OPTIMAL QUOTIENTS OF MODULAR JACOBIANS

Matthew Emerton

Northwestern University

Abstract. Let N be a positive integer, and f a normalized newform of weight two on $\Gamma_0(N)$. Attached to f is an optimal quotient A_f of the Jacobian $J_0(N)$. We prove two theorems concerning such optimal quotients. (A) Let $\mathbb{T}$ denote the algebra of endomorphisms of $J_0(N)$ generated by the Hecke operators, and let $\mathfrak{F}_f$ denote the ideal of fusion of f in $\mathbb{T}$. If $\hat{A}_f$ denotes the dual abelian variety to A_f, then the canonical polarization of $J_0(N)$ induces a polarization $\theta_f : \hat{A}_f \to A_f$. We show that there is an embedding $\ker(\theta_f) \subset J_0(N)[\mathfrak{F}_f]$ whose cokernel is supported at maximal ideals $\mathfrak{m}$ of $\mathbb{T}$ for which $J_0(N)[\mathfrak{m}]$ is *not* two-dimensional. (B) If N is prime, let C denote the subgroup of $J_0(N)$ generated by the divisor $0 - \infty$ on $X_0(N)$. Mazur has shown that C is equal to the full torsion subgroup of $J_0(N)(\mathbb{Q})$, and that specialization modulo N induces an isomorphism of C with the group of connected components $\Phi_{J_0(N)}$ of the characteristic N fibre of the Néron model of $J_0(N)$. We prove that analogous results hold for every optimal quotient of prime conductor, thereby generalizing results of Mestre and Oesterlé (who treated the case of strong Weil curves) and confirming William Stein's *refined Eisenstein conjecture*. The key idea in the proof of these two theorems is encapsulated in corollary 2.5 below, which allows us to apply multiplicity one results in a novel way to the study of optimal quotients.

Let N be a positive integer, let $S(N)$ denote the space of weight two cuspforms on $\Gamma_0(N)$, and let $\mathbb{T}$ denote the $\mathbb{Z}$-algebra of Hecke operators acting on $S(N)$. If f is a newform, let I_f denote the ideal in $\mathbb{T}$ that is the kernel of the map $\mathbb{T} \to \mathbb{C}$ induced by the action of the Hecke operators on f. We let $J_0(N)$ denote the Jacobian of the modular curve $X_0(N)$; then $\mathbb{T}$ acts on $J_0(N)$ by Picard functoriality, and we write $A_f = J_0(N)/I_f$. We refer to A_f as the *optimal quotient* of $J_0(N)$ attached to f. The aim of this paper is to prove two results concerning such optimal quotients, which we will describe in turn.

Our first result relates the kernel of the canonical polarization θ_f of A_f to the ideal of fusion $\mathfrak{F}_f$ of f. Before stating the result, we recall the relevant notions.

We begin with the construction of the polarization θ_f. If A is an abelian variety, let $\hat{A}$ denote its dual. The Jacobian $J_0(N)$ is endowed with a canonical principal polarization $\theta : J_0(N)\hat{} \to J_0(N)$, which induces a polarization $\theta_f : \hat{A}_f \to A_f$. More precisely, if π_f denotes the surjection $J_0(N) \to A_f$, then dualizing yields an embedding $\hat{\pi}_f : \hat{A}_f \to J_0(N)\hat{}$. (That this is an embedding follows from the fact that $\ker \pi_f = I_f J_0(N)$ is connected.) The polarization θ_f is equal to the composite $\theta_f = \pi_f \circ \theta \circ \hat{\pi}_f$.

We now define the ideal of fusion $\mathfrak{F}_f$. Let S_f denote the subspace of $S(N)$ spanned by f and its Galois conjugates, and write $S_f^{\perp}$ for the orthogonal complement of S_f under the Petersson inner product. Note that I_f is the annihilator of S_f

in $\mathbb{T}$; we let $I_f^\perp$ denote the annihilator of $S_f^\perp$ in $\mathbb{T}$. We define the *ideal of fusion* of f to be the ideal $\mathfrak{F}_f = I_f + I_f^\perp$ in $\mathbb{T}$. Then $\mathfrak{F}_f$ has finite index in $\mathbb{T}$, and "measures" the congruences between f and normalized Hecke eigenforms in $S_f^\perp$.

Finally, we introduce some terminology regarding maximal ideals of $\mathbb{T}$. If $\mathfrak{m}$ is such a maximal ideal, then attached canonically to $\mathfrak{m}$ is a semi-simple representation $\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}/\mathfrak{m})$ [12, prop. 5.1]. We say that $\mathfrak{m}$ satisfies *multiplicity one* if $J_0(N)[\mathfrak{m}]$ is two-dimensional over the residue field $\mathbb{T}/\mathfrak{m}$. (The motivation for this terminology is that if $\rho_{\mathfrak{m}}$ is irreducible, then $J_0(N)[\mathfrak{m}]$ is isomorphic to a direct sum of copies of $\rho_{\mathfrak{m}}$ [2], and so $\mathfrak{m}$ satisfies multiplicity one if and only if $J_0(N)[\mathfrak{m}]$ is isomorphic to a single copy of $\rho_{\mathfrak{m}}$.)

We now state our first result.

Theorem A. *Let f be a normalized new form in $S(N)$. If we embed $\hat{A}_f$ into $J_0(N)$ via the composite $\theta \circ \hat{\pi}_f : \hat{A}_f \to J_0(N)$, then this restricts to an embedding $\ker(\theta_f) \to J_0(N)[\mathfrak{F}_f]$ whose cokernel is supported at maximal ideals of $\mathbb{T}$ that do not satisfy multiplicity one.*

This theorem is related to [20, thm. 3], which (for prime N) relates the modular degree of a strong Weil curve and the modulus of congruence of the corresponding eigenform. However, even when A_f is an elliptic curve, the above result differs from that of [20], insofar as it relates the kernel of θ_f to the kernel of $\mathfrak{F}_f$ on the entire Jacobian $J_0(N)$. (Consider the examples discussed below, involving certain Weil curves of conductors 431 and 503.)

The strength of the result stems from the fact that "many" maximal ideals of $\mathbb{T}$ are known to satisfy multiplicity one. For example, if $\rho_{\mathfrak{m}}$ is irreducible, if the residue characteristic ℓ of $\mathfrak{m}$ is odd, and if ℓ is prime to N, or if ℓ exactly divides N and $\mathfrak{m}$ is not ℓ-old, then [12, thm. 5.2 (b)] and [7, main theorem] show that $\mathfrak{m}$ satisfies multiplicity one. (The result of [7] is strengthened by the results of [13]. Some cases of residue characteristic two are treated in [3]. See also [15, thm. 3.5] for a related summary of results.) If N is prime, then the results of [6] show that *all* $\mathfrak{m}$ of odd residue characteristic satisfy multiplicity one.

We should point out, though, that multiplicity one need not hold for all maximal ideals (even if N is prime), and that correspondingly the cokernel of the inclusion $\ker(\theta_f) \subset J_0(N)[\mathfrak{F}_f]$ need not vanish. We illustrate this by an example. Calculations of Lloyd Kilford and William Stein show that when $N = 431$ or 503 there is a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ having residue characteristic two that does not satisfy multiplicity one. Furthermore, there is a strong Weil curve E arising from a newform f of level N for which the $\mathfrak{m}$-adic completion of $\mathfrak{F}_f$ is non-trivial. Thus $J[\mathfrak{m}] \subset J[\mathfrak{F}_f]$. On the other hand, $J[\mathfrak{m}]$ cannot be contained in $\ker\theta_f$, since $J[\mathfrak{m}] \cap E = E[2]$, and the fact that $\mathfrak{m}$ does not satisfy multiplicity one shows that the inclusion $E[2] \subset J[\mathfrak{m}]$ is not an equality.

The second result that we prove is Stein's *refined Eisenstein conjecture* [19, conj. 1.1]. This is a conjecture that concerns optimal quotients of prime conductor. Recall that if N is prime, then the results of [6] give a very precise description of the arithmetic properties of $J_0(N)$. If C denotes the subgroup of $J_0(N)$ generated by image of the divisor $0 - \infty$ on $X_0(N)$, then C is a finite subgroup of $J_0(N)(\mathbb{Q})$ that in fact equals the full torsion subgroup of $J_0(N)(\mathbb{Q})$ [6, thm. III.1.2]. Also, if $\Phi_{J_0(N)}$ denotes the group of connected components of the characteristic N fibre of the Néron model $J_0(N)$, then the specialization map $C \to \Phi_{J_0(N)}$ is an isomorphism [6, p. 99].

Stein has conjectured that the analogous statements are true for each optimal quotient of A_f, and that furthermore, if $\{f_i\}$ denotes a complete set of conjugacy class representatives of normalized eigenforms in $S(N)$, then the product of the orders of the torsion subgroups of the $A_{f_i}(\mathbb{Q})$ is equal to the order of C. The following theorem proves his conjecture in its entirety.

Theorem B. *Let f be a newform of weight two and prime conductor N. Let C_f denote the image of C in A_f (so that C_f is the subgroup of A_f generated by the image of the divisor $0 - \infty$ on $X_0(N)$); C_f is a $\mathbb{T}$-submodule of the torsion subgroup $A_f(\mathbb{Q})_{\mathrm{tor}}$ of the group of $\mathbb{Q}$-rational points on A_f. Let Φ_{A_f} (respectively $\Phi_{\hat{A}_f}$) denote the group of connected components of the characteristic N fibre of the Néron model of A_f (respectively $\hat{A}_f$).*

(i) The $\mathbb{T}$-module C_f is isomorphic to C/I_f.

(ii) The inclusion $C_f \to A_f(\mathbb{Q})_{\mathrm{tor}}$ is an isomorphism of $\mathbb{T}$-modules.

(iii) The $\mathbb{T}$-module $\hat{A}_f(\mathbb{Q})_{\mathrm{tor}}$ is abstractly isomorphic to C_f.

(iv) The specialization map $A_f(\mathbb{Q})_{\mathrm{tor}} \to \Phi_{A_f}$ is an isomorphism of $\mathbb{T}$-modules.

(v) The specialization map $\hat{A}_f(\mathbb{Q})_{\mathrm{tor}} \to \Phi_{\hat{A}_f}$ is an isomorphism of $\mathbb{T}$-modules.

(vi) The (étale) group schemes Φ_{A_f} and $\Phi_{\hat{A}_f}$ over $\mathbb{F}_N$ are constant (that is, have trivial Galois action).

(vii) If $\{f_i\}$ is a complete set of conjugacy class representatives of the normalized eigenforms in $S(N)$, then $\prod_{f_i} \#C_{f_i} = \#C$.

In the special case when A_f is an elliptic curve, parts (ii), (iii), (iv), (v) and (vi) of this result were proved by Mestre and Oesterlé [8, §5] (in this case parts (iii) and (v) follow from parts (ii) and (iv), because the elliptic curve A_f is self-dual). Their proof depends on calculations that are very particular to the situation of elliptic curves. The most powerful tools that they use are Mazur's classification of the possible torsion subgroups of the group of $\mathbb{Q}$-rational points of an elliptic curve over $\mathbb{Q}$ [6, thm. III.5.1], and Ribet's lowering-the-level theorem [12, thm. 1.1]. Our proof also depends on the results of [6], in a more direct fashion – we use crucially Mazur's description of the commutative algebra properties of the Eisenstein ideal of $\mathbb{T}$, as well as his calculation of the kernel of the Eisenstein ideal acting on $J_0(N)$. We also depend on the work of both Ribet and Tate on Serre's conjectures (in particular, [14, prop. 2.2]).

One general difficulty in studying optimal quotients is that the description of the kernel of the map $J_0(N) \to A_f$ as being $I_f J_0(N)$ is difficult to work with. A potentially more useful description is that it is equal to the connected component of $J_0(N)[I_f^{\perp}]$. However, *a priori* the latter algebraic subgroup of $J_0(N)$ may not be connected, and without control of its connected component group, this characterization would again be rather unsatisfactory. The key to the proof of both theorems A and B is the following result, which provides the necessary control: if $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ that satisfies multiplicity one, then the $\mathfrak{m}$-adic completion of the connected component group of $J_0(N)[I_f]$ is trivial, and so the inclusion $I_f J_0(N) \subset J_0(N)[I_f^{\perp}]$ induces an isomorphism on $\mathfrak{m}$-divisible groups. With this result in hand, it is easy to relate properties of optimal quotients to the commutative algebra properties of the Hecke ring (as long as one is willing to forsake information supported away from the multiplicity one maximal ideals of $\mathbb{T}$). By itself it is already enough to imply theorem A, and when combined with the results of [6], to prove part (ii) of theorem B.

The result itself is proved in section 2, in a suitably abstracted situation; it is a special case of corollary 2.5. The rest of that section is devoted to elaborating some of its consequences.

To obtain information about the connected component groups Φ_{A_f} we apply the results of section 2 in the context of rigid analytic uniformizations of $J_0(N)$ and its optimal quotients. This is the subject of section 3. The key result is corollary 3.6.

Section 4 presents the proofs of theorems A and B. In order to prove theorem B in its entirety, we find it necessary to generalize the notion of optimal quotient, and introduce a more flexible notion of an optimal subquotient of $J_0(N)$. We then prove a more general version of theorem B for optimal subquotients (theorem 4.13), which has theorem B as an immediate corollary.

In section 1 we develop the algebra that is needed for the later sections. This section is intended to organize as usefully as possible the information on the commutative algebra of Hecke rings that can be deduced from the results of [6].

To conclude this introduction, let us emphasize that we regard the main technical innovation of this paper to be the results of section 2, which allow us to apply multiplicity one results to obtain precise descriptions of the Tate-modules of optimal quotients. We hope that these results might have additional applications to the analysis of optimal quotients.

Acknowledgments. I would like to thank William Stein and Shuzo Takahashi for their comments on some earlier versions of this paper. I would also like to thank the anonymous referee for their careful examination of the paper, which led to the clarification of several obscure points in the exposition.

0. NOTATION AND CONVENTIONS

All rings and algebras that we consider are commutative with unit. If I_1 and I_2 are two ideals of a ring R, we write $(I_1 : I_2) = \{r \in R \,|\, rI_2 \subset I_1\}$. If I is an ideal of R we also write $I^\perp = (0 : I) = \mathrm{Ann}_R(I)$. (See lemma 4.1 below for a reconcilliation of this use of the notation $I^\perp$ with the notation $I_f^\perp$ used in the introduction.)

If M is a locally compact abelian group, we write M^* for the Pontrjagin dual of M. We will apply this notation only in the cases when M is either ind-finite (that is, torsion and discrete) or pro-finite. In these cases, $M^* = \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}/\mathbb{Z})$, with $\mathbb{Q}/\mathbb{Z}$ being regarded as a discrete group.

1. ALGEBRAIC PRELIMINARIES

In this section, we let R be a finite flat $\mathcal{O}$-algebra, where $\mathcal{O}$ is a Dedekind domain with field of fractions L. If we write that an R-module is "torsion", or "torsion-free", we will always mean that it is $\mathcal{O}$-torsion, or $\mathcal{O}$-torsion-free. We say that an ideal I of R is *saturated* if R/I is torsion-free. Note that the association of $I \otimes_{\mathcal{O}} L$ to I induces a bijection between the saturated ideals of R and the ideals of $R \otimes_{\mathcal{O}} L$. Note also that $I^\perp \otimes_{\mathcal{O}} L = (I \otimes_{\mathcal{O}} L)^\perp$.

Recall that R is *Gorenstein* if the R-module $\mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O})$ is locally free (necessarily of rank one). We say that R is *monogenic* if it is generated by a single element as an $\mathcal{O}$-algebra. If R is monogenic, then it is Gorenstein.

Lemma 1.1. *Let I_1 and I_2 be two ideals of R. If I_1 is saturated then $(I_1 : I_2)$ is saturated. In particular, for any ideal I of R, the ideal $I^\perp$ is saturated.*

Proof. This is immediate from the definitions. □

Lemma 1.2. *Suppose that R is either Gorenstein or reduced.*
(i) If I is a saturated ideal of R, then the inclusion $I \subset (I^\perp)^\perp$ is an equality.
(ii) If I_1 and I_2 are two saturated ideals of R, then $(I_2^\perp : I_1^\perp) = (I_1 : I_2)$.

Proof. Since $(I^\perp)^\perp/I \subset R/I$ is torsion free, by the assumption on I, it suffices to verify part (i) after tensoring over $\mathcal{O}$ with L. The assumption on R then implies that $R \otimes_{\mathcal{O}} L$ is Gorenstein. Since it also zero-dimensional, it is in fact a product of Gorenstein local rings. Thus (proceeding factor by factor) we may find a perfect $R\otimes_{\mathcal{O}} L$-bilinear pairing $(R\otimes_{\mathcal{O}} L)\times(R\otimes_{\mathcal{O}} L) \to L$. This pairing puts $(R\otimes_{\mathcal{O}} L)/(I\otimes_{\mathcal{O}} L)$ and $I^\perp \otimes_{\mathcal{O}} L = (I \otimes_{\mathcal{O}} L)^\perp$ in duality with one another. Applying this remark also with $I^\perp$ in place of I , and then counting dimensions over L, proves part (i).

To prove part (ii), note that for $r \in R$, $rI_1^\perp \subset I_2^\perp$ if and only if $rI_1^\perp I_2 = 0$, which holds if and only if $rI_2 \subset (I_1^\perp)^\perp$. Part (i) shows that $(I_1^\perp)^\perp = I_1$, and this establishes part (ii). □

Lemma 1.3. *If R is reduced and I is a saturated ideal of R, then the natural map $R \to R/I \oplus R/I^\perp$ is injective, with torsion cokernel.*

Proof. It suffices to check that the map $R \otimes_{\mathcal{O}} L \to (R \otimes_{\mathcal{O}} L)/(I \otimes_{\mathcal{O}} L) \oplus (R \otimes_{\mathcal{O}} L)/(I \otimes_{\mathcal{O}} L)^\perp$ is an isomorphism. This follows from that fact that our assumption on R implies that $R \otimes_{\mathcal{O}} L$ is reduced, and so is a product of fields. □

If I is an ideal in R then the surjection $R \to R/I$ gives rise to an embedding $\mathrm{Hom}_{\mathcal{O}}(R/I, \mathcal{O}) \to \mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O})$, identifying $\mathrm{Hom}_{\mathcal{O}}(R/I, \mathcal{O})$ with the R-module $\mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O})[I]$ of maps in $\mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O})$ that annihilate I.

Corollary 1.4. *If R is monogenic and I is a saturated ideal of R, then I is locally principal, and so (since it is a faithful $R/I^\perp$-module) is locally free of rank one over $R/I^\perp$.*

Proof. Since R is monogenic, the same is clearly true of R/I. Since both are also finite flat $\mathcal{O}$-algebras, they are both Gorenstein. Thus $\mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O})$ is, locally on $\mathrm{Spec}\, R$, isomorphic to R, and so by the preceding remark, there are, locally on $\mathrm{Spec}\, R$, isomorphisms between $\mathrm{Hom}_{\mathcal{O}}(R/I, \mathcal{O})$ and $I^\perp$. Since R/I is Gorenstein, we conclude $I^\perp$ is locally free of rank one over R/I. Replacing I by $I^\perp$ (and noting that $I = (I^\perp)^\perp$, since $I^\perp$ is locally free over R/I, or alternatively by part (i) of lemma 1.2), we establish the corollary. □

Another proof of corollary 1.4 follows by noting that any saturated ideal in the polynomial ring $\mathcal{O}[X]$ is locally principal.

Corollary 1.5. *If R is monogenic and $I_1 \subset I_2$ are saturated ideals of R, then $I_2^\perp \subset I_1^\perp$, and $I_1^\perp/I_2^\perp$ is a locally free $R/(I_1 : I_2)$-module of rank one.*

Proof. Since $I_1 \subset I_2$, it is immediate that $I_2^\perp \subset I_1^\perp$. Corollary 1.4 shows that $I_1^\perp$ is a locally principal ideal of R, and so $I_1^\perp/I_2^\perp$ is a locally free $R/(I_2^\perp : I_1^\perp)$-module of rank one. Part (ii) of lemma 1.2 now completes the proof (once we note that R is Gorenstein, since it is monogenic). □

Lemma 1.6. *If I_1 is a principal ideal of R for which R/I_1 is torsion, and I_2 is a saturated ideal of R, then $I_1 \cap I_2 = I_1 I_2$.*

Proof. Write $I_1 = rR$. Since R/I_1 is torsion, we deduce that r is a unit in $R \otimes_{\mathcal{O}} L$, and thus is a non-zero divisor in each of the torsion-free R-modules appearing in the exact sequence

$$0 \to I_2 \to R \to R/I_2 \to 0.$$

This implies that $I_2 \cap rR = rI_2$, proving the lemma. □

Corollary 1.7. *Suppose that I_1 is a principal ideal of R for which R/I_1 is torsion, and that I_2 is a saturated principal ideal of R. Then the surjection $I_2^{\perp}/(I_1 I_2^{\perp}) \to I_2^{\perp}(R/I_1)$ (defined by mapping $x \in I_2^{\perp}$ to the coset of x in R/I_1) and the inclusion $I_2^{\perp}(R/I_1) \to (R/I_1)[I_2]$ are both isomorphisms.*

Proof. Lemmas 1.1 and 1.6 show that $I_1 \cap I_2^{\perp} = I_1 I_2^{\perp}$. This implies the first statement of the corollary.

Note that there is an inclusion $I_1 + I_2^{\perp} \subset (I_1 : I_2)$. Write $I_1 = r_1 R$ and $I_2 = r_2 R$. Let $r \in (I_1 : I_2)$, so that $r_2 r = r_1 r'$ for some $r' \in R$. Then lemma 1.6 implies that $r_1 r' = r_1 r_2 r''$ for some $r'' \in R$, and so $r_2(r - r_1 r'') = 0$. Thus $r - r_1 r'' \in I_2^{\perp}$, and so in fact $I_1 + I_2^{\perp} = (I_1 : I_2)$. We conclude that

$$I_2^{\perp}(R/I_1) = (I_1 + I_2^{\perp})/I_1 = (I_1 : I_2)/I_1 = (R/I_1)[I_2].$$

This proves the second statement of the corollary. □

Corollary 1.8. *Suppose that R is monogenic, that I_1 is a principal ideal of R for which R/I_1 is torsion, and that $I_2 \subset I_3$ are saturated ideals of R. Then $((R/I_1)[I_2])/((R/I_1)[I_3])$ is a locally free $R/(I_1 + (I_2 : I_3))$-module of rank one.*

Proof. Corollary 1.4 shows that I_2 and I_3 are locally principal. Corollary 1.7 then shows that $((R/I_1)[I_2])/((R/I_1)[I_3])$ is (locally, and hence globally, since it is finitely generated and torsion) isomorphic to

$$(I_2^{\perp}/I_1 I_2^{\perp})/(I_3^{\perp}/I_1 I_3^{\perp}) = (I_2^{\perp}/I_3^{\perp})/(I_1(I_2^{\perp}/I_3^{\perp})).$$

Corollary 1.5 implies that $I_2^{\perp}/I_3^{\perp}$ is locally free of rank one over $R/(I_2 : I_3)$. This implies the corollary. □

2. RINGS OF OPERATORS ON ALGEBRAIC GROUPS

If G is a smooth commutative algebraic group over a field K of characteristic zero, then for any integer n we let $G[n]$ denote the the algebraic subgroup of G consisting of the n-torsion elements of G. Since we are in characteristic zero, multiplication by n is a smooth morphism from G to itself, and consequently $G[n]$ is a finite algebraic group (since a smooth morphism from a variety to itself must have finite fibres).

If n divides n', then $G[n] \subset G[n']$. We will be especially interested in the case when we fix a prime ℓ, and consider the ℓ-power torsion $G[\ell^n]$ of G. We write $G[\ell^\infty]$ for the ind-finite algebraic subgroup of G formed by the $G[\ell^n]$ as n ranges over all positive integers.

The formation of $G[\ell^\infty]$ is evidently functorial in G. If G is connected, then multiplication by ℓ is surjective from G to itself, and so $G[\ell^\infty]$ is an ℓ-divisible group.

For any G of the type we are considering, we will let G^0 denote the connected component of the identity of G. The quotient G/G^0 is a finite algebraic group, *the group of connected components of G*.

Let us remark that if we choose an algebraic closure $\overline{K}$ of K, then the $\overline{K}$-valued points of any finite algebraic group over K form a finite group, and we will not distinguish between a finite algebraic group over K and its group of $\overline{K}$-valued points. (This is permissible, since the finite algebraic group can be recovered up to isomorphism from its group of $\overline{K}$-valued points, equipped with its natural $\mathrm{Gal}(\overline{K}/K)$-action.)

We will require the following easily proved results:

Lemma 2.1. *The formation of $G[\ell^\infty]$ is exact in G.*

Proof. Let $H \subset G$ be an inclusion of smooth commutative algebraic groups over K. We must show that the exact sequence

$$0 \to H[\ell^\infty] \to G[\ell^\infty] \to (G/H)[\ell^\infty] \tag{2.2}$$

is also exact on the right. If H is connected, then $H(\overline{K})$ is divisible (and hence injective as an abelian group), and so we can be more precise: for any non-negative integer n we have a short exact sequence

$$0 \to H[\ell^n] \to G[\ell^n] \to (G/H)[\ell^n] \to 0.$$

On the other hand, if H is finite, then it is in particular torsion, and so it is clear that (2.2) is exact on the right.

In general, the kernel of the map $G/H^0 \to G/H$ is equal to the finite group H/H^0. Applying the results of the preceding paragraph successively to the finite group H/H^0 and to the connected group H^0, we find that (2.2) is exact on the right, as required. □

Lemma 2.3. *For any G as above and any prime ℓ, the inclusion $G^0[\ell^\infty] \to G[\ell^\infty]$ identifies $G^0[\ell^\infty]$ with the maximal ℓ-divisible subgroup of $G[\ell^\infty]$. The cokernel of this inclusion is canonically isomorphic to the ℓ-Sylow subgroup of G/G^0.*

Proof. Since multiplication by ℓ is surjective on the connected algebraic group G, it is clear that $G^0[\ell^\infty]$ is a divisible abelian group. Also, the quotient group $G[\ell^\infty]/G^0[\ell^\infty]$ embeds into G/G^0, the group of connected components of G. Since this latter group is finite, so is the former. In particular, we see that any divisible subgroup of $G[\ell^\infty]$ is contained in $G^0[\ell^\infty]$. (Recall that any quotient of a divisible abelian group is divisible, and that any finite divisible group is trivial.) This establishes the claim of the first sentence. The claim of the second sentence follows from lemma 2.1, which shows that

$$0 \to G^0[\ell^\infty] \to G[\ell^\infty] \to (G/G^0)[\ell^\infty] \to 0$$

is a short exact sequence. □

For the remainder of this section, let us fix a group G as above. Furthermore, let $\mathbb{T}$ denote a finite flat commutative $\mathbb{Z}$-algebra that acts on G. (As indicated in the introduction, in the applications $\mathbb{T}$ will be a Hecke algebra, as the notation suggests.) If I is any ideal in $\mathbb{T}$, we let $G[I]$ denote the algebraic subgroup of G consisting of elements annihilated by I. Taking R to be $\mathbb{T}$ and $\mathcal{O}$ to be $\mathbb{Z}$ puts us in a particular case of the situation of section 1. Thus we will say that an ideal I in $\mathbb{T}$ is saturated if the quotient $\mathbb{T}/I$ is torsion-free as a $\mathbb{Z}$-module.

If ℓ is any prime number then the ℓ-adic completion of $\mathbb{T}$ factors as the direct product of completions $\mathbb{T}_\mathfrak{m}$, where $\mathfrak{m}$ ranges over the maximal ideals of $\mathbb{T}$ of residue characteristic ℓ. Thus any object on which this ℓ-adic completion acts similarly factors. For example, $G[\ell^\infty]$ factors into such a product of ℓ-divisible subgroups. We let $G[\mathfrak{m}^\infty]$ denote the factor corresponding to the maximal ideal $\mathfrak{m}$. The formation of $G[\mathfrak{m}^\infty]$ is an exact functor of G, since lemma 2.1 shows that this is true of the formation of $G[\ell^\infty]$. Similarly, the ℓ-adic Tate module $T_\ell G$ (by which we refer to the

Pontrjagin dual $G[\ell^\infty]^* = \mathrm{Hom}(G[\ell^\infty], \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ of $G[\ell^\infty]$; this is the contravariant ℓ-adic Tate module) factors into such a product, and we let $T_\mathfrak{m}G$ denote the factor corresponding to the maximal ideal $\mathfrak{m}$. The formation of $T_\mathfrak{m}G$ is also an exact functor of G (since Pontrjagin duality is an exact functor).

Let us make a remark which we will use several times below. If I is an ideal of $\mathbb{T}$, and if we write $H = G[I]$, then there are natural isomorphisms $T_\mathfrak{m}G/I \xrightarrow{\sim} T_\mathfrak{m}H$ and $T_\mathfrak{m}(G/H) \xrightarrow{\sim} IT_\mathfrak{m}G$. Indeed, by the exactness of the formation of $\mathfrak{m}$-adic Tate modules, there is a short exact sequence

$$0 \to T_\mathfrak{m}(G/H) \to T_\mathfrak{m}G \to T_\mathfrak{m}H \to 0.$$

The fact that Pontrjagin duality is a perfect duality, together with the definition of $T_\mathfrak{m}G$ (respectively $T_\mathfrak{m}H$) as the Pontrjagin dual of $G[\mathfrak{m}^\infty]$ (respectively $H[\mathfrak{m}^\infty]$, which of course equals $G[\mathfrak{m}^\infty, I]$, the I-torsion subgroup of the ind-finite group $G[\mathfrak{m}^\infty]$), shows that the natural map $T_\mathfrak{m}G/IT_\mathfrak{m}G \to T_\mathfrak{m}H$ is an isomorphism. The preceding short exact sequence then yields the second of the two stated isomorphisms.

We say that a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ is *good* (or *good with respect to G*, if it is necessary to specify the group G) if $T_\mathfrak{m}G$ is a free $\mathbb{T}_\mathfrak{m}$-module.

Lemma 2.4. *Suppose that $\mathfrak{m}$ is good, and that I is a saturated ideal of $\mathbb{T}$. Then the ind-finite group $G[\mathfrak{m}^\infty, I]$ is ℓ-divisible.*

Proof. This follow by Pontrjagin duality. More precisely, $G[\mathfrak{m}^\infty, I] = (T_\mathfrak{m}G)^*[I] = (T_\mathfrak{m}/I)^*$, showing that $T_\mathfrak{m}G/I$ is the Pontrjagin dual of $G[\mathfrak{m}^\infty, I]$. (This fact was already used in the preceding remark.) Now $G[\mathfrak{m}^\infty, I]$ is ℓ-divisible if and only if its Pontrjagin dual $T_\mathfrak{m}G/I$ is torsion-free. But since $\mathfrak{m}$ is good, this latter group is free over $\mathbb{T}_\mathfrak{m}/I$, which is torsion-free by virtue of our assumption on I. □

Corollary 2.5. *Let I be a saturated ideal of $\mathbb{T}$, and write $H = G[I]$.*

(i) If $\mathfrak{m}$ is a good maximal ideal of $\mathbb{T}$ then the natural map $H^0[\mathfrak{m}^\infty] \to G[\mathfrak{m}^\infty, I]$ is an isomorphism. Equivalently, the natural map $T_\mathfrak{m}H \to T_\mathfrak{m}H^0$ is an isomorphism.

(ii) The connected component group H/H^0 is supported at maximal ideals of $\mathbb{T}$ that are not good.

Proof. Both claims follows immediately from lemmas 2.1 and 2.4. □

The preceding corollary will be our basic tool in this paper. We now apply it to prove some additional results involving good maximal ideals, which will be used in what is to come.

Lemma 2.6. *Let $\mathfrak{m}$ be a good maximal ideal in $\mathbb{T}$, let I be a saturated ideal of $\mathbb{T}$, let $\mathcal{I}$ be an ideal of finite index in $\mathbb{T}$, and suppose that $\mathcal{I}\mathbb{T}_\mathfrak{m}$ is a principal ideal in $\mathbb{T}_\mathfrak{m}$. If we write $H = G[I]$, then the sequence*

$$0 \to H^0[\mathcal{I}]_\mathfrak{m} \to G[\mathcal{I}]_\mathfrak{m} \to (G/H^0)[\mathcal{I}]_\mathfrak{m} \to 0$$

is short exact. (The subscript $\mathfrak{m}$ denotes $\mathfrak{m}$-adic completion.)

Proof. Since $\mathcal{I}$ has finite index in $\mathbb{T}$, the group $G[\mathcal{I}]$ is finite. Thus $G[\mathcal{I}]_\mathfrak{m} = G[\mathfrak{m}^\infty, \mathcal{I}]$. A similar remark holds with H^0 and G/H^0 in place of G. Thus we must show that the sequence

$$0 \to H^0[\mathfrak{m}^\infty, \mathcal{I}] \to G[\mathfrak{m}^\infty, \mathcal{I}] \to (G/H^0)[\mathfrak{m}^\infty, \mathcal{I}] \to 0$$

is short exact.

Part (i) of corollary 2.5 shows that the map $H^0[\mathfrak{m}^\infty] \to H[\mathfrak{m}^\infty]$ is an isomorphism, and hence that $(G/H^0)[\mathfrak{m}^\infty] \to (G/H)[\mathfrak{m}^\infty]$ is an isomorphism. Thus it suffices to prove that

$$0 \to H[\mathfrak{m}^\infty, \mathcal{I}] \to G[\mathfrak{m}^\infty, \mathcal{I}] \to (G/H)[\mathfrak{m}^\infty, \mathcal{I}] \to 0$$

is short exact. This sequence is Pontrjagin dual to the sequence

$$0 \to (IT_\mathfrak{m}G)/\mathcal{I}(IT_\mathfrak{m}G) \to T_\mathfrak{m}G/\mathcal{I}T_\mathfrak{m}G \to T_\mathfrak{m}G/(I+\mathcal{I})T_\mathfrak{m}G \to 0,$$

which is clearly exact on the right. (Here we have applied the remark preceding the statement of lemma 2.4 to the ideal I, so as to identify the Tate modules of G/H and H with $IT_\mathfrak{m}G$ and $T_\mathfrak{m}G/IT_\mathfrak{m}G$ respectively. We have also used the fact that Pontrjagin duality is perfect to conclude that $T_\mathfrak{m}G/\mathcal{I}T_\mathfrak{m}G$ is Pontrjagin dual to $G[\mathfrak{m}^\infty, \mathcal{I}]$, as well as to draw similar conclusions with G/H and H in place of G.) We must show that it is also exact on the left.

Since $\mathfrak{m}$ is good, $T_\mathfrak{m}G$ is free over $\mathbb{T}_\mathfrak{m}$, and so it suffices to show that the map

$$I/\mathcal{I}I \to \mathbb{T}_\mathfrak{m}/\mathcal{I}$$

is injective. This follows from lemma 1.6 □

Lemma 2.7. *Suppose that G is either an abelian variety or a torus. Let $\hat{G}$ denote the dual of G, endowed with the dual $\mathbb{T}$-action. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ for which the completion $\mathbb{T}_\mathfrak{m}$ is Gorenstein. Then $\mathfrak{m}$ is good for G if and only if it is good for $\hat{G}$.*

Proof. Let ℓ denote the residue characteristic of $\mathfrak{m}$. Recall that $\hat{G}[\ell^\infty]$ is naturally isomorphic to the Cartier dual of $G[\ell^\infty]$. Since this isomorphism is natural, it is $\mathbb{T}$-equivariant, and so there is an induced isomorphism between $\hat{G}[\mathfrak{m}^\infty]$ and the Cartier dual of $G[\mathfrak{m}^\infty]$. Thus (if we ignore the implicit $\mathrm{Gal}(\overline{K}/K)$-actions) there is an isomorphism of $\mathbb{T}_\mathfrak{m}$-modules $T_\mathfrak{m}\hat{G} \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\mathfrak{m}G, \mathbb{Z}_\ell)$. Since $\mathbb{T}_\mathfrak{m}$ is a Gorenstein ring, it follows that $T_\mathfrak{m}\hat{G}$ is free over $\mathbb{T}_\mathfrak{m}$ if and only if $T_\mathfrak{m}G$ is free over $\mathbb{T}_\mathfrak{m}$. This proves the lemma. □

Lemma 2.8. *Suppose that G is either an abelian variety or a torus, and that I is an ideal of $\mathbb{T}$. Let $(G/I)\hat{} \to \hat{G}$ be dual to the surjection $G \to G/I$. Then this morphism is injective, and identifies $(G/I)\hat{}$ with $\hat{G}[I]^0$.*

Proof. Dualizing the short exact sequence $0 \to IG \to G \to G/I \to 0$ yields the short exact sequence $0 \to (G/I)\hat{} \to \hat{G} \to (IG)\hat{} \to 0$. (Exactness on the left follows from the fact that IG is connected.) Let $\alpha_1, \ldots, \alpha_r$ be generators for I. Write $G' = \prod_{i=1}^r G$. Dualizing the surjection $G' \to IG$ defined by $(g_1, \ldots, g_r) \mapsto \alpha_1 g_1 + \cdots + \alpha_r g_r$ yields a morphism $(IG)\hat{} \to \hat{G}' = \prod_{i=1}^r \hat{G}$, whose kernel is a finite subgroup of $(IG)\hat{}$. Composing this injection with the preceding short exact sequence yields the sequence

$$0 \to (G/I)\hat{} \to \hat{G} \to \hat{G}',$$

which is exact on the left, and exact in the middle up to finite index. The right-hand arrow is given by $\hat{g} \mapsto (\alpha_1\hat{g}, \ldots, \alpha_r\hat{g})$, and so its kernel is equal to $\hat{G}[I]$. Thus we find that $(G/I)\hat{}$ is contained in $\hat{G}[I]$ with finite index. Since it is connected, the lemma follows. $\square$

By abuse of terminology, we say that a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ is *monogenic* if the completion $\mathbb{T}_{\mathfrak{m}}$ is monogenic as a $\mathbb{Z}_\ell$-algebra (where ℓ is the residue characteristic of $\mathfrak{m}$).

Lemma 2.9. *Let $\mathfrak{m}$ be a good maximal ideal of $\mathbb{T}$, and let $I \subset \mathfrak{m}$ be a saturated ideal of $\mathbb{T}$. Let $\mathfrak{m}'$ denote the image of $\mathfrak{m}$ in $\mathbb{T}/I$. Note that the ring $\mathbb{T}/I$ acts on each of $G[I]$ and G/I.*

(i) The maximal ideal $\mathfrak{m}'$ is good with respect to $G[I]^0$.

(ii) Suppose that G is either an abelian variety or a torus. If $\mathfrak{m}$ is monogenic, then $\mathfrak{m}'$ is also monogenic, and is good with respect to G/I.

Proof. The proof of lemma 2.4 shows that $T_{\mathfrak{m}'}G[I] = T_{\mathfrak{m}}G/I$. Thus if $T_{\mathfrak{m}}G$ is free over $\mathbb{T}_{\mathfrak{m}}$, we see that $T_{\mathfrak{m}'}G[I]$ is free over $(\mathbb{T}/I)_{\mathfrak{m}'} = \mathbb{T}_{\mathfrak{m}}/I$. Also, part (i) of corollary 2.5 shows that the map $T_{\mathfrak{m}'}G[I] \to T_{\mathfrak{m}'}G[I]^0$ is an isomorphism. This proves part (i).

We now turn to proving part (ii). Since $(\mathbb{T}/I)_{\mathfrak{m}'} = \mathbb{T}_{\mathfrak{m}}/I$, the fact that $\mathfrak{m}$ is monogenic immediately implies the same for $\mathfrak{m}'$. Both $\mathbb{T}$ and $\mathbb{T}/I$ are torsion-free by assumption. Thus both $\mathbb{T}_{\mathfrak{m}}$ and $(\mathbb{T}/I)_{\mathfrak{m}'}$ are Gorenstein $\mathbb{Z}_\ell$-algebras. Lemma 2.7 now shows that $\mathfrak{m}$ is good for $\hat{G}$, and that to prove that $\mathfrak{m}'$ is good for G/I, it suffices to prove that it is good for $(G/I)\hat{}$.

The surjection $G \to G/I$ has connected kernel, and so dualizing leads to an injection $(G/I)\hat{} \to \hat{G}$. Lemma 2.8 shows that this embedding identifies $(G/I)\hat{}$ with $\hat{G}[I]^0$, and it follows from part (i) that $\mathfrak{m}'$ is good for $\hat{G}[I]^0$. This proves part (ii) of the lemma. $\square$

We record the following result for later use.

Lemma 2.10. *If G is connected, then $\mathrm{Ann}_{\mathbb{T}}(G)$ is a saturated ideal of $\mathbb{T}$.*

Proof. Let $T \in \mathbb{T}$ and $n \in \mathbb{Z}$ such that nT annihilates G. Then T annihilates nG. Since G is connected, $nG = G$. This proves the lemma. $\square$

We finish this section by proving an abstract version of theorem A. We begin by describing the necessary set-up. To begin with, suppose that I_1 and I_2 are two saturated ideals of $\mathbb{T}$, and that the natural map $\mathbb{T} \to \mathbb{T}/I_1 \oplus \mathbb{T}/I_2$ is injective, with finite-order cokernel.

Lemma 2.11. *Suppose that G is connected. Then $I_1G = G[I_2]^0$.*

Proof. The assumptions on I_1 and I_2 imply that $I_1I_2 \subset I_1 \cap I_2 = 0$. Thus $I_1G \subset G[I_2]$. Since G is connected, I_1G is also connected, and so in fact $I_1G \subset G[I_2]^0$. To see the converse, note that the assumptions on I_1 and I_2 imply that $I_1 + I_2$ has finite index in $\mathbb{T}$, and so we may choose $n \in \mathbb{Z}$ such that $n\mathbb{T} \subset I_1 + I_2$. Since $G[I_2]^0$ is connected, we find that

$$G[I_2]^0 = nG[I_2]^0 \subset (I_1 + I_2)G[I_2]^0 = I_1G[I_2]^0 \subset I_1G.$$

This establishes the lemma. $\square$

Now suppose in addition that G is either an abelian variety or a torus, and that there is a $\mathbb{T}$-equivariant isomorphism $\phi : \hat{G} \to G$. By lemma 2.8, the surjection $G \to G/I_1$ gives rise to an embedding $(G/I_1)\hat{} \to \hat{G}$. We let ϕ' denote the composite

$$(G/I_1)\hat{} \to \hat{G} \xrightarrow{\phi} G \to G/I_1.$$

Lemma 2.12. *In the preceding situation, the restriction of* ϕ *to* $\ker(\phi')$ *embeds* $\ker(\phi')$ *into* $G[I_1 + I_2]$. *The cokernel of this embedding is supported away from the good maximal ideals of* $\mathbb{T}$.

Proof. Lemma 2.11 shows that $I_1 G = G[I_2]^0$, and so $\phi^{-1} : G \to \hat{G}$ identifies $I_1 G$ with $\hat{G}[I_2]^0$. Also, lemma 2.8 shows that $(G/I_1)\hat{} \xrightarrow{\sim} \hat{G}[I_1]^0$, and hence

$$\ker(\phi') = \hat{G}[I_1]^0 \cap \hat{G}[I_2]^0 \subset \hat{G}[I_1] \cap \hat{G}[I_2] = \hat{G}[I_1 + I_2].$$

It follows immediately that ϕ embeds $\ker(\phi')$ into $G[I_1 + I_2]$. The assumptions on I_1 and I_2, together with part (ii) of corollary 2.5, imply that the inclusion of $\hat{G}[I_1]^0 \cap \hat{G}[I_2]^0$ into $\hat{G}[I_1] \cap \hat{G}[I_2]$ becomes an equality after localizing at any good maximal ideal of $\mathbb{T}$. Thus the cokernel of the embedding of $\ker(\phi')$ into $G[I_1 + I_2]$ is supported away from the good maximal ideals of $\mathbb{T}$. □

3. Abelian varieties with semi-abelian reduction

In this section we assume that the field K is complete with respect to a discrete valuation, and has a perfect residue field. If A is an abelian variety over K having semi-abelian reduction, in the sense that the connected component of the special fibre of its Néron model over the ring of integers of K is an extension of an abelian variety by a torus, then A has a uniformization in the category of rigid analytic spaces over K. This consists of a short exact sequence

$$0 \to \Gamma_A \to G_A \to A \to 0,$$

in which Γ_A is a finite rank free $\mathbb{Z}$-module equipped with a continuous $\mathrm{Gal}(\overline{K}/K)$-action, G_A is a semi-abelian variety, and the maximal abelian variety quotient of G_A is isomorphic to the maximal quotient of A having good reduction (see [5, §§7, 14] and [9]). The formation of Γ_A and G_A is functorial in the category of abelian varieties A having semi-abelian reduction. (To be precise, if $B \to A$ is a morphism of abelian varieties over K having semi-abelian reduction, then there is induced functorially an *algebraic* morphism $G_B \to G_A$ of semi-abelian varieties over K, which restricts to a morphism $\Gamma_B \to \Gamma_A$.) Furthermore, Γ_A is canonically isomorphic (as a $\mathrm{Gal}(\overline{K}/K)$-module) to the character lattice of the toric part of the special fibre of the Néron model of the dual abelian variety to A. (In particular, the Galois action on Γ_A is unramified.)

In fact, it will do no harm to recall in a little more detail the construction of this uniformization. Thus we suppose that A is an abelian variety over K having semi-abelian reduction, and we let $\mathcal{A}$ denote the Néron model of A over the ring of integers $\mathcal{O}_K$ of K; then $\mathcal{A}$ is a finite type smooth commutative group scheme over $\mathcal{O}_K$, whose generic fibre is naturally isomorphic to A, and whose special fibre $\mathcal{A}_s$ is an extension of a finite étale group scheme Φ_A (which can alternatively be regarded as an unramified Galois module over K) by a semi-abelian variety $\mathcal{A}_s^0$. We let $\mathcal{A}^0$

denote the complement in $\mathcal{A}$ of the non-identity connected components of $\mathcal{A}_s$; it is an open subgroup scheme of $\mathcal{A}$.

The semi-abelian variety G_A is defined to be the generic fibre of the formal completion of $\mathcal{A}^0$ along its special fibre $\mathcal{A}^0_s$. Although the generic fibre of a formal scheme over $\mathcal{O}_K$ is in general defined only as a rigid analytic variety, the formal scheme that we are considering can be algebraized in a natural way, and so G_A is in fact a semi-abelian variety over K. For details, see the discussion of [5, §§7.1, 7.2], where (due to apparent notational inconsistency) the algebraization of the formal completion of $\mathcal{A}^0$ along its special fibre is denoted alternately by $A^\natural$ and $G^\natural$.

The natural isomorphism $\mathcal{A}^0_{/K} \xrightarrow{\sim} A$ induces a rigid analytic map $G_A \to A$, and it is this map that provides the uniformization of A. One shows that this map is surjective, and that the kernel Γ_A of this map is naturally isomorphic to the character lattice of the torus part of the special fibre of $\hat{\mathcal{A}}$, where $\hat{\mathcal{A}}$ denotes the Néron model of the abelian variety $\hat{A}$ dual to A. (See the discussion of [5, §14].)

That a map $A \to B$ between abelian varieties with semi-abelian reduction induces an algebraic map (i.e. a map in the category of K-schemes, not just in the category of K-rigid analytic spaces) $G_A \to G_B$ follows from [5, lem. 7.2.1]. To be precise, the functoriality of the construction of Néron models shows that we obtain a morphism $\mathcal{A} \to \mathcal{B}$ of Néron models, which in turn induces a morphism of the formal completions of these $\mathcal{O}_K$-schemes along their special fibres. The preceding reference then shows that, since these formal completions can be algebraized, the same is true of this morphism.

The following lemma recalls the exactness properties of the formation of Γ_A and G_A.

Lemma 3.1. *Let $B \to A$ be a morphism of abelian varieties over K, both having semi-abelian reduction.*

(i) If $B \to A$ is injective, then the same is true of the morphisms $\Gamma_B \to \Gamma_A$ and $G_B \to G_A$.

(ii) If $B \to A$ is surjective, then the same is true of the morphism $G_B \to G_A$.

(iii) If the morphism $B \to A$ is surjective, and has a connected kernel, then the maps $G_B \to G_A$ and $\Gamma_B \to \Gamma_A$ are both surjective.

Proof. Functoriality of uniformization yields a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma_B & \longrightarrow & G_B & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Gamma_A & \longrightarrow & G_A & \longrightarrow & A & \longrightarrow & 0, \end{array}$$

with exact rows. Applying the snake lemma, we obtain an exact sequence

$$0 \to \ker(\Gamma_B \to \Gamma_A) \to \ker(G_B \to G_A) \to \ker(B \to A) \\ \to \operatorname{coker}(\Gamma_B \to \Gamma_A) \to \operatorname{coker}(G_B \to G_A) \to \operatorname{coker}(B \to A) \to 0.$$

If $B \to A$ is injective, then we obtain an isomorphism $\ker(\Gamma_B \to \Gamma_A) \xrightarrow{\sim} \ker(G_B \to G_A)$. The source of this isomorphism is a free $\mathbb{Z}$-module of finite rank, while the target is the kernel of an algebraic morphism between semi-abelian varieties. It follows that both source and target vanish, and so we have proved (i).

If $B \to A$ is surjective, then we find that the map

$$\operatorname{coker}(\Gamma_B \to \Gamma_A) \to \operatorname{coker}(G_B \to G_A)$$

is a surjection from a finitely generated abelian group onto the connected group scheme $\operatorname{coker}(G_B \to G_A)$. Thus this cokernel vanishes, and so we have proved (ii). If furthermore $\ker(B \to A)$ is connected, then we find that $\ker(B \to A) \to \operatorname{coker}(\Gamma_B \to \Gamma_A)$ is a surjection from a connected group scheme onto a finitely generated abelian group, and hence that $\operatorname{coker}(\Gamma_B \to \Gamma_A)$ also vanishes, proving (iii). □

If $0 \to C \to B \to A$ is an exact sequence of abelian varieties, then uniformizing B and A yields a commutative diagram in which all rows and columns are short exact:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Gamma'_C & \longrightarrow & G'_C & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Gamma_B & \longrightarrow & G_B & \longrightarrow & B & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Gamma_A & \longrightarrow & G_A & \longrightarrow & A & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & .
\end{array}$$

(The top row is defined so as to make the columns exact; we are also taking into account part (iii) of the preceding lemma.)

The top row of this diagram need not necessarily be the rigid-analytic uniformization of C, since the algebraic group G'_C need not be connected. The following lemma clarifies the situation.

Lemma 3.2. *There is a canonical identification of G_C (the semi-abelian variety that uniformizes C) with $(G'_C)^0$ (the connected component of the identity in G'_C), with respect to which Γ_C is identified with the intersection $\Gamma'_C \cap (G'_C)^0$. Furthermore, the induced map $\Gamma'_C/\Gamma_C \to G'_C/G_C$ is an isomorphism.*

Proof. The group G'_C appearing in the preceding diagram is the kernel of the map of semi-abelian varieties $G_B \to G_A$, and so is an algebraic group, of dimension equal to the difference of the dimensions of G_B and G_A, which is the difference of the dimensions of B and A, which is the dimension of C. By functoriality of uniformizations, and taking into account part (i) of lemma 3.1, the injection $C \to B$ induces an injection $G_C \to G_B$. Since the image of G_C in G_B certainly maps to zero in G_A, the image of G_C lies in G'_C; in fact, since G_C is connected, it lies in $(G'_C)^0$. Since G_C and $(G'_C)^0$ have the same dimension, the image of G_C must equal $(G'_C)^0$. This proves the first statement of the lemma. The rest of the lemma follows from a consideration of the diagram

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Gamma_C & \longrightarrow & G_C & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \Gamma'_C & \longrightarrow & G'_C & \longrightarrow & C & \longrightarrow & 0, \end{array}$$

whose rows and columns are exact. □

We may dualize our exact sequence of abelian varieties to obtain the exact sequence of dual abelian varieties $0 \to \hat{A} \to \hat{B} \to \hat{C} \to 0$, and a diagram

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Gamma'_{\hat{A}} & \longrightarrow & G'_{\hat{A}} & \longrightarrow & \hat{A} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Gamma_{\hat{B}} & \longrightarrow & G_{\hat{B}} & \longrightarrow & \hat{B} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Gamma_{\hat{C}} & \longrightarrow & G_{\hat{C}} & \longrightarrow & \hat{C} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & . \end{array}$$

Lemma 3.2 applies equally well in this situation, to yield isomorphisms $G_{\hat{A}} \xrightarrow{\sim} (G'_{\hat{A}})^0$ and $\Gamma'_{\hat{A}}/\Gamma'_{\hat{A}} \xrightarrow{\sim} G'_{\hat{A}}/(G_{\hat{A}})$.

The description of the kernel of the monodromy pairing [5, §9] provided by [5, thm. 11.5] yields a short exact sequence of complexes (the complexes are in the vertical direction; the exact sequence is in the horizontal direction)

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Gamma_C & \longrightarrow & \mathrm{Hom}(\Gamma_{\hat{C}}, \mathbb{Z}) & \longrightarrow & \Phi_C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Gamma_B & \longrightarrow & \mathrm{Hom}(\Gamma_{\hat{B}}, \mathbb{Z}) & \longrightarrow & \Phi_B & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Gamma_A & \longrightarrow & \mathrm{Hom}(\Gamma_{\hat{A}}, \mathbb{Z}) & \longrightarrow & \Phi_A & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & . \end{array}$$

Taking the associated long exact sequence of cohomology, and using the preceding diagrams, we obtain the exact sequence

$$0 \to \ker(\Phi_C \to \Phi_B) \to \Gamma'_C/\Gamma_C \to 0 \to \ker(\Phi_B \to \Phi_A)/\operatorname{im}(\Phi_C \to \Phi_B)$$
$$\to 0 \to \operatorname{Ext}^1(\Gamma'_{\hat{A}}/\Gamma_{\hat{A}}, \mathbb{Z}) \to \operatorname{coker}(\Phi_B \to \Phi_A) \to 0.$$

Recall the isomorphisms $\Gamma'_C/\Gamma_C \xrightarrow{\sim} G'_C/G_C$ and $\Gamma'_{\hat{A}}/\Gamma_{\hat{A}} \xrightarrow{\sim} G'_{\hat{A}}/G_{\hat{A}}$ of lemma 3.2. Also recall that if M is any finite group, then there is an isomorphism

$$\operatorname{Ext}^1(M, \mathbb{Z}) \xrightarrow{\sim} \operatorname{Hom}(M, \mathbb{Q}/\mathbb{Z}) = M^*.$$

Using these isomorphisms, we may reorganize the information contained in the preceding exact sequence to obtain the exact sequence

$$0 \to G'_C/G_C \to \Phi_C \to \Phi_B \to \Phi_A \to (G'_{\hat{A}}/G_{\hat{A}})^* \to 0. \tag{3.3}$$

(This exact sequence is a generalization of [16, prop. 2], which treats the case when B is the Jacobian of a Shimura curve of square-free level, and A is an elliptic curve that is an optimal quotient of B.)

The remainder of this section is devoted to applying the preceding discussion in the context of section 2. From now on we suppose that $\mathbb{T}$ is a finite flat commutative $\mathbb{Z}$-algebra that acts on B, that I_1 and I_2 are saturated ideals in $\mathbb{T}$ for which the morphism $\mathbb{T} \to \mathbb{T}/I_1 \oplus \mathbb{T}/I_2$ is injective with finite-order cokernel, that $C = I_1 B$, and that $A = B/I_1$.

The functoriality of the constructions of this section imply that $\mathbb{T}$ acts naturally on G_B, Γ_B, Φ_B, and similarly with B replaced by any of A, C, $\hat{A}$, $\hat{B}$, or $\hat{C}$. The ring $\mathbb{T}$ also acts naturally on G'_C and $G'_{\hat{A}}$, and all morphisms appearing in the diagrams of the preceding discussion are $\mathbb{T}$-equivariant. In particular, $\mathbb{T}$ acts on all the objects appearing in the exact sequence (3.3), and all the morphisms of this exact sequence are $\mathbb{T}$-equivariant.

Lemma 3.4. *We have the following sequences of equalities and inclusions:*

$$G_C = (G'_C)^0 = I_1 G_B = G_B[I_2]^0 \subset G'_C \subset G_B[I_2],$$

and

$$G_{\hat{A}} = (G'_{\hat{A}})^0 = I_2 G_{\hat{B}} = G_{\hat{B}}[I_1]^0 \subset G'_{\hat{A}} \subset G_{\hat{B}}[I_1].$$

Proof. Since I_1 annihilates A, it also annihilates G_A, and so $I_1 G_B \subset G'_C$. Since $I_1 G_B$ is connected, in fact $I_1 G_B \subset (G'_C)^0$. The assumptions on I_1 and I_2, together with lemma 2.11, imply that $I_1 G_B = G_B[I_2]^0$, and lemma 3.2 implies that $G_C = (G'_C)^0$. Combining all these observations, we obtain the sequence of inclusions and equalities $I_1 G_B = G_B[I_2]^0 \subset G_C = (G'_C)^0 \subset G'_C$.

Again by lemma 2.11, we see that $C = I_1 B$ is also equal to $B[I_2]^0$. Since I_2 annihilates C, we see that $I_2 G'_C \subset \Gamma'_C$. Now $I_2 G'_C$ is an algebraic group, while Γ'_C is a lattice. Thus $I_2 G'_C = 0$, and we deduce that $G'_C \subset G_B[I_2]$. Passing to connected components, we also find that $G_C = (G'_C)^0 \subset G_B[I_2]^0$. Combining these two inclusions with the result of the preceding paragraph proves the first claim of the lemma. The second claim follows from the first, once one notes that lemmas 2.8 and 2.11 imply that $\hat{A} = I_2 \hat{B}$, and hence that $\hat{C} = \hat{B}/I_2$. □

Corollary 3.5. *The kernel of the map $\Phi_C \to \Phi_B$ is a subobject of the $\mathbb{T}$-module $G_B[I_2]/G_B[I_2]^0$, while the cokernel of the map $\Phi_B \to \Phi_A$ is a quotient of the $\mathbb{T}$-module $(G_{\hat{B}}[I_1]/G_{\hat{B}}[I_1]^0)^*$.*

Proof. Lemma 3.4 shows that there is an injection $G'_C/G_C \to G_B[I_2]/G_B[I_2]^0$. The first claim of lemma now follows, since the exact sequence (3.3) identifies G'_C/G_C with the kernel of the map $\Phi_C \to \Phi_B$. The second claim of the lemma is proved similarly. □

Corollary 3.6. *Suppose that $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ that is good for both G_B and $G_{\hat{B}}$. Then the sequence*

$$0 \to (\Phi_C)_{\mathfrak{m}} \to (\Phi_B)_{\mathfrak{m}} \to (\Phi_A)_{\mathfrak{m}} \to 0$$

is short exact. (Here the subscript $\mathfrak{m}$ denotes $\mathfrak{m}$-adic completion, of course.)

Proof. This follows immediately from the exact sequence (3.3), and corollaries 3.5 and 2.5. □

We conclude this section with an analogue of lemma 2.9.

Lemma 3.7. *Suppose that G_B is a torus, that $\mathfrak{m}$ is good for G_B, and that $\mathfrak{m}$ is monogenic. Let $\mathfrak{m}_i$ denote the image of $\mathfrak{m}$ in $\mathbb{T}/I_i$ (for $i = 1, 2$). Then $\mathfrak{m}_1$ (respectively $\mathfrak{m}_2$) is monogenic, and good for G_A (respectively G_C).*

Proof. By lemma 3.4, $G_C = G_B[I_2]^0$. This equality, together with part (i) of lemma 2.9, implies that $\mathfrak{m}_2$ is good for G_C.

To show that $\mathfrak{m}_1$ is good for G_A, note that again by lemma 3.4, $I_1 G_B = G_B[I_2]^0 \subset G'_C \subset G_B[I_2]$. Thus there is a surjection $G_B/I_1 \to G_B/G'_C = G_A$, whose kernel $G'_C/I_1 G_B$ is a subgroup of the connected component group $G_B[I_2]/G_B[I_2]^0$. Since $\mathfrak{m}$ is good for G_B, part (ii) of corollary 2.5 shows that this group is supported away from $\mathfrak{m}$, and so the surjection $G_B/I_1 \to G_A$ induces an isomorphism on $\mathfrak{m}$-adic Tate modules. Thus it suffices to show that $\mathfrak{m}_1$ is good for G_B/I_1. This follows from part (ii) of lemma 2.9, and completes the proof of the lemma. □

4. Applications to optimal quotients

In this section, we present the proofs of the two theorems stated in the introduction. We will see that theorem A is a quite straightforward consequence of the results of section 2. While theorem B also follows from these results (as augmented by the discussion of section 3), the process of deducing it from them is slightly more involved.

As in the introduction, we let N be a positive integer, $S(N)$ the space of weight two cuspforms on $\Gamma_0(N)$, and $\mathbb{T}$ the Hecke algebra acting on $S(N)$.

Lemma 4.1. *Let f be a normalized newform in $S(N)$, let I_f denote the annihilator of f in $\mathbb{T}$, let S_f denote the subspace of $S(N)$ spanned by all the algebraic conjugates of f, and let $S_f^\perp$ denote the orthogonal complement with respect to the Petersson inner product of S_f in $S(N)$. As usual, write $I_f^\perp = \mathrm{Ann}_{\mathbb{T}}(I_f)$.*

(i) $I_f^\perp$ is the annihilator of $S_f^\perp$ in $\mathbb{T}$.

(ii) The map $\mathbb{T} \to \mathbb{T}/I_f \oplus \mathbb{T}/I_f^\perp$ is injective and its cokernel has finite order.

Proof. The finite dimensional $\mathbb{Q}$-algebra $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ decomposes as a product of Artin local $\mathbb{Q}$-algebras $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q} = \prod_{i=1}^d A_i$, which are in bijection with the normalized eigenforms in $S(N)$. In particular, the newform f corresponds to one of these factors, say A_1. Since f is a newform, A_1 is a field, and so $I_f \otimes_{\mathbb{Z}} \mathbb{Q} = \prod_{i=2}^{d} A_i$, and $I_f^{\perp} \otimes \mathbb{Q} = A_1$. In particular, the map $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q} \to (\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q})/(I_f \otimes_{\mathbb{Z}} \mathbb{Q}) \oplus (\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q})/(I_f^{\perp} \otimes_{\mathbb{Z}} \mathbb{Q})$ is an isomorphism. Part (ii) follows from this.

The decomposition of $\mathbb{T}$ into a product gives rise to a decomposition $S(N) = \prod_{i=1}^{d} S_i$ of the $\mathbb{T}$-module $S(N)$. Each S_i is a faithful $A_i \otimes_{\mathbb{Q}} \mathbb{C}$-module, whose dimension over $\mathbb{C}$ is equal to the dimension of A_i over $\mathbb{Q}$. (In fact, S_i is canonically isomorphic as an A_i-module to $\mathrm{Hom}_{\mathbb{Q}}(A_i, \mathbb{C})$ [11, thm. 2.2].) Now $S_f = S_1$, while $S_f^{\perp} = \prod_{i=2}^{d} S_i$. Thus $\mathrm{Ann}_{T\otimes\mathbb{Q}}(S_f^{\perp}) = A_1 = I_f^{\perp} \otimes_{\mathbb{Z}} \mathbb{Q}$. This implies part (i). □

Note that part (i) of this lemma reconciles our use of the $\perp$ notation in the introduction with its use in the main body of the paper.

Proof of theorem A. We will deduce theorem A from lemma 2.12. One of the complications in doing this is that the natural principal polarization $\theta : J_0(N)^{\vee} \xrightarrow{\sim} J_0(N)$ of $J_0(N)$ does not respect the action of $\mathbb{T}$ on $J_0(N)$. For this reason, we have to pay (routine, but) close attention to questions of variance in the course of the proof.

As we stated in the introduction, the action of the correspondences $T \in \mathbb{T}$ on $J_0(N)$ that we are considering is that induced via Picard functoriality. This induces a dual action of $\mathbb{T}$ on $J_0(N)^{\vee}$. If $T \in \mathbb{T}$ we let $T^{\dagger}$ denote the endomorphism of $J_0(N)$ defined by $\theta \circ T \circ \theta^{-1}$. (Thus † denotes the Rosati involution.) As discussed in [12, pp. 443-444], the endomorphism $T^{\dagger}$ is the endomorphism of $J_0(N)$ obtained from the correspondence T via Albanese functoriality, and in general T and $T^{\dagger}$ are not the same endomorphism. However, it is pointed out in [12, p. 444, eqns. (3), (4)] that one has the equality $T^{\dagger} = w_N T w_N$, where w_N is the Atkin-Lehner involution of $J_0(N)$. Thus if we write $\phi = w_N \circ \theta : J_0(N)^{\vee} \to J_0(N)$, then ϕ is $\mathbb{T}$-equivariant. Note that since w_N (as an automorphism of $J_0(N)$) is induced by an involution of the curve $X_0(N)$, it is fixed by the Rosati involution. (By functoriality of the formation of the theta divisor, and hence of the polarisation θ, the involution w_N commutes with the principal polarization θ.) Thus we may equally well write $\phi = \theta \circ w_N$.

A useful observation will be that there is an isomorphism of $S(N)$ (with its usual Hecke action) with the tangent space at the origin of $J_0(N)$ (equipped with the Hecke action induced by the Hecke action on $J_0(N)$ defined by Picard functoriality). To see this, note that $S(N)$ equipped with its usual Hecke action is naturally isomorphic to the cotangent space at the origin of $J_0(N)$, equipped with the Hecke action induced by Albanese functoriality [12, p. 444]. Thus if $T \in \mathbb{T}$ acts on $J_0(N)$ via Picard functoriality, the action that it induces on $S(N)$ is equal to the usual action of $T^{\dagger} = w_N T w_N$ on $S(N)$. We may use the Petersson inner product to identify $\overline{S(N)}$ with the dual to $S(N)$, and thus with the tangent space at the origin of $J_0(N)$. (Here $\overline{S(N)}$ denotes the complex conjugate vector space to $S(N)$.) With respect to this inner product, the actions of T and $T^{\dagger}$ on $S(N)$ are adjoint to one another. Thus we obtain an identification of $\overline{S(N)}$ with the tangent space at the origin of $J_0(N)$ equipped with the Hecke action induced by Picard functoriality. The subspace of $S(N)$ consisting of cuspforms with real Fourier coefficients endows $S(N)$ with a $\mathbb{T}$-invariant real structure, which in turn yields a $\mathbb{T}$-equivariant isomorphism of $S(N)$ with $\overline{S(N)}$. Composing this with the preceding identification yields a $\mathbb{T}$-equivariant isomorphism of $S(N)$ with the tangent space of $J_0(N)$ equipped with the Hecke action induced by Picard functoriality.

Now let f be a newform in $S(N)$, corresponding to the ideal I_f in $\mathbb{T}$. Note that by part (ii) of lemma 4.1, the ideals I_f and $I_f^{\perp}$ satisfy the hypotheses of lemma 2.12. Thus, if we let $\phi' : \hat{A}_f \to A_f$ be the polarization of $\hat{A}_f$ induced by the principal polarization ϕ of $J_0(N)$, we deduce from lemma 2.12 that ϕ embeds $\ker \phi'$ into $J_0(N)[I_f + I_f^{\perp}] = J_0(N)[\mathfrak{F}_f]$, with cokernel supported away from the good maximal ideals of $\mathbb{T}$.

To complete the proof of theorem A, it suffices to prove the following two claims. First, that each of $I_f J_0(N) \subset J_0(N)$ and $\hat{A}_f \subset J_0(N)\hat{}$ is invariant under w_N, so that $\phi(\ker(\phi')) = \theta(\ker(\theta_A))$. Second, that if $\mathfrak{m}$ satisfies multiplicity one, then it is good for $J_0(N)$.

One may regard the exact sequence of abelian varieties

$$0 \to I_f J_0(N) \to J_0(N) \to A_f \to 0$$

as arising by applying the exponential map to the exact sequence of tangent spaces

$$0 \to S_f^{\perp} \to S(N) \to S_f \to 0.$$

It follows from the results of [1] and the fact that f is a newform that each of S_f and $S_f^{\perp}$ is invariant under the action of w_N. As a consequence, we deduce that w_N restricts to an automorphism of $I_f J_0(N)$. Dualizing, we observe that w_N restricts to an involution of $\hat{A}_f$. This proves the first of the above claims.

To prove the second of the above claims, it suffices to show that the $\mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Q}$-module $T_{\mathfrak{m}} J_0(N) \otimes_{\mathbb{Z}} \mathbb{Q}$ is free of rank two. For this implies that if $\mathfrak{m}$ satisfies multiplicity one, then $T_{\mathfrak{m}} J_0(N)$ is free of rank two over $\mathbb{T}_{\mathfrak{m}}$, and so in particular, that $\mathfrak{m}$ is good for $J_0(N)$. To see the required fact about $\mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Q}$, note that this $\mathbb{T}$-module is isomorphic to the $\mathfrak{m}$-adic component of the cohomology space $\mathrm{H}^1(J_0(N), \mathbb{Q}_\ell)$ (where ℓ is the residue characteristic of $\mathfrak{m}$). (Recall that our Tate-modules are defined to be contravariant.) Thus it suffices to show that this cohomology space is free of rank two over $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. To verify this statement, we may replace $\mathbb{Q}_\ell$ by any other field of characteristic zero, for example $\mathbb{R}$. We will show that $\mathrm{H}^1(J_0(N), \mathbb{R})$ is free of rank two over $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{R}$.

There is a natural isomorphism of $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{R}$-modules between the tangent space at the origin of $J_0(N)$ and the first homology space $\mathrm{H}_1(J_0(N), \mathbb{R})$. Since this tangent space is isomorphic to $S(N)$, we see that $S(N)$ and $H^1(J_0(N), \mathbb{R})$ are naturally dual as $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{R}$-modules. As already observed in the proof of lemma 4.1, [11, thm. 2.2] implies that $S(N)$ is naturally isomorphic to $\mathrm{Hom}(\mathbb{T}, \mathbb{C})$, and thus we see that $H^1(J_0(N), \mathbb{R})$ is isomorphic to $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{C}$ as a $\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{R}$-module. In particular, it is free of rank two, which is what we intended to show. □

As already mentioned, the proof of theorem B is more involved. We begin by recalling some additional terminology concerning maximal ideals of the Hecke ring. For any prime p, we say that a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ is *p-finite* if the representation $\rho_{\mathfrak{m}}$ is *finite at p* [17, p. 189]. We say that a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ is *Eisenstein* if $\rho_{\mathfrak{m}}$ is reducible.

We now prove a result that controls the support of the connected component groups of special fibres of Néron models of certain $\mathbb{T}$-equivariant subquotients of $J_0(N)$. It is a minor variation on the argument of [19, §4].

Proposition 4.2. *Let N be a positive integer, and let A be a subquotient of $J_0(N)$ in the category of abelian varieties over $\mathbb{Q}$ with $\mathbb{T}$-action. Suppose that A has semi-abelian reduction at a prime p, and let Φ_A denote the $\mathbb{T}$-module of connected components of the characteristic p fibre of the Néron model of A. Then Φ_A is supported on the union of the p-finite and Eisenstein locus of $\mathbb{T}$.*

Proof. Consider the p-adic rigid analytic uniformization $0 \to \Gamma_A \to G_A \to A \to 0$ of A. If ℓ is a prime, then applying $\mathrm{Hom}(\mathbb{Z}/\ell, –)$ to this short exact sequence yields the short exact sequence of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules

$$0 \to G_A[\ell] \to A[\ell] \to (\Gamma_A/\ell)^* \to 0.$$

(Here we have used the natural isomorphism $\mathrm{Ext}^1(\mathbb{Z}/\ell, \Gamma_A) \xrightarrow{\sim} (\Gamma_A/\ell)^*$.) The $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules $G_A[\ell]$ and $(\Gamma_A/\ell)^*$ appearing at either end of this short exact sequence are finite (not only in cardinality (!), but in the sense of [17, p. 189]).

The asserted finiteness is a standard fact, but (with the encouragement of the referee) we will recall the reasons for it. As in the discussion preceding the statement of lemma 3.1, we let $\mathcal{A}$ denote the Néron model of A over $\mathbb{Z}_p$, and let $\mathcal{A}^0$ denote the "connected component of the identity" in $\mathcal{A}$. We let $\hat{S}$ denote the formal completion of $\mathcal{A}^0$ along its special fibre (so that $\hat{S}$ is a formal semi-abelian scheme). As we observed, the formal scheme $\hat{S}$ may be naturally algebraized, yielding a semi-abelian scheme S over $\mathbb{Z}_p$.

The semi-abelian G_A is defined to be the generic fibre of S. Thus $G_A[\ell]$ is naturally isomorphic to the generic fibre of the group scheme $S[\ell]$ over $\mathbb{Z}_p$. Since S is a semi-abelian scheme over $\mathbb{Z}_p$, its ℓ-torsion subgroup scheme is finite flat over $\mathbb{Z}_p$. Thus $G_A[\ell]$ extends to a finite flat group scheme over $\mathbb{Z}_p$, and so (by definition) is finite. (By Zariski's main theorem, the quasi-finite flat group scheme $\mathcal{A}^0[\ell]$ over $\mathbb{Z}_p$ contains a unique closed subgroup scheme that is finite flat over $\mathbb{Z}_p$, and whose special fibre is equal to $\mathcal{A}^0_s[\ell]$ (see [5, §2.2.3]). The proceeding discussion shows that the natural map $S[\ell] \to \mathcal{A}^0[\ell]$ identifies $S[\ell]$ with this "finite part" of $\mathcal{A}^0[\ell]$.)

To see the finiteness of $(\Gamma_A/\ell)^*$ is easier; one simply recalls that the Galois action on Γ_A, and hence on $(\Gamma_A/\ell)^*$, is even unramified. (Recall that Γ_A is naturally isomorphic to the character lattice of the toric part of the special fibre of the Néron model of $\hat{A}$, the dual abelian variety to A.)

Applying $\mathrm{Hom}(\mathbb{Z}/\ell, –)$ to the exact sequence $0 \to \Gamma_A \to \mathrm{Hom}(\Gamma_{\hat{A}}, \mathbb{Z}) \to \Phi_A \to 0$ provided by [5, thm. 11.5] yields an injection $\Phi_A[\ell] \to (\Gamma_A/\ell)^*$. Pulling back the above short exact sequence by this map yields a morphism of short exact sequences of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_A[\ell] & \longrightarrow & E & \longrightarrow & \Phi_A[\ell] & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & G_A[\ell] & \longrightarrow & A[\ell] & \longrightarrow & (\Gamma_A/\ell)^* & \longrightarrow & 0. \end{array} \tag{4.3}$$

We claim that E is also finite at p.

Just as with $\mathcal{A}^0[\ell]$, Zariski's main theorem guarantees the existence of a unique closed subgroup scheme of $\mathcal{A}[\ell]$ that is finite flat over $\mathbb{Z}_p$, and whose special fibre is equal to $\mathcal{A}_s[\ell]$; we refer to this subgroup scheme as the "finite part" of $\mathcal{A}[\ell]$. We will show that its generic fibre is isomorphic to E.

If T denotes the finite part of $\mathcal{A}[\ell]$, then T contains the finite part of $\mathcal{A}^0[\ell]$, which as we observed above is equal to $S[\ell]$. The quotient $T/S[\ell]$ is a finite flat group scheme over $\mathbb{Z}_p$ whose special fibre is equal to $\Phi_A[\ell]$ (since $\mathcal{A}_s[\ell]$ is an extension of $\mathcal{A}_s^0[\ell]$ by $\Phi_A[\ell]$). Since Φ_A, and hence $\Phi_A[\ell]$, is an étale group scheme over $\mathbb{F}_p$, we see that $T/S[\ell]$ is an étale group scheme over $\mathbb{Z}_p$ (in fact the unique deformation of $\Phi_A[\ell]$ to an étale group scheme over $\mathbb{Z}_p$). Passing to generic fibres, and to the point of view of Galois modules, we find that the generic fibre $T_{/\mathbb{Q}_p}$ of T is an extension of the unramified $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module $\Phi_A[\ell]$ by the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module $G_A[\ell]$.

We claim that the extension class of $T_{/\mathbb{Q}_p}$ in $\mathrm{Ext}^1_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}(\Phi_A[\ell], G_A[\ell])$ is equal to the extension class of E. Indeed, this follows from the very construction (in [5, §11.6]) of the exact sequence of [5, thm. 11.5]. In particular, E is naturally isomorphic to the generic fibre of the finite flat group scheme T over $\mathbb{Z}_p$, and hence is finite.

The diagram (4.3) may be localized at any maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ having residue characteristic ℓ to yield the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_A[\ell]_{\mathfrak{m}} & \longrightarrow & E_{\mathfrak{m}} & \longrightarrow & \Phi_A[\ell]_{\mathfrak{m}} & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & G_A[\ell]_{\mathfrak{m}} & \longrightarrow & A[l]_{\mathfrak{m}} & \longrightarrow & (\Gamma_A/\ell)^*_{\mathfrak{m}} & \longrightarrow & 0. \end{array}$$

Now suppose that $\mathfrak{m}$ is not Eisenstein. Then $A[\ell]_{\mathfrak{m}}$ has a filtration $F^\bullet$ as a $\mathbb{T}_{\mathfrak{m}}/\ell\,[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module whose successive quotients F^i/F^{i+1} are isomorphic to $\rho_{\mathfrak{m}}$ [12, thm. 5.2].

Suppose in addition that $\mathfrak{m}$ is not p-finite. Since $G_A[\ell]_{\mathfrak{m}}$ and $(\Gamma_A/\ell)^*_{\mathfrak{m}}$ are both finite at p, the short exact sequence

$$0 \to (F^i \cap G_A[\ell]_{\mathfrak{m}})/(F^{i+1} \cap G_A[\ell]_{\mathfrak{m}}) \\ \to F^i/F^{i+1} \to F^i/(F^{i+1} + F^i \cap G_A[\ell]_{\mathfrak{m}}) \to 0,$$

which exists for each i, shows that the graded pieces of the filtration induced by $F^\bullet$ on each of these $\mathbb{T}_{\mathfrak{m}}/\ell$-modules are one-dimensional $\mathbb{T}/\mathfrak{m}$-vector spaces. (Note that these graded pieces are precisely the kernel and cokernel in the preceding short exact sequence.) Thus each of these $\mathbb{T}_{\mathfrak{m}}/\ell$-modules is of the same length; that is, they are both of length equal to the length of the filtration $F^\bullet$. Now $E_{\mathfrak{m}}$ is also finite at p, and so the submodule $(F^i \cap E_{\mathfrak{m}})/(F^{i+1} \cap E_{\mathfrak{m}})$ of $F^i/F^{i+1} = \rho_{\mathfrak{m}}$ must again be one dimensional. Thus $E_{\mathfrak{m}}$ is also of length equal to the length of the filtration $F^\bullet$, the inclusion $G_A[\ell]_{\mathfrak{m}} \to E_{\mathfrak{m}}$ must be an isomorphism, and so $\Phi_A[\ell]_{\mathfrak{m}} = 0$. This establishes the proposition. □

We now assume that N is prime. Our first object will be to obtain a correspondence between saturated prime ideals of $\mathbb{T}$ and abelian subvarieties of $J_0(N)$. In order to apply some results of section 1, it will be useful to note that since N is prime, the Hecke algebra $\mathbb{T}$ is reduced.

Proposition 4.4. *If A is an abelian subvariety of $J_0(N)$ then A is defined over $\mathbb{Q}$, and is closed under the action of $\mathbb{T}$ on $J_0(N)$.*

Proof. Let us remark that if A is an abelian subvariety of any abelian variety J, then there is an endomorphism of J whose image is equal to A. (Since the category of abelian varieties up to isogeny is semi-simple, we may find a map $\sigma : J/A \to J$ whose composition with the projection $\pi : J \to J/A$ is multiplication by an integer m on J/A; then $m - \sigma \circ \pi$ is the desired endomorphism.) In our case $J = J_0(N)$, and so [10, prop. 3.1] shows that any endomorphism of $J_0(N)$ is defined over $\mathbb{Q}$, and hence so is its image. This proves that any abelian subvariety A of $J_0(N)$ is defined over $\mathbb{Q}$.

Now define $\mathbb{T}'$ to be the subring of $\mathbb{T}$ generated by the Hecke operators T_n for those n prime to N. Since there are no oldforms in $S(N)$, the subring $\mathbb{T}'$ has finite index in $\mathbb{T}$; let m be a non-zero integer for which $m\mathbb{T} \subset \mathbb{T}'$. From [18, prop. 7.19] we see that A is closed under the action of $\mathbb{T}'$. Since A is connected, $mA = A$, and so $\mathbb{T}A = \mathbb{T}mA \subset \mathbb{T}'A \subset A$. This completes the proof of the proposition. □

If A is an abelian subvariety of $J_0(N)$, we may associate to A the ideal $\mathrm{Ann}_{\mathbb{T}}(A)$, the annihilator in $\mathbb{T}$ of A. Lemma 2.10 shows that this is a saturated ideal of $\mathbb{T}$. Conversely, if I is a saturated ideal of $\mathbb{T}$, then $J_0(N)[I]^0$ is an abelian subvariety of $J_0(N)$.

Proposition 4.5. *The preceding correspondences between abelian subvarieties of $J_0(N)$ and saturated ideals of $\mathbb{T}$ put these two sets of objects in order-reversing bijection with one other. More precisely:*

(i) If A is an abelian subvariety of $J_0(N)$ and $I = \mathrm{Ann}_{\mathbb{T}}(A)$, then $A = J_0(N)[I]^0$.

(ii) If I is a saturated ideal of $\mathbb{T}$, then $\mathrm{Ann}_{\mathbb{T}}(J_0(N)[I]^0) = I$.

(iii) If I_1 and I_2 are two saturated ideals of $\mathbb{T}$, then I_1 is contained in I_2 if and only if $J_0(N)[I_1]^0$ contains $J_0(N)[I_2]^0$.

Proof. This is an easy consequence of the results of [10]; see the discussion of [6, II.10]. □

We now generalize the notion of optimal quotient of $J_0(N)$. If A_1 and A_2 are two abelian subvarieties of $J_0(N)$, such that $A_2 \subset A_1$, we refer to the quotient $A = A_1/A_2$ as an *optimal subquotient* of $J_0(N)$. An important invariant of the optimal subquotient A of $J_0(N)$ is the saturated (by lemma 2.10) ideal $I = \mathrm{Ann}_{\mathbb{T}}(A)$. The following result describes this ideal in terms of the annihilators of A_1 and A_2.

Lemma 4.6. *Let $A = A_1/A_2$ be an optimal subquotient of $J_0(N)$. If we write $I = \mathrm{Ann}_{\mathbb{T}}(A)$, and $I_i = \mathrm{Ann}_{\mathbb{T}}(A_i)$ (for $i = 1, 2$), then $I = (I_1 : I_2)$.*

Proof. An alternative description of I is that it is the ideal of elements of $\mathbb{T}$ that multiply A_1 into A_2. Thus II_2 annihilates A_1, and so $II_2 \subset I_1$. This proves that $I \subset (I_1 : I_2)$.

Proposition 4.5 shows that $A_1 = J_0(N)[I_1]^0$ and that $A_2 = J_0(N)[I_2]^0$. Thus

$$(I_1 : I_2)A_1 = (I_1 : I_2)J_0(N)[I_1]^0 \subset J_0(N)[I_2]^0 = A_2,$$

and so $(I_1 : I_2) \subset I$. Combining this with the result of the preceding paragraph proves the lemma. □

The following result shows that the collection of optimal subquotients of $J_0(N)$ is closed under passing to duals.

Lemma 4.7. *If A is an optimal subquotient of $J_0(N)$, then $\hat{A}$ is naturally isomorphic (as an abelian variety with $\mathbb{T}$-action) to an optimal subquotient of $J_0(N)$.*

Proof. Write $A = A_1/A_2$, $B_1 = J_0(N)/A_1$, and $B_2 = J_0(N)/A_2$. The surjections $J_0(N) \to B_2 \to B_1$ each have connected kernels, and so dualize to yield injections $\hat{B}_1 \to \hat{B}_2 \to J_0(N)\hat{}$. Dualizing the short exact sequence

$$0 \to A \to B_2 \to B_1 \to 0$$

(and using the fact that A is connected) yields the short exact sequence

$$0 \to \hat{B}_1 \to \hat{B}_2 \to \hat{A} \to 0,$$

and so we have an isomorphism $\hat{B}_2/\hat{B}_1 \xrightarrow{\sim} \hat{A}$. The lemma follows once we note that $J_0(N)\hat{}$ is $\mathbb{T}$-equivariantly isomorphic to $J_0(N)$. (See the proof of theorem A. In fact, since w_N centralizes $\mathbb{T}$ when N is prime, the canonical polarization of $J_0(N)$ yields such an isomorphism.) □

Let $\mathcal{I}$ denote the Eisenstein ideal of $\mathbb{T}$ [6, p. 95]. We recall the following consequences of the results of [6], concerning the Eisenstein ideal $\mathcal{I}$ and the Eisenstein maximal ideals of $\mathbb{T}$.

Proposition 4.8. *(i) If $\mathfrak{m}$ is an Eisenstein maximal ideal of $\mathbb{T}$ of residue characteristic ℓ, then $\mathbb{T}_{\mathfrak{m}}$ is a monogenic $\mathbb{Z}_\ell$-algebra, and $\mathcal{I}\mathbb{T}_{\mathfrak{m}}$ is a principal ideal of $\mathbb{T}_{\mathfrak{m}}$.*

(ii) If $\mathfrak{m}$ is a non-Eisenstein maximal ideal of $\mathbb{T}$, then $\mathcal{I}\mathbb{T}_{\mathfrak{m}}$ is the unit ideal of $\mathbb{T}_{\mathfrak{m}}$.

Proof. We begin by noting that [6, prop. II.14.1] reconciles our definition of Eisenstein maximal ideals as being those whose associated Galois representation is reducible with that of Mazur as being those in the support of $\mathbb{T}/\mathcal{I}$. Given this, part (i) follows from [6, cor. II.16.2, thm. II.18.10], while part (ii) is immediate. (To avoid confusion, let us note that our ℓ corresponds to Mazur's p in the preceding references. The role of the "good prime" ℓ that appears in these references is to explicitly describe a local generator of the Eisenstein ideal. This explicit description will be of no importance to us.) □

We are now in a position to show that the results of sections 2 and 3 may be applied to analyze the local structure of optimal subquotients at Eisenstein maximal ideals of $\mathbb{T}$.

Proposition 4.9. *Let A be an optimal subquotient of $J_0(N)$, and let $I = \mathrm{Ann}_{\mathbb{T}}(A)$. If $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$, let $\mathfrak{m}'$ denote the image of $\mathfrak{m}$ in $\mathbb{T}/I$. As in section 3, let G_A denote the semi-abelian variety over $\mathbb{Q}_N$ that rigid analytically uniformizes A over $\mathbb{Q}_N$. Note that $\mathbb{T}/I$ acts on both A and (by functoriality) on G_A. If $\mathfrak{m}$ is an Eisenstein maximal ideal of $\mathbb{T}$, then $\mathfrak{m}'$ is good for both A and G_A.*

Proof. The results of [6] imply that every Eisenstein maximal ideal is good for both $J_0(N)$ and $G_{J_0(N)}$ (see [4, thm. 0.5] and the discussion following its statement). Now repeated applications of lemmas 2.9 and 3.7 prove the proposition (bearing in mind proposition 4.8). □

Recall that C denotes the subgroup of $J_0(N)$ generated by the image of the divisor $0 - \infty$ on $X_0(N)$. We know that C is a free $\mathbb{T}/\mathcal{I}$-module [6, props. II.9.7, II.11.1].

If $A = A_1/A_2$ is an optimal subquotient of $J_0(N)$, we define C_A to be the quotient $C \cap A_1/C \cap A_2$. Note that C_A is a subgroup of $A(\mathbb{Q})_{\mathrm{tor}}$. As in section 3, we also let Φ_A denote the group of connected components of the characteristic N fibre of the Néron model of A.

Lemma 4.10. *If A is an abelian subvariety of $J_0(N)$, if $I = \mathrm{Ann}_{\mathbb{T}}(A)$, and if H is a finite order $\mathbb{T}$-submodule of $J_0(N)$ that is supported on the Eisenstein locus of $\mathbb{T}$, then $H \cap A = H[I]$.*

Proof. Proposition 4.5 shows that $A = J_0(N)[I]^0$. Proposition 4.9, together with corollary 2.5, shows that $J_0(N)[I]/J_0(N)[I]^0$ is supported away from the Eisenstein maximal ideals of $\mathbb{T}$. By assumption H is supported at the Eisenstein maximal ideals of $\mathbb{T}$. Thus we conclude that

$$H \cap A = H \cap J_0(N)[I]^0 = H \cap J_0(N)[I] = H[I],$$

proving the lemma. □

Corollary 4.11. *If A is an abelian subvariety of $J_0(N)$, with annihilator $I = \mathrm{Ann}_{\mathbb{T}}(A)$, then $C \cap A = C[I]$.*

Proof. Part (ii) of proposition 4.8 shows that C is supported at the Eisenstein maximal ideals of $\mathbb{T}$. The corollary is thus a special instance of lemma 4.10. □

Lemma 4.12. *If A is an optimal subquotient of $J_0(N)$, then $A(\mathbb{Q})_{\mathrm{tor}}$ is supported on the Eisenstein locus of $\mathbb{T}$.*

Proof. This follows from [6, lem. III.1.1]. □

We can now state and prove our main theorem concerning optimal subquotients of $J_0(N)$, which will have theorem B as a corollary.

Theorem 4.13. *Let A be an optimal subquotient of $J_0(N)$, and let $I = \mathrm{Ann}_{\mathbb{T}}(A)$.*
(i) C_A is a free $\mathbb{T}/(\mathcal{I} + I)$-module of rank one.
(ii) The specialization map $C_A \to \Phi_A$ is an isomorphism
(iii) The (étale) group scheme Φ_A over $\mathbb{F}_N$ is constant (that is, has trivial Galois action).
(iv) The inclusion $C_A \subset A(\mathbb{Q})_{\mathrm{tor}}$ is an isomorphism.

Proof. For the duration of the proof, write $A = A_1/A_2$, and write $I_i = \mathrm{Ann}_{\mathbb{T}}(A_i)$ (for $i = 1, 2$). We will prove each part of the theorem in turn.

For part (i), note that lemma 4.10 shows that $C_A = C[I_1]/C[I_2]$. Thus C_A is a $\mathbb{T}/(I_1 : I_2)$-module. Lemma 4.6 shows that $(I_1 : I_2) = I$, and so C_A is a $\mathbb{T}/I$-module. Since it is certainly annihilated by $\mathcal{I}$, it is in fact a $\mathbb{T}/(\mathcal{I}+I)$-module.

To show that it is free of rank one, it suffices to check this after completing at each of the Eisenstein maximal ideals $\mathfrak{m}$, since $\mathbb{T}/\mathcal{I}$ is supported at these maximal ideals. If we complete at such a maximal ideal, part (i) of proposition 4.8 shows that we are in the situation of corollary 1.8, and the conclusion of that result gives us what we want. This proves part (i).

We begin our proof of part (ii) by noting that by [14, prop. 2.2], no non-Eisenstein maximal ideal of $\mathbb{T}$ is N-finite. Thus proposition 4.2 implies that Φ_A, Φ_{A_1}, and Φ_{A_2} are all supported on the Eisenstein locus of $\mathbb{T}$. Let $\mathfrak{m}$ be an Eisenstein maximal ideal of $\mathbb{T}$, and let $\mathfrak{m}_1$ denote the image of $\mathfrak{m}$ in $\mathbb{T}/I_1$. Proposition 4.9, together with lemma 4.7, shows that $\mathfrak{m}_1$ is good for both G_{A_1} and $G_{\hat{A}_1}$. Thus corollary 3.6 implies that the sequence

$$0 \to (\Phi_{A_2})_{\mathfrak{m}} \to (\Phi_{A_1})_{\mathfrak{m}} \to (\Phi_A)_{\mathfrak{m}} \to 0$$

is short exact. Since this is true for every Eisenstein maximal ideal, we deduce that

$$0 \to \Phi_{A_2} \to \Phi_{A_1} \to \Phi_A \to 0$$

is short exact.

Now consider the morphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_{A_2} & \longrightarrow & C_{A_1} & \longrightarrow & C_A & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Phi_{A_2} & \longrightarrow & \Phi_{A_1} & \longrightarrow & \Phi_A & \longrightarrow & 0, \end{array}$$

in which the vertical arrows are provided by specialization to characteristic N. Corollary 4.11 implies that $C_{A_2} = C_{A_1}[I_2]$, while $\Phi_{A_2} \subset \Phi_{A_1}[I_2]$, since I_2 annihilates A_2, and hence Φ_{A_2}. Thus if we knew that the central vertical arrow were an isomorphism, we would conclude that the same is true of the left-hand vertical arrow, and hence also of the right-hand vertical arrow. Applying the same argument with A_1, $J_0(N)$ and $J_0(N)/A_1$ in place of A_2, A_1 and A, and using the fact that we know that part (ii) holds for $J_0(N)$ [6, p. 99], we deduce that the central arrow *is* an isomorphism, and thus that part (ii) holds for A. This completes the proof of part (ii).

Part (iii) is an immediate consequence of part (ii), which shows that Φ_A is obtained by specializing a group, all of whose points are defined over $\mathbb{Q}$.

To prove part (iv), we begin by noting that C_A is a direct factor of $A(\mathbb{Q})_{\mathrm{tor}}$. The argument is the same as that of [6, p. 99], namely that the composite of the specialization map $A(\mathbb{Q})_{\mathrm{tor}} \to \Phi_A$ with the inverse of the isomorphism $C_A \xrightarrow{\sim} \Phi_A$ of part (ii) yields a retraction to the inclusion $C_A \subset A(\mathbb{Q})_{\mathrm{tor}}$. Write $A(\mathbb{Q})_{\mathrm{tor}} = C_A \oplus M_A$.

Observe that $C_A \subset A(\mathbb{Q})[\mathcal{I}]$. Suppose that we could prove that this inclusion were an equality. Then we would conclude that $M_A[\mathcal{I}] = 0$, and thus $M_A[\mathfrak{m}]$, and so also $(M_A)_{\mathfrak{m}}$, would be trivial for every Eisenstein maximal ideal $\mathfrak{m}$. Since M_A is supported at the Eisenstein maximal ideals of $\mathbb{T}$ (by lemma 4.12) we would conclude that $M_A = 0$, and part (iv) would be proved. Thus we turn to proving that the inclusion $C_A \subset A(\mathbb{Q})[\mathcal{I}]$ is an equality.

It suffices to prove that for each Eisenstein maximal ideal $\mathfrak{m}$ of $\mathbb{T}$, the corresponding inclusion of $\mathfrak{m}$-adic completions $(C_A)_{\mathfrak{m}} \to A(\mathbb{Q})[\mathcal{I}]_{\mathfrak{m}}$ is an equality. Fix one such $\mathfrak{m}$. We claim that the sequence

$$0 \to A_2[\mathcal{I}]_{\mathfrak{m}} \to A_1[\mathcal{I}]_{\mathfrak{m}} \to A[\mathcal{I}]_{\mathfrak{m}} \to 0$$

is exact. Indeed, this follows from lemma 2.6, once we note that the image $\mathfrak{m}_1$ of $\mathfrak{m}$ in $\mathbb{T}/I_1$ is good for A_1 by proposition 4.9, that I_2/I_1 is a saturated ideal of $\mathbb{T}/I_1$, that $\mathcal{I}(\mathbb{T}/I)_{\mathfrak{m}_1}$ is principal by part (i) of proposition 4.8, and that $A_2 = A_1[I_2/I_1]$. Now $A_i[\mathcal{I}]_{\mathfrak{m}} = J_0(N)[\mathcal{I} + I_i]_{\mathfrak{m}}$, by lemma 4.10, for $i = 1, 2$. Since $(C_{A_i})_{\mathfrak{m}}$ is equal to the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariants of $J_0(N)[\mathcal{I} + I_i]_{\mathfrak{m}}$, we are reduced to proving that the morphism $J_0(N)[\mathcal{I} + I_1]_{\mathfrak{m}} \to J_0(N)[\mathcal{I} + I_1]_{\mathfrak{m}}/J_0(N)[\mathcal{I} + I_2]_{\mathfrak{m}}$ induces a surjection after passing to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariants.

Corollary 1.4 implies that $I_2\mathbb{T}_{\mathfrak{m}}$ is principal; write $I_2\mathbb{T}_{\mathfrak{m}} = \alpha\mathbb{T}_{\mathfrak{m}}$. Multiplication by α induces an isomorphism $J_0(N)[\mathcal{I}+I_1]_{\mathfrak{m}}/J_0(N)[\mathcal{I}+I_2]_{\mathfrak{m}} \xrightarrow{\sim} I_2 J_0(N)[\mathcal{I}+I_1]_{\mathfrak{m}}$.

Thus we must show that multiplication by α induces a surjection from the Galois invariants of $J_0(N)[\mathcal{I}+I_1]_\mathfrak{m}$ onto those of $I_2J_0(N)[\mathcal{I}+I_1]_\mathfrak{m}$.

Since $T_\mathfrak{m}J_0(N)$ is free of rank two over $\mathbb{T}_\mathfrak{m}$ [6, cor. II.16.3], we see that $J_0(N)[\mathcal{I}+I_1]_\mathfrak{m}$ is dual to a module that is free of rank two over $\mathbb{T}_\mathfrak{m}/(\mathcal{I}+I_1)$ (recall again that our Tate modules are contravariant), and so is itself free of rank two over $\mathbb{T}_\mathfrak{m}/(\mathcal{I}+I_1)$. (Since $\mathbb{T}_\mathfrak{m}/(\mathcal{I}+I_1)$ is a quotient of $\mathbb{T}/\mathcal{I}$, which is a quotient of $\mathbb{Z}$, and so is obviously Gorenstein.) Thus corollary 1.7 shows that $I_2J_0(N)[\mathcal{I}+I_1]_\mathfrak{m} = J_0(N)[\mathcal{I}+I_1+I_2^\perp]_\mathfrak{m}$. The Galois invariants of $J_0(N)[\mathcal{I}+I_1]_\mathfrak{m}$ are equal to $C[I_1]_\mathfrak{m}$, and so the Galois invariants of $J_0(N)[\mathcal{I}+I_1+I_2^\perp]_\mathfrak{m}$ are equal to $C[I_1+I_2^\perp]_\mathfrak{m}$. Hence we must show that multiplication by α induces a surjection from $C[I_1]_\mathfrak{m}$ onto $C[I_1+I_2^\perp]_\mathfrak{m}$. Since $C[I_1]_\mathfrak{m}$ is free of rank one over $\mathbb{T}_\mathfrak{m}/(\mathcal{I}+I_1)$, by part (i), this again follows from corollary 1.7. Thus part (iv) is proved. (We remark that rather than appealing to corollary 1.7 in this final step, we could instead have used the fact that $\mathbb{T}/\mathcal{I}$ is isomorphic to $\mathbb{Z}/n$ for an integer n [6, prop. II.9.7]; this allows one to make an analogous argument, using the elementary and explicit description of ideals in $\mathbb{Z}/n$.) □

Proof of theorem B. Let f be a normalized eigenform in $S(N)$. Then A_f and $\hat{A}_f$ are optimal subquotients of $J_0(N)$, both of whose annihilators in $\mathbb{T}$ are equal to I_f. The first six parts of theorem B thus follow immediately from theorem 4.13.

It remains to prove part (vii). Let $\{f_1,\dots,f_d\}$ be a complete set of conjugacy class representatives of the normalized eigenforms in $S(N)$. Observe that we may find a descending sequence of saturated ideals $0 = I_0 \subset I_1 \subset \cdots \subset I_d = \mathbb{T}$ of $\mathbb{T}$ such that $(I_{i-1} : I_i) = I_{f_i}$. Let $A_i = J_0(N)[I_{i-1}]^0/J_0(N)[I_i]^0$ (for $i = 1,\dots,d$). Lemma 4.6 shows that $\mathrm{Ann}_\mathbb{T}(A_i) = I_{f_i}$. Thus part (i) of theorem 4.13 shows that C_{A_i} and $C_{f_i} = C_{A_{f_i}}$ are isomorphic $\mathbb{T}$-modules, and so in particular have the same order. Also, corollary 4.11 shows that $C_{A_i} = C[I_{i-1}]/C[I_i]$. Thus we conclude that

$$\prod_{f_i} \#C_{f_i} = \prod_{i=1}^{d} \frac{\#C[I_{i-1}]}{\#C[I_i]} = \#C.$$

This proves part (vii). □

References

1. A. O. L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.
2. N. Boston, H.W. Lenstra, Jr., K.A. Ribet, *Quotients of group rings arising from two-dimensional representations*, C. R. Acad. Sci. Paris Sér. I Math. **312** (1991), 323–328.
3. K. Buzzard, *On level-lowering for mod 2 representations*, Math. Res. Lett. **7** (2000), 95–110.
4. M. Emerton, *Supersingular elliptic curves, theta series, and weight two modular forms*, J. Amer. Math. Soc. **15** (2002), 671–714.
5. A. Grothendieck, *SGA 7, Exposé IX*, SLN **288** (1972), 313–523.
6. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Étud. Sci. **47** (1977), 33–186.
7. B. Mazur K. A. Ribet, *Two-dimensional representations in the arithmetic of modular curves*, Astérisque **196–197** (1991), 215–255.
8. J.-F. Mestre, J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math., **400** (1989), 173–184.
9. M. Raynaud, *Variétés abéliennes et géométrie rigide*, Actes, Congrès Intern. Math., 1970, Tome 1, 473–477.
10. K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. of Math. **101** (1975), 555–562.

11. ______, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), 193–205.
12. ______, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
13. ______, *Multiplicities of p-finite mod p Galois representations in* $J_0(Np)$, Bol. Soc. Brasil. Mat. (N. S.) **21** (1991), 177–188.
14. ______, *Torsion points on* $J_0(N)$ *and Galois representations*, Arithmetic Theory of Elliptic Curves (J. Coates, ed.), SLN, vol. 1716, 1999.
15. K. A. Ribet, W. A. Stein, *Lectures on Serre's conjectures*, Proceedings of the 1999 IAS/Park City Mathematics Institute, 2000, to appear.
16. K. A. Ribet, S. Takahashi, *Parametrizations of elliptic curves by Shimura curves and by classical modular curves*, Proc. Natl. Acad. Sci. **94** (1997), 11110–11114.
17. J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.
18. G. Shimura, Publ. Math. Soc. Japan **11**, Tokyo-Princeton, 1971.
19. W. A. Stein, *The refined Eisenstein conjecture* , preprint (1999), available at `http://modular.fas.harvard.edu/Tables/Notes/refinedeisen.html`.
20. D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), 372–384.

Northwester University
Department of Mathematics
2033 Sheridan Rd.
Evanston, IL 60208-2730, USA
E-mail address: `emerton@math.northwestern.edu`