degeneracy operators $\xi(D_{M,d})$, $\xi({}^tD_{M,d})$ with $dM|N$. Then $\mathbb{T}'_{\mathbb{Q}} = Z(\mathbb{E})$ is the centre of $\mathbb{E}$ and*

$$\dim_{\mathbb{Q}}(\mathbb{E}) = \sum_{f \in \mathcal{N}_2(\Gamma)} n_f^2. \tag{11}$$

Proof. As before, write $X = X_H(N)$. It is well-known that $\mathbf{E} := \mathrm{End}^0_{\mathbb{Q}}(J_X)$ acts *faithfully* on the space(s) $\Omega^1(J_X/\mathbb{Q}) \simeq \Omega^1(X/\mathbb{Q}) = H^0(X, \omega_{X/\mathbb{Q}})$ of holomorphic differentials of $J_X/\mathbb{Q}$ and $X/\mathbb{Q}$ (cf. e.g. [3]). Thus, the same is true for the subalgebra $\mathbb{E}$ and hence $\mathbb{E} \otimes \mathbb{C}$ acts faithfully on $\Omega^1(X_\Gamma/\mathbb{C}) = \Omega^1(X/\mathbb{Q}) \otimes \mathbb{C}$. Now via the identification $S_2(\Gamma) \xrightarrow{\sim} \Omega^1(X_\Gamma/\mathbb{C})$, the action of $\mathbb{E} \otimes \mathbb{C}$ on $S_2(\Gamma)$ is the same as that given by the double cosets (cf. [8], p. 171), so that we have a ring isomorphism $\mathbb{E} \otimes \mathbb{C} \simeq \mathbb{E}_{2,\mathbb{C}}$. Thus, by Theorem 5 (or by Theorem 11) we see that $\dim_{\mathbb{Q}} \mathbb{E} = \dim_{\mathbb{C}} \mathbb{E} \otimes \mathbb{C} = \dim_{\mathbb{C}} \mathbb{E}_{2,\mathbb{C}} = \sum_{f \in \mathcal{N}_2(\Gamma)} n_f^2$, which proves (11).

Furthermore, since by Theorem 11 we have $Z(\mathbb{E}) \otimes \mathbb{C} = Z(\mathbb{E} \otimes \mathbb{C}) = \mathbb{T}'_{\mathbb{Q}} \otimes \mathbb{C}$ (equality as subalgebras of $\mathbb{E} \otimes \mathbb{C}$), it follows that $Z(\mathbb{E}) = \mathbb{T}'_{\mathbb{Q}}$.

We can refine the above proposition by determining the isotypic $\mathbb{E}$-module decomposition of the $\mathbb{E}$-module $\Omega(J_X/\mathbb{Q}) \simeq S_2(\Gamma, \mathbb{Q})$, where the latter denotes space of cusp form $f \in S_2(\Gamma)$ with rational Fourier coefficients. For this, let $[f] = fG_{\mathbb{Q}}$ denote the Galois orbit of $f \in \mathcal{N}(\Gamma)$ and put $S_{[f]} = (\oplus_{g \in [f]} S_g) \cap S_2(\Gamma, \mathbb{Q})$; cf. [2], p. 36. We then have:

Corollary 15. *Each $S_{[f]}$ is an irreducible $\mathbb{E}$-module, and every irreducible $\mathbb{E}$-module is of this form. Thus, the isotypic $\mathbb{E}$-module decomposition of $\Omega^1(J_X/\mathbb{Q})$ is given by*

$$\Omega^1(J_X/\mathbb{Q}) \simeq S_2(\Gamma, \mathbb{Q}) \simeq \bigoplus_{f \in \mathcal{N}(\Gamma)/G_{\mathbb{Q}}} S_{[f]}. \tag{12}$$

Proof. It is immediate that each $S_{[f]}$ is a $\mathbb{E}$-module. Since $S_{[f]} \otimes \mathbb{C} = \oplus_{g\in[f]} S_g$, we see from Theorem 11 (together with the fact that $S_g \not\simeq S_{g'}$, if $g \neq g'$) that $S_{[f]} \otimes \mathbb{C}$ cannot have any nontrivial $\mathbb{E} \otimes \mathbb{C}$-submodules which are $G_{\mathbb{Q}}$-stable. Thus, $S_{[f]}$ is an irreducible $\mathbb{E}$-module.

Since $\Omega^1(J_X/\mathbb{Q}) \simeq \Omega^1(X/\mathbb{Q}) \simeq S_2(\Gamma, \mathbb{Q})$ (cf. [2], p. 35), we thus see that (12) is the decomposition of $\Omega^1(J_X/\mathbb{Q})$ into pairwise non-isomorphic irreducible $\mathbb{E}$-modules. In particular, every irreducible $\mathbb{E}$-module is isomorphic to some $S_{[f]}$ because $\Omega^1(J_X/\mathbb{Q})$ is a faithful $\mathbb{E}$-module (and $\mathbb{E}$ is semisimple).

We next study the structure of the algebra $\mathbf{E} = \mathrm{End}^0_{\mathbb{Q}}(J_X)$. To this end, recall that by the Shimura construction, each (weight 2) normalized newform $f \in \mathcal{N}(\Gamma) = \mathcal{N}_2(\Gamma)$ of some level $N_f|N$ defines an abelian variety $A_f/\mathbb{Q}$ of dimension $[K_f : \mathbb{Q}]$, where $K_f = \mathbb{Q}(\{a_n\}_{n\geq 1})$ denotes the field generated by the coefficients of $f = \sum a_n q^n$; cf. [8], p. 183, [9] or [3]. (Note that $A_f = A_{f^\sigma}$, for any Galois conjugate f^σ, where $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.) Then the abelian varieties A_f determine J_X up to $\mathbb{Q}$-isogeny, for we have the relation

$$J_X \sim \prod_{f\in\mathcal{N}(\Gamma)/G_{\mathbb{Q}}} A_f^{m_f}, \tag{13}$$

for some positive integers m_f; cf. Ribet[7], Proposition (2.3). (We shall see below that $m_f = n_f := \dim S_f$; cf. Remark 18(a).)

In order to deduce Theorem 6 from (13), we require the following facts which were (essentially) proven by Ribet[7]:

Theorem 16. *(a)* $\mathrm{End}^0_{\mathbb{Q}}(A_f) \simeq K_f$*, for all* $f \in \mathcal{N}(\Gamma)$.

(b) If $f, g \in \mathcal{N}(\Gamma)$*, then* $A_f \sim A_g$ *if and only if* $g = f^\sigma$*, for some* $\sigma \in G_{\mathbb{Q}}$.

Proof. (a) Ribet[7], Corollary 4.2.

(b) This follows from Ribet's results; cf. [1], Proposition 3.2.

Corollary 17. $\dim Z(\mathrm{End}^0_{\mathbb{Q}}(J_X)) = \#\mathcal{N}(\Gamma) = \dim \mathbb{T}'_{\mathbb{Q}}$.

Proof. By Theorem 16(a) we see that each A_f is $\mathbb{Q}$-simple, and hence by part (b) we have $\mathrm{Hom}^0_{\mathbb{Q}}(A_f, A_g) = 0$ if $f \neq g^\sigma$, for all $\sigma \in G_{\mathbb{Q}}$. We thus obtain from (13) that

$$\mathrm{End}^0_{\mathbb{Q}}(J_X) \simeq \prod_{f\in\mathcal{N}(\Gamma)/G_{\mathbb{Q}}} \mathrm{End}^0_{\mathbb{Q}}(A_f^{m_f}) \simeq \prod_{f\in\mathcal{N}(\Gamma)/G_{\mathbb{Q}}} M_{m_f}(K_f), \tag{14}$$

and that hence

$$\dim Z(\mathrm{End}^0_{\mathbb{Q}}(J_X)) = \dim \prod_{f\in\mathcal{N}(\Gamma)/G_{\mathbb{Q}}} K_f = \sum_{f\in\mathcal{N}(\Gamma)/G_{\mathbb{Q}}} [K_f : \mathbb{Q}] = \#\mathcal{N}(\Gamma), \tag{15}$$

where the last equation follows from the fact that $\#(fG_{\mathbb{Q}}) = [K_f : \mathbb{Q}]$. Since $\dim \mathbb{T}'_{\mathbb{Q}} = \dim_{\mathbb{C}} \mathbb{T}'_{2,\mathbb{C}} = \#\mathcal{N}(\Gamma)$ (cf. comment after equation (10)), the assertion follows.

Proof of Corollary 3. Since $\mathbb{E}_{\mathbb{C}} := \mathbb{E} \otimes \mathbb{C} \subset \mathbf{E}_{\mathbb{C}} := \mathbf{E} \otimes \mathbb{C} \subset \mathrm{End}_{\mathbb{C}}(S)$, we have $Z(\mathbf{E}_{\mathbb{C}}) \subset C_S(\mathbf{E}_{\mathbb{C}}) \subset C_S(\mathbb{E}_{\mathbb{C}}) = \mathbb{T}'_{2,\mathbb{C}}$, the latter by Theorem 11. Now by Corollary 17 we have $\dim_{\mathbb{C}}(\mathbf{E}_C) = \dim \mathbb{T}'_{2,\mathbb{C}}$, and so we have equality throughout, i.e. $Z(\mathbf{E}_{\mathbb{C}}) = C_S(\mathbf{E}_{\mathbb{C}}) = C_S(\mathbb{E}_{\mathbb{C}}) = \mathbb{T}'_{2,\mathbb{C}}$.

Proof of Theorem 1. Since $\mathbb{E}_{\mathbb{C}} = \mathbb{E} \otimes \mathbb{C}$ and $\mathbf{E}_{\mathbb{C}} = \mathbf{E} \otimes \mathbb{C}$ are semi-simple subalgebras of $\mathrm{End}_{\mathbb{C}}(S)$ with $C_S(\mathbb{E}_{\mathbb{C}}) = C_S(\mathbf{E}_{\mathbb{C}})$ (cf. proof of Corollary 3), it follows from the double centralizer theorem that $\mathbb{E}_{\mathbb{C}} = \mathbf{E}_{\mathbb{C}}$. Thus $\mathbb{E} = \mathbf{E}$, as asserted.

Proof of Corollary 2. By construction (cf. §2) we have $\tilde{\mathbb{E}} \subset \tilde{\mathbb{M}}$, and so the image $\mathbb{M}$ of $\tilde{\mathbb{M}} \otimes \mathbb{Q}$ in $\mathrm{End}^0_{\mathbb{Q}}(J_X)$ contains the image $\mathbb{E}$ of $\tilde{\mathbb{E}} \otimes \mathbb{Q}$. Thus, since $\mathbf{E} = \mathbb{E}$ by Theorem 1, we have $\mathbf{E} \subset \mathbb{M}$, as claimed.

Proof of Corollary 4. Since $S = S_2(\Gamma, \mathbb{Q}) \otimes \mathbb{C}$ and $C_S(\mathbf{E}_{\mathbb{C}}) = \mathbb{T}'_{\mathbb{C}}$ by the proof of Corollary 3, the first assertion follows (via the isomorphism $\Omega^1(J_X) \simeq S_2(\Gamma, \mathbb{Q})$). The second assertion follows from this by Theorem 4.4 (or Corollary 4.6) of [3].

Proof of Theorem 6. By (14) it is enough to show that $m_f = n_f$, for all $f \in \mathcal{N}(\Gamma)$. For this, fix $f \in \mathcal{N}(\Gamma)$ and let $\mathbf{E}_f = \mathrm{End}^0(A_f^{m_f})$, which by (13) (and Theorem 16) is naturally a simple two-sided ideal of $\mathbf{E}$. Since $\mathbb{E} = \mathbf{E}$ by Theorem 1, we know by Corollary 15 that $S_{[f]}$ is an irreducible (right) $\mathbf{E}$-module. By the Shimura construction we know that $S_{[f]}\mathbf{E}_f \neq 0$, and so $S_{[f]}$ is a faithful irreducible $\mathbf{E}_f$-module. Thus, since $\mathbf{E}_f \simeq M_{m_f}(K_f)$, we see that $\dim_{\mathbb{Q}} S_{[f]} = m_f[K_f : \mathbb{Q}]$. On the other hand, since $S_{[f]} \otimes \mathbb{C} = \oplus_{g \in [f]} S_g$, we have $\dim_{\mathbb{Q}} S_{[f]} = (\dim_{\mathbb{C}} S_f)[K_f : \mathbb{Q}] = n_f[K_f : \mathbb{Q}]$, and so $m_f = n_f$.

Remark 18. (a) It follows from the above proof that (13) holds with $m_f = n_f = \dim S_f = \sigma_0(N/N_f)$. This was asserted without proof in [1], equation (3.4).

(b) All the above results also hold for the curves $X_H(N', t)$ associated to the groups $\Gamma_H(N', t) = \beta_t \Gamma_H(tN')\beta_t^{-1}$ of Remark 13(b); in fact, the matrix β_t induces a $\mathbb{Q}$-isomorphism $(\beta_t)_* : X_H(N't) \xrightarrow{\sim} X_H(N', t)$.

(c) In a letter to the author, Ken Ribet (July 2005) pointed out that it is possible to deduce Corollary 3 and the first assertion of Corollary 4 directly from Theorem 6 together with the fact that $\mathbb{T}' \subset Z(\mathbf{E})$.

Example 19. (a) If $J_0(p^2)$ is the Jacobian of the modular curve $X_0(p^2)/\mathbb{Q}$, where p is a prime, then

$$\mathrm{End}^0_{\mathbb{Q}}(J_0(p^2)) = \langle \mathbb{T}'_{\mathbb{Q}}, \tau, \xi(T_p), \xi({}^tT_p) \rangle_{\mathbb{Q}} = \langle \mathbb{T}'_{\mathbb{Q}}, \tau, \tau' \rangle_{\mathbb{Q}}, \tag{16}$$

where $\tau = \eta^* \eta_*$ and $\tau' = (\eta')^* \eta'_*$ are the endomorphisms associated to the degeneracy maps $\eta := B_{p,1} : X_0(p^2) \to X_0(p)$ and $\eta' := B_{p,p} : X_0(p^2) \to X_0(p)$.

(b) If $J(p)$ is the Jacobian of the modular curve $X(p)/\mathbb{Q}$ defined by the principal congruence subgroup $\Gamma(p)$, then

$$\mathrm{End}^0_{\mathbb{Q}}(J(p)) = \langle \mathbb{T}'_{\mathbb{Q}}, \tilde{\tau}, \xi(T_p), \xi({}^tT_p)\rangle_{\mathbb{Q}} = \langle \mathbb{T}'_{\mathbb{Q}}, \tilde{\tau}, \tilde{\tau}'\rangle_{\mathbb{Q}}, \tag{17}$$

where $\tilde{\tau} = \tilde{\eta}^*\tilde{\eta}_*$ and $\tilde{\tau}' = (\tilde{\eta}')^*\tilde{\eta}'_*$ are the endomorphisms associated to the covers $\tilde{\eta} : X(p) \to X^1(p)$ and $\tilde{\eta}' : X(p) \to X_1(p)$ which are induced by the inclusions $\Gamma^1(p) \subset \Gamma(p)$ and $\Gamma_1(p) \subset \Gamma(p)$, respectively.

Proof. (a) Applying Theorem 1 with $N = p^2$ and $H = (\mathbb{Z}/p^2\mathbb{Z})^\times$ yields $\mathrm{End}^0_{\mathbb{Q}}(J_0(p^2)) = \langle \mathbb{T}'_{\mathbb{Q}}, \xi(D_{p,1}), \xi(D_{p,p}), \xi({}^tD_{p,p})\rangle_{\mathbb{Q}}$. (Note that $\xi(D_{p^2,1}) = id$ and that $\xi(D_{1,d}) = 0$ because $X_H(1) = X(1)$ has genus 0). Now $\xi(D_{p,1}) = \tau$ by definition because $\Gamma_H(p) = \Gamma_0(p)$. Moreover, since ${}^tT_p \subset D_{p,p}$ (cf. (3)) and since by (2) $\deg D_{p,p} = [\Gamma_0(p) : \Gamma_0(p^2)] = p = \deg {}^tT_p$, we see that $D_{p,p} = {}^tT_p$ and hence that also ${}^tD_{p,p} = T_p$. This proves the first equality of (16).

To prove the second equality, we shall apply Corollary 12 to $\mathbb{E}' = \langle \mathbb{T}'_{2,\mathbb{C}}, [\tau]_2, [\tau']_2\rangle_{\mathbb{C}}$. Since ${}^t\tau = \tau$ and ${}^t\tau' = \tau'$, it is clear that $\mathbb{E}'$ is semi-simple. Consider $\tilde{D}_{p,p} := [\tau\tau']_2 \in \mathbb{E}'$, and let $T = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Since $\{T^a\}_{0\le a\le p-1}$ is a system of coset representatives of $\Gamma_0(p)/\Gamma_0(p,p)$, we see that $f|[\tau']_2 = \sum_{a=0}^{p-1} f|_2\alpha_p T^a\beta_p = f|T_p\beta_p$. Now since $\mathrm{Im}([\tau]) = S_2(\Gamma_0(p))$ and since T_p acts bijectively on $S_2(\Gamma_0(p))$ (use [5], Th. 4.6.17), we thus see that $\mathrm{Im}([\tau\tau']) = S_2(\Gamma_0(p))\beta_p$. By Corollary 12 we therefore have that $\mathbb{E}' = \mathbb{E}_{2,\mathbb{C}}$, and so $\mathbb{E}$ is generated by $\mathbb{T}'_{\mathbb{Q}}$, τ, and τ'. This proves the second equality of (16).

(b) We observe that the proof of (a) shows more generally that if H is any subgroup with $\mathrm{Ker}(r_{p^2,p}) \le H \le (\mathbb{Z}/p^2\mathbb{Z})^\times$, then the analogous formula of (16) holds for the Jacobian $J_H(p^2)$ of the curve $X_H(p^2)$, i.e.

$$\mathrm{End}^0_{\mathbb{Q}}(J_H(p^2)) = \langle \mathbb{T}'_{\mathbb{Q}}, \tau_H, \xi(T_p), \xi({}^tT_p)\rangle_{\mathbb{Q}} = \langle \mathbb{T}', \tau_H, \tau'_H\rangle_{\mathbb{Q}}, \tag{18}$$

where $\tau_H = \eta_H^*(\eta_H)_*$ and $\tau'_H = (\eta'_H)^*(\eta'_H)_*$ are defined by the degeneracy maps $\eta_H := B_{p,1} : X_H(p^2) \to X_H(p)$ and $\eta'_H := B_{p,p} : X_H(p^2) \to X_H(p)$.

Applying this to $H = \mathrm{Ker}(r_{p^2,p})$ and noting that $\Gamma(p) = \Gamma_H(p,p) = \beta_p\Gamma_H(p^2)\beta_p^{-1}$, we see that $\mathrm{End}^0_{\mathbb{Q}}(J(p)) = \langle \mathbb{T}'_{\mathbb{Q}}, \rho_p(\tau_H), \xi(T_p), \xi({}^tT_p)\rangle_{\mathbb{Q}} = \langle \mathbb{T}'_{\mathbb{Q}}, \rho_p(\tau_H), \rho_p(\tau'_H)\rangle_{\mathbb{Q}}$; cf. Remarks 18(b) and 13(b). Now since $\beta_p\Gamma_H(p)\beta_p^{-1} = \Gamma_H(1,p) = \Gamma^1(p)$, we see that $\rho_p(\tau_H) = \tilde{\tau}$. Moreover, $\rho_p(\tau'_H) = \tilde{\tau}'$ because $f|\rho_p(\tau'_H) = f|\beta_p[\tau']_2\beta_p^{-1} = \sum f|T^a = f|[\tilde{\tau}']$, and so (17) holds.

Acknowledgements. I would like to thank Ken Ribet for his helpful comments on this paper; cf. Remark 18(c). In addition, I would like to gratefully acknowledge receipt of funding from the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] M. Baker, E. González-Jiménez, J. Gonzalez, B. Poonen, Finiteness results for modular curves of genus at least 2. *Am. J. Math.* **127** (2005), 1325-1387.

[2] H. Darmon, F. Diamond and R. Taylor, Fermat's last theorem. In: *Current Developments in Mathematics, 1995* (R. Bott et al, eds.), International Press Inc., Boston, 1994, pp. 1–154.

[3] E. Kani, Abelian subvarieties and the Shimura construction. Preprint.

[4] B. Mazur, Rational isogenies of prime degree. *Inv. math.* **44** (1978), 129-162.

[5] T. Miyake, *Modular Forms.* Springer-Verlag, Berlin, 1989.

[6] K. Ribet, Endomorphisms of semi-stable abelian varieties over number fields. *Ann. Math.* **101** (1975), 555–562.

[7] K. Ribet, Twists of newforms and endomorphisms of abelian varieties. *Math. Ann.* **253** (1980), 43–62.

[8] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, NJ, 1971.

[9] G. Shimura, On the factors of the Jacobian variety of a modular function field. *J. Math. Soc. Japan* **25** (1973), 523–544.