

GALOIS EXTENSIONS AND A CONJECTURE OF OGG

KRZYSZTOF KLOSIN AND MIHRAN PAPIKIAN

ABSTRACT. Let $N = pq$ be a product of two distinct primes. There is an isogeny $J_0(N)^{\text{new}} \rightarrow J^N$ defined over \mathbf{Q} between the new quotient of $J_0(N)$ and the Jacobian of the Shimura curve attached to the indefinite quaternion algebra of discriminant N . In the case when $p = 2, 3, 5, 7, 13$, Ogg made predictions about the kernels of these isogenies. We show that Ogg's conjecture is false in general. Afterwards, we propose a strategy for proving results toward Ogg's conjecture in certain situations. Finally, we discuss this strategy in detail for $N = 5 \cdot 13$.

1. INTRODUCTION

1.1. Ogg's conjecture. Let N be a product of an even number of distinct primes. Let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$. In [19], Ribet proved the existence of an isogeny defined over \mathbf{Q} between the “new” part $J_0(N)^{\text{new}}$ of $J_0(N)$ and the Jacobian J^N of the Shimura curve X^N attached to a maximal order in the indefinite quaternion algebra over \mathbf{Q} of discriminant N . The proof proceeds by showing that the \mathbf{Q}_ℓ -adic Tate modules of $J_0(N)^{\text{new}}$ and J^N are isomorphic as $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ -modules, which is a consequence of a correspondence between automorphic forms on $\text{GL}(2)$ and automorphic forms on the multiplicative group of a quaternion algebra. The existence of the isogeny $J_0(N)^{\text{new}} \rightarrow J^N$ defined over \mathbf{Q} then follows from a special case of Tate's isogeny conjecture for abelian varieties over number fields, also proved in [19] (the general case of Tate's conjecture was proved a few years later by Faltings). Unfortunately, this argument provides no information about the isogenies $J_0(N)^{\text{new}} \rightarrow J^N$ beyond their existence.

In [14], Ogg made explicit predictions about the kernel of Ribet's isogeny when $N = pq$ is a product of two distinct primes and $p = 2, 3, 5, 7, 13$. In this case, $J_0(N)^{\text{new}}$ is the quotient of $J_0(N)$ by the subvariety generated by the images of $J_0(q)$ in $J_0(N)$ under the maps induced by the two degeneracy morphisms $X_0(pq) \rightrightarrows X_0(q)$ (note that $J_0(p) = 0$). Let \mathcal{C} be the cuspidal divisor group of $J_0(N)$, which is well-known to be a finite abelian subgroup of $J_0(N)(\mathbf{Q})$; we refer to [3] for a complete description of \mathcal{C} . Let $\overline{\mathcal{C}}$ be the image of \mathcal{C} in $J_0(N)^{\text{new}}$. Denote

$$M = \text{numerator of } (q+1)/12.$$

2010 *Mathematics Subject Classification.* 11G18.

Key words and phrases. Modular curves; Ribet's isogeny; Ogg's conjecture; Eisenstein ideal; cuspidal divisor group.

The first author's research was supported by a Collaboration for Mathematicians Grant #578231 from the Simons Foundation and by a PSC-CUNY research award jointly funded by the Professional Staff Congress and the City University of New York.

The second author's research was supported by a Collaboration for Mathematicians Grant #637364 from the Simons Foundation.

Ogg's conjecture predicts that there is an isogeny $J_0(N)^{\text{new}} \rightarrow J^N$ whose kernel \mathcal{K} is a subgroup of $\overline{\mathcal{C}}$ such that

$$(1.1) \quad \begin{aligned} \mathcal{K} &\cong \mathbf{Z}/M && \text{for } p = 2, 3, 5, \\ \mathcal{K} &\cong \mathbf{Z}/2M && \text{for } p = 7, \\ \mathcal{K} &\cong \mathbf{Z}/7 \oplus \mathbf{Z}/M && \text{for } p = 13. \end{aligned}$$

The underlying idea behind Ogg's conjecture is to compare the component groups of the Néron models of $J_0(N)$ and J^N at q , which provides some reasonable guesses for the kernels of Ribet's isogenies. In fact, Ogg imposes the restriction $p = 2, 3, 5, 7, 13$ to be able to carry out the necessary calculations. We briefly sketch Ogg's reasoning. For simplicity, we ignore the 2 and 3-primary torsion of the groups involved in the discussion, and also the case $p = 13$ where \mathcal{K} might not be cyclic. The component groups of $J_0(N)$ for square-free N are relatively easy to describe; cf. [13, Appendix]. On the other hand, although the component groups of J^N can be computed for a given N by combining a classical method of Raynaud with a result of Cherednik and Drinfeld about the reduction of X^N at q , these groups do not exhibit any regular patterns so cannot be described using only the prime decomposition of N (as is the case for $J_0(N)$). One exception is the case when $N = pq$ and $p = 2, 3, 5, 7, 13$. In this case (and only in this case), the dual graph of the special fibre of the Cherednik-Drinfeld model of X^N at q has two vertices, so the component group is easy to compute and turns out to be cyclic of order $(q+1)$. The component group Φ_q of $J_0(N)$ at q is cyclic of order $(q-1)$. Next, Ogg considers the canonical specialization $\mathcal{C} \rightarrow \Phi_q$, and shows that the "old" part of \mathcal{C} arising from the cuspidal divisor group of $J_0(q)$ maps surjectively onto Φ_q , whereas a specific "new" cuspidal divisor D of order $q+1$ maps to 0 in Φ_q . Then the kernel \mathcal{K} in (1.1) is predicted to be generated by the image of D in $J_0(N)^{\text{new}}$. The fact that $J_0(N)^{\text{new}}$ and J^N have purely toric reduction at q is implicitly used in this last step. (Given an abelian variety A over a local field K with purely toric reduction and a finite constant subgroup $H \subset A(K)$, it is possible to describe the component group of A/H in terms of the component group Φ_A of A and the kernel/image of the canonical specialization $H \rightarrow \Phi_A$; cf. [16, Thm. 4.3].)

Let $\mathbf{T} \subset \text{End}(J_0(N))$ be the Hecke algebra generated over \mathbf{Z} by all Hecke correspondences T_ℓ with prime indices (including those that divide N). The ring \mathbf{T} also acts on $J_0(N)^{\text{new}}$ and J^N (cf. [18]), and it is implicit in [19] that there is an isogeny $J_0(N)^{\text{new}} \rightarrow J^N$ over \mathbf{Q} which is \mathbf{T} -equivariant (cf. [9, Cor. 2.4]). Since the cuspidal divisor group \mathcal{C} is annihilated by the Eisenstein ideal of \mathbf{T} , Ogg's conjecture implies that, in the case when $N = pq$ and $p = 2, 3, 5, 7, 13$, there is an isogeny $J_0(N)^{\text{new}} \rightarrow J^N$ whose kernel is supported on the (new) Eisenstein maximal ideals. (The Eisenstein ideal \mathcal{E} of \mathbf{T} is the ideal generated by all $T_\ell - (\ell + 1)$ for primes $\ell \nmid N$; the Eisenstein maximal ideals are the maximal ideals containing \mathcal{E} .)

In [21], Ribet proved a theorem which implies that the support of the kernel of a \mathbf{T} -equivariant isogeny $J_0(pq)^{\text{new}} \rightarrow J^{pq}$ must, in general, contain maximal ideals of \mathbf{T} which are not Eisenstein, so any construction of such an isogeny must be relatively elaborate. He then gave a concrete example with $p = 11, q = 193$ where this phenomenon occurs. Next, we show that Ribet's construction can be carried

out also in some cases when $p = 2, 3, 5, 7, 13$; thus Ogg's conjecture (1.1) is false in general¹.

Example 1.1. Let E be the elliptic curve over \mathbf{Q} defined by the equation

$$y^2 + y = x^3 - x^2 - 2x + 1.$$

This is the unique, up to isomorphism, elliptic curve of conductor $q = 701$ (which is a prime); cf. [4]. In particular, E has no cyclic isogenies defined over \mathbf{Q} , so $E[3]$ is an irreducible $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ -module. Let $\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{Aut}(E[3])$ be the corresponding Galois representation. Put $p = 7$. By [21, Thm. 1], there is a maximal ideal $\mathfrak{m} \triangleleft \mathbf{T}$ of residue characteristic 3 such that the kernel $J_0(pq)[\mathfrak{m}]$ of \mathfrak{m} on $J_0(pq)(\overline{\mathbf{Q}})$ defines a representation equivalent to ρ . One easily checks either by hand, or with the help of `Magma`, that $E(\mathbf{F}_p) \cong \mathbf{Z}/3 \times \mathbf{Z}/3$. This implies that $\rho(\text{Frob}_p) = 1$. In particular,

$$\text{Tr}(\rho(\text{Frob}_p)) = 2 \equiv (p + 1) \pmod{\mathfrak{m}}.$$

As is explained in [21], the above congruence implies that \mathfrak{m} is new. By Theorem 2 in [21], $\dim_{\mathbf{F}_3} J_0(pq)^{\text{new}}[\mathfrak{m}] = 2$. On the other hand, since ρ is unramified at p , Theorem 3 in [21] applies, so $\dim_{\mathbf{F}_3} J^{pq}[\mathfrak{m}] = 4$. It easily follows from this that the kernel of any \mathbf{T} -equivariant isogeny $J_0(pq)^{\text{new}} \rightarrow J^{pq}$ must have the non-Eisenstein \mathfrak{m} in its support, contrary to Ogg's conjecture. (Otherwise, by duality, there is a homomorphism $J^{pq} \rightarrow J_0(pq)$ with finite kernel whose support does not contain \mathfrak{m} . This implies that there is an injection $J^{pq}[\mathfrak{m}] \rightarrow J_0(pq)[\mathfrak{m}]$, which is absurd.)

A similar construction also works for $p = 13$ and $q = 571$. Let $E : y^2 + y = x^3 + x^2 - 4x + 2$ be the curve 571 B1 in Cremona's table [4]. Again, $E[3]$ is irreducible and the corresponding Galois representation ρ satisfies $\rho(\text{Frob}_{13}) = -1$. Ribet's theorems then imply that $\dim_{\mathbf{F}_3} J^{pq}[\mathfrak{m}] = 4$ and $\dim_{\mathbf{F}_3} J_0(pq)^{\text{new}}[\mathfrak{m}] = 2$, from which one obtains a contradiction to (1.1) as before.

Despite the fact that Ogg's conjecture is false in general, some cases of the conjecture for *small* levels have been proved. The conjecture is easy to verify when $J_0(pq)^{\text{new}}$ and J^{pq} are elliptic curves (there are five such cases). When X^{pq} is hyperelliptic of genus 2 or 3, Ogg's conjecture is verified in [6] and [5] (there are twelve such cases). The strategy here is to explicitly compute and compare the period matrices of $J_0(pq)^{\text{new}}$ and J^{pq} , which itself relies on a lengthy calculation of the defining equations of hyperelliptic Shimura curves. When $N = 5 \cdot 13$, Ogg's conjecture is verified in [10], up to 2-primary torsion supported on a maximal Eisenstein ideal. In this case, X^N has genus 5 and is not hyperelliptic. Our approach in [10] is completely different from [6, 5] and relies on the Hecke equivariance of Ribet isogenies and the fact that the Hecke algebra of level 65 is a rather simple ring.

For general $N = pq$, Yoo [31] proved that, under certain congruence assumptions on p , q , and ℓ , the kernel of a Ribet isogeny $J_0(N)^{\text{new}} \rightarrow J^N$ must contain the ℓ -primary subgroup of the cuspidal divisor group $\overline{\mathcal{C}}$. This result implies that for $p = 2, 3, 5, 7, 13$ and odd $\ell \geq 5$, $\ker(\pi)$ contains $\mathcal{K} \otimes \mathbf{Z}_\ell$ from (1.1), in accordance with Ogg's conjecture.

¹To be fair, Ogg writes in his paper [14, p. 213] "On devine (deviner est plus faible que conjecturer) donc qu'on peut prendre \mathcal{K} comme noyau de l'isogénie, avec confiance si la partie ancienne est triviale, i.e. si $(q - 1) \mid 12$." Hence, perhaps, we should have called (1.1) "Ogg's guess".

1.2. Main result. In this article we continue exploring avenues that lead to partial results toward Ogg's conjecture. While we again employ the Hecke algebra, we propose a different approach from [10] which has the advantage of being applicable to larger values of N than 65.

Now we outline our approach and state the main results. To simplify the notation, let $J := J_0(N)$ and $J' := J^N$. Let S denote the finite set of maximal ideals of \mathbf{T} that are either Eisenstein, or of residue characteristic 2 or 3. There is an element $\sigma_S \in \mathbf{T}$ such that for any maximal ideal \mathfrak{m} of \mathbf{T} , one has $\sigma_S \in \mathfrak{m}$ if and only if $\mathfrak{m} \in S$ (cf. Lemma 3.2 in [9]). Set $\mathbf{T}_S := \mathbf{T}[\sigma_S^{-1}]$.

J^{new} and J' have purely toric reduction at the primes p and q , and good reduction everywhere else. For $A = J^{\text{new}}$ or J' , denote by $M_p(A) = \text{Hom}(\mathcal{A}_{\mathbf{F}_p}^0, \mathbf{G}_{m, \overline{\mathbf{F}_p}})$ the character group of A at p . Here \mathcal{A} is the Néron model of A over \mathbf{Z}_p , and $\mathcal{A}_{\mathbf{F}_p}^0$ is the connected component of the identity of the special fibre of \mathcal{A} at p . The character group $M_p(A)$ is a free abelian group of rank equal to $\dim(A)$. We similarly define the character group $M_q(A)$ at q . By the Néron mapping property, \mathbf{T} acts on $M_p(A)$ and $M_q(A)$.

A special case of a result of Helm [9, Prop. 8.13] implies that there is an isomorphism of \mathbf{T}_S -modules

$$(1.2) \quad \text{Hom}(J^{\text{new}}, J') \cong_{\mathbf{T}_S} \text{Hom}(M_q(J'), M_q(J^{\text{new}})).$$

On the other hand, a special case of a result of Ribet [18, Thm. 4.1] implies that

$$(1.3) \quad M_q(J') \cong_{\mathbf{T}} M_p(J^{\text{new}}).$$

Since the cuspidal divisor group of J is annihilated by the Eisenstein ideal of \mathbf{T} , (1.1) combined with (1.2) and (1.3) implies that

$$(1.4) \quad M_p(J^{\text{new}}) \cong_{\mathbf{T}_S} M_q(J^{\text{new}}).$$

Conversely, if (1.4) is true, then (1.2) and (1.3) imply that there is an isogeny $\pi : J^{\text{new}} \rightarrow J'$ whose kernel is supported on the maximal ideals in S .

This offers a natural strategy for proving results toward Ogg's conjecture. First, one needs to prove (1.4). Since the character groups are free \mathbf{Z} -modules, this step involves only linear algebra calculations, which may be quite daunting in practice - but we note here that there exist algorithms that allow one to do this at least in principle; cf. Section 3. The second step comprises classifying isogenies supported on the maximal ideals in S . This can be achieved by excluding the existence of certain subgroup schemes in $J[\mathfrak{m}^s]$ for $\mathfrak{m} \in S$, a problem which in [10] (for $N = 65$) was handled by an ad hoc counting argument.

In this paper we offer a more systematic approach for step 2 based on the non-existence of certain deformations of non-split Galois extensions

$$(1.5) \quad 0 \rightarrow \mathbf{Z}/\ell \rightarrow \overline{\rho} \rightarrow \mu_\ell \rightarrow 0,$$

where $\ell \geq 5$ is a prime. By the results of Ohta and Yoo [15, 30], one knows that the residue characteristic of an Eisenstein maximal ideal divides either $p \pm 1$ or $q \pm 1$. We will assume that ℓ satisfies one of the following conditions:

$$(1.6) \quad \ell \mid (p + 1) \text{ and } \ell \nmid (q \pm 1),$$

$$(1.7) \quad \ell \mid (q + 1) \text{ and } \ell \nmid (p \pm 1).$$

Put $\mathfrak{m} = (T_p + 1, T_q - 1, \mathcal{E}, \ell)$ in the first case, and $\mathfrak{m} = (T_p - 1, T_q + 1, \mathcal{E}, \ell)$ in the second case. Then \mathfrak{m} is a new Eisenstein maximal ideal of residue characteristic ℓ

and $\dim_{\mathbf{F}_\ell} J[\mathfrak{m}] = 2$; cf. [30], [29]. In particular, the action of $G_{\mathbf{Q}} = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $J[\mathfrak{m}]$ gives rise to an extension

$$(1.8) \quad 0 \rightarrow \mathbf{Z}/\ell \rightarrow J[\mathfrak{m}] \rightarrow \mu_\ell \rightarrow 0.$$

This extension does not split. Indeed, by a theorem of Vatsal [25], the extension (1.8) splits if and only if $\mu_\ell \subset \mathcal{S}$, where \mathcal{S} denotes the Shimura subgroup of J . Ignoring the 2 and 3-primary torsion, one has $\#\mathcal{S} = (p-1)(q-1)$; cf. [12]. Thus for $\ell \nmid (p-1)(q-1)$ we see that $\mu_\ell \not\subset \mathcal{S}$. Hence (1.8) can in fact be viewed as a non-split extension of Galois modules of the form (1.5). We also note that, ignoring the 2 and 3-primary torsion, the cuspidal divisor group \mathcal{C} of J and the Eisenstein ideal \mathcal{E} satisfy (cf. [3], [15], [30])

$$\mathbf{T}/\mathcal{E} \cong \mathcal{C} \cong \mathbf{Z}/(p-1)(q-1) \oplus \mathbf{Z}/(p+1)(q-1) \oplus \mathbf{Z}/(p-1)(q+1).$$

This implies that \mathfrak{m} is the unique Eisenstein maximal ideal of residue characteristic ℓ and the constant subgroup scheme of $J[\mathfrak{m}]$ in (1.8) is $\mathcal{C}[\ell]$.

In Theorem 2.9 (and Corollary 2.10) we prove that under the above assumptions on ℓ , the Galois representation $\bar{\rho} := J[\mathfrak{m}]$ does not admit any (non-trivial) reducible (Fontaine-Laffaille) deformations of determinant ϵ , the ℓ -adic cyclotomic character (or its mod ℓ^m reduction). This allows us to prove the following result, which is the main theorem of the paper.

Theorem 1.2. *Assume (1.4) is satisfied, so that there is an isogeny $\pi : J^{\text{new}} \rightarrow J'$ with kernel supported on the maximal ideals in S . Assume π is chosen to have minimal degree. Let $\ell \geq 5$ be a prime that satisfies either (1.6) or (1.7). Let $\mathfrak{m} \in S$ be the new Eisenstein maximal ideal of residue characteristic ℓ . Assume further that $J^{\text{new}}/J^{\text{new}}[\mathfrak{m}] \cong J^{\text{new}}$. Then the ℓ -primary part of $\ker \pi$ is contained in $\mathcal{C}[\ell] \cong \mathbf{Z}/\ell$.*

Proof. Let H be the ℓ -primary part of $\ker(\pi)$. Note that $J^{\text{new}}[\mathfrak{m}] \not\subset H$, since otherwise π factors through

$$J^{\text{new}} \rightarrow J^{\text{new}}/J^{\text{new}}[\mathfrak{m}] \cong J^{\text{new}} \xrightarrow{\pi'} J',$$

contradicting the minimality of the degree of π . Since \mathfrak{m} is new and satisfies multiplicity one, we have $J[\mathfrak{m}] \cong J^{\text{new}}[\mathfrak{m}]$. One can consider H as a subgroup scheme of $J[\mathfrak{m}^s]$ for some $s \in \mathbf{Z}_+$. We claim that H is a proper subscheme of $J[\mathfrak{m}]$. If this is not the case (i.e., H is not a proper subscheme of $J[\mathfrak{m}]$) then we see as in the proof of Proposition 4.5 in [10] that without loss of generality we may assume that $s = 2$. The equivalence of (1) and (2) in Lemma 15.1 of [13] implies that since $\dim_{\mathbf{F}_\ell} J[\mathfrak{m}] = 2$ we get $J[\mathfrak{m}^2] \cong \mathbf{T}/\mathfrak{m}^2 \oplus \mathbf{T}/\mathfrak{m}^2$ as \mathbf{T} -modules. Hence $H = \mathbf{T}/\mathfrak{m}^{s_1} \oplus \mathbf{T}/\mathfrak{m}^{s_2}$, with $0 \leq s_1 \leq s_2$. Clearly $s_1 = 0$ since otherwise $H \supset H[\mathfrak{m}] = J[\mathfrak{m}]$. Also $s_2 = 2$ as otherwise $H \subset J[\mathfrak{m}]$. Hence H is a Galois stable line (free $\mathbf{T}/\mathfrak{m}^2$ -module of rank 1) in $J[\mathfrak{m}^2]$. Let χ_1 be the character by which $G_{\mathbf{Q}}$ acts on this line and write χ_2 for the character by which it acts on the quotient $J[\mathfrak{m}^2]/H$. Then the Galois representation $\rho : G_{\mathbf{Q}} \rightarrow \text{GL}_2(\mathbf{T}/\mathfrak{m}^2)$ afforded by $J[\mathfrak{m}^2]$ satisfies the conditions in Corollary 2.10 with $\{\ell_1, \ell_2\} = \{p, q\}$, $\Sigma' = \{p, q, \ell\}$ (we note that ρ is in the image of the Fontaine-Laffaille functor since it arises as a subquotient of the Galois representation afforded by the Tate module of an abelian variety), so it cannot exist. Thus, $H \subsetneq J[\mathfrak{m}]$. Finally, because $J[\mathfrak{m}]$ is non-split, the only $G_{\mathbf{Q}}$ -stable subgroup of $J[\mathfrak{m}]$ is its constant subgroup \mathbf{Z}/ℓ which comes from the cuspidal divisor group. \square

To conclude the introduction, let us comment on how Theorem 1.2 applies to Ogg's conjecture. Assumption (1.4) can be checked using an explicit matrix representation of generators of \mathbf{T} . In the case $N = 65$ we carry out this calculation in Section 3. In fact, in this case, we are able to prove a stronger result, namely that $M_p(J) \cong M_q(J)$ as \mathbf{T} -modules without inverting σ_S . (This also shows that (1.2) is not true without inverting the Eisenstein maximal ideals since the Jacobians J and J' are not isomorphic in this case.)

The assumption $J^{\text{new}}/J^{\text{new}}[\mathfrak{m}] \cong J^{\text{new}}$ is essentially equivalent to \mathfrak{m} being principal in \mathbf{T}^{new} , where \mathbf{T}^{new} denotes the quotient by which \mathbf{T} acts on J^{new} . Indeed, if $\mathfrak{m} = (\eta) \triangleleft \mathbf{T}^{\text{new}}$ is principal, then $J^{\text{new}}[\mathfrak{m}]$ is the kernel of the isogeny $J^{\text{new}} \xrightarrow{\eta} J^{\text{new}}$. Conversely, if $J^{\text{new}}/J^{\text{new}}[\mathfrak{m}] \cong J^{\text{new}}$, then $J^{\text{new}}[\mathfrak{m}]$ is the kernel of an endomorphism η of J^{new} . If $\eta \in \mathbf{T}^{\text{new}}$, then \mathfrak{m} is generated by η . If pq is odd, then [20, Prop. 3.2] and [26, Cor. 2.4] imply that $\text{End}(J^{\text{new}}) = \mathbf{T}^{\text{new}}$, so $\eta \in \mathbf{T}^{\text{new}}$. The assumption on the principality of \mathfrak{m} is satisfied for some Eisenstein maximal ideals in Hecke algebras of small levels, for example, those $N = pq$ for which $J = J^{\text{new}}$ (equiv. $(p-1)$ and $(q-1)$ divide 12), which is related to the fact that in those cases the Hecke algebra $\mathbf{T} \otimes \mathbf{Q}$ turns out to be a direct product of number fields of class number 1.

Finally, once we know $\ker(\pi) \otimes \mathbf{Z}_\ell \subset \overline{\mathcal{C}}[\ell]$, the ℓ -primary part of $\ker(\pi)$ can be determined by comparing the component groups of J^{new} and $J^{\text{new}}/\overline{\mathcal{C}}[\ell]$ with the component groups of J' , as was originally done by Ogg. In the case $N = 65$, the prime $\ell = 7$ is the only one which satisfies the conditions of Theorem 1.2 (the other two Eisenstein primes are 2 and 3). Thus Theorem 1.2 gives an alternative proof that for $N = 65$ there is an isogeny $\pi : J \rightarrow J'$ such that $\ker(\pi) \otimes \mathbf{Z}_\ell \cong \mathcal{K} \otimes \mathbf{Z}_\ell$ for \mathcal{K} in (1.1) and $\ell \geq 5$.

2. NON-EXISTENCE OF CERTAIN GALOIS EXTENSIONS

Let $\ell > 2$ and $\Sigma := \{\ell_1, \ell_2, \dots, \ell_k\}$ be a set of distinct primes such that $\ell \nmid \ell_i(\ell_i - 1)$ for $i = 1, \dots, k$. Write $\Sigma' := \Sigma \cup \{\ell\}$ and $G_{\Sigma'}$ for the absolute Galois group of the maximal Galois extension of \mathbf{Q} unramified outside Σ' .

Consider a representation $\bar{\rho} : G_{\Sigma'} \rightarrow \text{GL}_2(\mathbf{F}_\ell)$ which is a non-split extension of the form

$$\bar{\rho} = \begin{bmatrix} 1 & * \\ & \bar{\epsilon} \end{bmatrix},$$

where ϵ will denote the ℓ -adic cyclotomic character (but we will also use ϵ to denote the reduction of the ℓ -adic cyclotomic character mod ℓ^m) and $\bar{\epsilon}$ its mod ℓ reduction.

The main result of this section is Theorem 2.9 (and Corollary 2.10) which asserts the non-existence of certain trace-reducible deformations of $\bar{\rho}$. The proof essentially boils down to showing that there are no (trace-reducible) deformations to \mathbf{Z}/ℓ^2 as well as no non-trivial (trace-reducible) deformations to the dual numbers $\mathbf{F}_\ell[X]/X^2$. We begin with the \mathbf{Z}/ℓ^2 -case – the harder of the two (Proposition 2.1 below), which we prove in a slightly greater generality than needed for our purposes. We fix once and for all an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$. Let $m \geq 2$ be an integer.

Proposition 2.1. *Suppose $\text{val}_\ell(\ell_1^2 - 1) = m - 1$ (which is equivalent to $\text{val}_\ell(\ell_1 + 1) = m - 1$) and $\text{val}_\ell(\ell_i^2 - 1) = 0$ (equivalent to $\text{val}_\ell(\ell_i + 1) = 0$) for all $i = 2, 3, \dots, k$. Then there does not exist a Galois representation $\rho_m : G_{\Sigma'} \rightarrow \text{GL}_2(\mathbf{Z}/\ell^m)$ such that*

- (i) ρ_m is crystalline in the image of the Fontaine-Laffaille functor at ℓ ;

- (ii) $\det \rho_m = \epsilon$;
- (iii) $\mathrm{tr} \rho_m = \chi_1 + \chi_2$ for some Galois characters $\chi_1, \chi_2 : G_{\Sigma'} \rightarrow (\mathbf{Z}/\ell^m)^\times$ with $\chi_1 \equiv 1 \pmod{\ell}$ and $\chi_2 \equiv \bar{\epsilon} \pmod{\ell}$;
- (iv) $\rho_m \equiv \bar{\rho} \pmod{\ell}$.

Remark 2.2. Below for brevity we will refer to representations in the image of the Fontaine-Laffaille functor simply as Fontaine-Laffaille representations. All the properties of such representations that we will use are stated e.g. in [1].

We prepare the proof of Proposition 2.1 by several lemmas.

Lemma 2.3. *We must have $\chi_1 = 1$ and $\chi_2 = \epsilon$*

Proof. It is enough to show that $\chi_1 = 1$ as then $\chi_2 = \epsilon$ by (ii). First note that since ρ_m is a Fontaine-Laffaille representation and the category of these is closed under taking subquotients, so is χ_1 . Furthermore, χ_1 is unramified outside Σ' . Hence to prove the claim it is enough to show that the trivial character does not admit any non-trivial Fontaine-Laffaille infinitesimal deformations $\psi : G_{\Sigma'} \rightarrow (\mathbf{F}[X]/X^2)^\times$. This in turn can be proven as Proposition 9.5 of [1]. \square

To prove Proposition 2.1 let us first note that by the main Theorem of [24] if ρ_m whose trace splits as in (iii) exists then it can be conjugated to an upper-triangular representation of the form

$$\rho_m = \begin{bmatrix} \chi_1 & * \\ & \chi_2 \end{bmatrix}.$$

We can treat ρ_m as an element of $H^1(\mathbf{Q}, (\mathbf{Z}/\ell^m)(\chi_1\chi_2^{-1}))$ which does not lie in $H^1(\mathbf{Q}, (\ell\mathbf{Z}/\ell^m\mathbf{Z})(\chi_1\chi_2^{-1}))$, i.e., is of maximal order. This is so, because the extension given by ρ_m reduces mod ℓ to $\bar{\rho}$ which is not split.

For the moment we will work in a slightly greater generality and assume that $\chi_1 = 1$ and $\chi_2 = \chi = \epsilon^n$ for $n \not\equiv 0 \pmod{\ell-1}$, however we apply it only in the case when $n = 1$. Set

$$T = \mathbf{Z}_\ell(-n) = \mathbf{Z}_\ell(\epsilon^{-n}), \quad V = \mathbf{Q}_\ell(-n), \quad W = \mathbf{Q}_\ell/\mathbf{Z}_\ell(-n)$$

and

$$W_M := \ell^{-M}\mathbf{Z}_\ell/\mathbf{Z}_\ell(-n) = \mathbf{Z}_\ell/\ell^M\mathbf{Z}_\ell(-n) = W[\ell^M],$$

where by $W[s]$ we mean the s -torsion. For a place v of \mathbf{Q} , and $M = V, W$ or W_M , set $H_{\mathrm{ur}}^1(\mathbf{Q}_v, M) = \ker(H^1(\mathbf{Q}_v, M) \rightarrow H^1(I_v, M))$. Then, following [22], section 1.3, we set

$$H_f^1(\mathbf{Q}_v, V) := \begin{cases} H_{\mathrm{ur}}^1(\mathbf{Q}_v, V) & \text{if } v \neq \ell \\ \ker(H^1(\mathbf{Q}_v, V) \rightarrow H^1(\mathbf{Q}_v, V \otimes_{\mathbf{Q}_v} B_{\mathrm{cris}})) & \text{if } v = \ell. \end{cases}$$

We define $H_f^1(\mathbf{Q}_v, W)$ as the image of $H_f^1(\mathbf{Q}_v, V)$ in $H^1(\mathbf{Q}_v, W)$. For the finite set Σ of finite places of \mathbf{Q} , we then define the global Selmer group (cf. [22], Definition 1.5.1):

$$\mathcal{S}^\Sigma(\mathbf{Q}, W) := \ker(H^1(\mathbf{Q}, W) \rightarrow \bigoplus_{v \notin \Sigma} \frac{H^1(\mathbf{Q}_v, W)}{H_f^1(\mathbf{Q}_v, W)}).$$

One defines $\mathcal{S}^\Sigma(\mathbf{Q}, W_M)$ similarly (cf. [22], p. 22).

Lemma 2.4. *One has $\mathcal{S}^\Sigma(\mathbf{Q}, W_M) = \mathcal{S}^\Sigma(\mathbf{Q}, W)[\ell^M]$.*

Proof. By Lemma 1.5.4 of [22], we get that there is a natural surjection of the left-hand side onto the right-hand side. However, the proof of that lemma uses the exact sequence in Lemma 1.2.2(i) in [22] and in our case $W^{G\mathbf{Q}} = 0$ as $n \not\equiv 0 \pmod{\ell - 1}$, which shows that the surjection is in fact an isomorphism. \square

Let us first relate $\mathcal{S}^\Sigma(\mathbf{Q}, W_m)$ to $\mathcal{S}^\emptyset(\mathbf{Q}, W_m)$.

Lemma 2.5. *Suppose $\text{val}_\ell(\ell_1^{n+1} - 1) = m - 1$ and $\text{val}_\ell(\ell_i^{n+1} - 1) = 0$ for all $i = 2, 3, \dots, k$. Then one has*

$$\#\mathcal{S}^\Sigma(\mathbf{Q}, W_m) \leq \ell^{m-1} \#\mathcal{S}^\emptyset(\mathbf{Q}, W_m).$$

Proof. Fix $s \in \{1, 2, \dots, k\}$. Since W is unramified at ℓ_s we get $H_{\text{ur}}^1(\mathbf{Q}_{\ell_s}, W) = H_f^1(\mathbf{Q}_{\ell_s}, W)$ (by Lemma 1.3.5(iv) in [22]) as well as $H_{\text{ur}}^1(\mathbf{Q}_{\ell_s}, W_m) = H_f^1(\mathbf{Q}_{\ell_s}, W_m)$ (by Lemma 1.3.8(ii) in [22]) and

$$(2.1) \quad H^1(I_{\ell_s}, W_m) = \text{Hom}(\mathbf{Z}_\ell(1), W_m) = W_m(-1).$$

This gives an upper bound of ℓ^m on the order of the quotient $H^1(\mathbf{Q}_{\ell_s}, W_m)/H_f^1(\mathbf{Q}_{\ell_s}, W_m)$. However, let us now show that the upper bound is in fact ℓ^{m-1} (resp. 1) if $s = 1$ (resp. $s \neq 1$). Indeed, this will follow if we show that the map $H^1(\mathbf{Q}_{\ell_s}, W_m) \rightarrow H^1(I_{\ell_s}, W_m)$ is not surjective (resp. is the zero map) if $s = 1$ (resp. $s \neq 1$). To do so consider the inflation-restriction sequence (where we set $G := \text{Gal}(\mathbf{Q}_{\ell_s}^{\text{ur}}/\mathbf{Q}_{\ell_s})$):

$$H^1(G, W_m) \rightarrow H^1(\mathbf{Q}_{\ell_s}, W_m) \rightarrow H^1(I_{\ell_s}, W_m)^G \rightarrow H^2(G, W_m).$$

The last group in the above sequence is zero since $G \cong \hat{\mathbf{Z}}$ and $\hat{\mathbf{Z}}$ has cohomological dimension one. This means that the image of the restriction map $H^1(\mathbf{Q}_{\ell_s}, W_m) \rightarrow H^1(I_{\ell_s}, W_m)$ equals $H^1(I_{\ell_s}, W_m)^G$. Let us show that the latter \mathbf{Z}_ℓ -module is a proper submodule of $H^1(I_{\ell_s}, W_m)$ (resp. is the zero module) if $s = 1$ (resp. $s \neq 1$). Indeed,

$$H^1(I_{\ell_s}, W_m)^G = \text{Hom}_G(\mathbf{Z}_\ell(1), \frac{1}{\mathbf{Z}_\ell} \mathbf{Z}_\ell(-n)) = \text{Hom}_G(\mathbf{Z}_\ell, \frac{1}{\mathbf{Z}_\ell} \mathbf{Z}_\ell(-n-1)).$$

So, $\phi \in H^1(I_{\ell_s}, W_m)$ lies in $H^1(I_{\ell_s}, W_m)^G = \text{Hom}_G(\mathbf{Z}_\ell, \frac{1}{\mathbf{Z}_\ell} \mathbf{Z}_\ell(-n-1))$ if and only if $\phi(x) = \phi(gx) = g \cdot \phi(x) = \epsilon^{-n-1}(g)\phi(x)$ for every $x \in I_{\ell_s}$ and every $g \in G$, i.e., if and only if

$$(2.2) \quad (\epsilon^{-n-1}(g) - 1)\phi(x) \in \mathbf{Z}_\ell \quad \text{for every } x \in I_{\ell_s}, g \in G.$$

Since Frob_{ℓ_s} topologically generates G , we see that (2.2) holds if and only if it holds for every $x \in I_{\ell_s}$ and for $g = \text{Frob}_{\ell_s}$. We have $\epsilon^{-n-1}(\text{Frob}_{\ell_s}) - 1 = \ell_s^{-n-1} - 1 = \frac{1 - \ell_s^{n+1}}{\ell_s^{n+1}}$. Since $\ell_s^{n+1} \in \mathbf{Z}_\ell^\times$, condition (2.2) becomes

$$(2.3) \quad (1 - \ell_s^{n+1})\phi(x) \in \mathbf{Z}_\ell \quad \text{for every } x \in I_{\ell_s}.$$

By our assumption $\text{val}_\ell(1 - \ell_s^{n+1}) = m - 1$ (resp. $\text{val}_\ell(1 - \ell_s^{n+1}) = 0$) if $s = 1$ (resp. $s \neq 1$), which implies that (2.3) is equivalent to $\ell^{m-1}\phi(x) = 0$ (resp. $\phi(x) = 0$) in W_m if $s = 1$ (resp. $s \neq 1$). Using the isomorphism (2.1) we see that this implies that $H^1(I_{\ell_s}, W_m)^G$ is a proper \mathbf{Z}_ℓ -submodule of $H^1(I_{\ell_s}, W_m)$ as $W_m(-1)$ certainly contains elements not annihilated by ℓ^{m-1} .

Now, by Theorem 1.7.3 in [22] we have an exact sequence

$$(2.4) \quad 0 \rightarrow \mathcal{S}^\emptyset(\mathbf{Q}, W_m) \rightarrow \mathcal{S}^\Sigma(\mathbf{Q}, W_m) \rightarrow \bigoplus_{i=1}^k \frac{H^1(\mathbf{Q}_{\ell_i}, W_m)}{H_f^1(\mathbf{Q}_{\ell_i}, W_m)}.$$

As shown above the order of the module on the right is bounded from above by ℓ^{m-1} . This gives the desired inequality. \square

Let us record here one consequence of the above proof.

Lemma 2.6. *Suppose $\mathcal{S}^\theta(\mathbf{Q}, W_m) = 0$. Assume $\text{val}_\ell(\ell_1^{n+1} - 1) = m - 1$ and $\text{val}_\ell(\ell_i^{n+1} - 1) = 0$ for all $i = 2, 3, \dots, k$. Then $\mathcal{S}^\Sigma(\mathbf{Q}, W_m)$ is a cyclic \mathbf{Z}_ℓ -module, i.e., $\mathcal{S}^\Sigma(\mathbf{Q}, W_m) \cong \mathbf{Z}/\ell^s$. Furthermore, $\dim_{\mathbf{F}_\ell} \mathcal{S}^\Sigma(\mathbf{Q}, W_1) = 1$.*

Proof. From (2.4) (and the first isomorphism theorem for modules) we get $\mathcal{S}^\Sigma(\mathbf{Q}, W_m) \subset \frac{H^1(\mathbf{Q}_{\ell_1}, W_m)}{H_{\text{ur}}^1(\mathbf{Q}_{\ell_1}, W_m)} \cong I$, where I is the image of the restriction map $H^1(\mathbf{Q}_{\ell_1}, W_m) \rightarrow H^1(I_{\ell_1}, W_m) \cong W_m$. The last module is cyclic. The one-dimensionality statement follows from this and Lemma 2.4. \square

From now on set $n = 1$, so $W = \mathbf{Q}_\ell/\mathbf{Z}_\ell(-1)$.

Proposition 2.7. *The Selmer group $\mathcal{S}^\theta(\mathbf{Q}, W_m)$ is trivial.*

Proof. It is enough to show that the group $\mathcal{S}^\theta(\mathbf{Q}, W_1)$ is trivial. Indeed, Lemma 2.4 shows $\mathcal{S}^\theta(\mathbf{Q}, W_m) = \mathcal{S}^\theta(\mathbf{Q}, W)[\ell^m]$. So it suffices to show that $\mathcal{S}^\theta(\mathbf{Q}, W) = 0$. Since the latter module is divisible, it is enough to show that it has no ℓ -torsion, i.e., that $\mathcal{S}^\theta(\mathbf{Q}, W)[\ell] = \mathcal{S}^\theta(\mathbf{Q}, W_1) = 0$. It follows from Fontaine-Laffaille theory that $H_f^1(\mathbf{Q}_\ell, W_1) = H_{\text{ur}}^1(\mathbf{Q}_\ell, W_1)$ so that $\mathcal{S}^\theta(\mathbf{Q}, W_1) = \text{Hom}(\text{Cl}_{\mathbf{Q}(\mu_\ell)}, W_1)^{\text{Gal}(\mathbf{Q}(\mu_\ell)/\mathbf{Q})}$. The latter module is zero by Herbrand's Theorem since the relevant Bernoulli number $B_2 = 1/6$ (see e.g., Theorem 6.17 in [28]). \square

Proof of Proposition 2.1. Assume that ρ_m as in the proposition exists. We can treat ρ_m as an element of $H^1(\mathbf{Q}, (\mathbf{Z}/\ell^m)(\chi_1\chi_2^{-1}))$ which is not annihilated by ℓ^{m-1} because its mod ℓ reduction is non-split. By Lemma 2.3 we have $\chi_1 = 1$ and $\chi_2 = \epsilon$. Also note that $\mathbf{Z}/\ell^m(\epsilon^{-1}) \cong W_m$. The extension given by ρ_m being unramified away from Σ' and Fontaine-Laffaille (at ℓ) in fact gives rise to an element inside $\mathcal{S}^\Sigma(\mathbf{Q}, W_m) \subset H^1(\mathbf{Q}, W_m)$ not annihilated by ℓ^{m-1} . However, combining Lemma 2.5 applied in the case $n = 1$ with Proposition 2.7 we see that $\mathcal{S}^\Sigma(\mathbf{Q}, W_m)$ is annihilated by ℓ^{m-1} which leads to a contradiction. \square

Proposition 2.8. *Let $\rho' : G_{\Sigma'} \rightarrow \text{GL}_2(\mathbf{F}_\ell[X]/X^2)$ be a representation such that*

- (i) ρ' is Fontaine-Laffaille;
- (ii) $\det \rho' = \bar{\epsilon}$;
- (iii) $\text{tr } \rho' = \chi_1 + \chi_2$ for some Galois characters $\chi_1, \chi_2 : G_{\Sigma'} \rightarrow (\mathbf{F}_\ell[X]/X^2)^\times$ with $\chi_1 \equiv 1 \pmod{X}$ and $\chi_2 \equiv \bar{\epsilon} \pmod{X}$;
- (iv) $\rho' \equiv \bar{\rho} \pmod{X}$.

Then ρ' is isomorphic to $\bar{\rho}$ viewed as an $\mathbf{F}_\ell[X]/X^2[G_{\Sigma'}]$ -module via the natural inclusion $\text{GL}_2(\mathbf{F}_\ell) \hookrightarrow \text{GL}_2(\mathbf{F}_\ell[X]/X^2)$.

Proof. Using again the main theorem of [24] we conclude that ρ' can be conjugated to a representation of the form $\begin{bmatrix} \chi_1 & * \\ & \chi_2 \end{bmatrix}$. Hence χ_1 and χ_2 as subquotients of ρ' are also Fontaine-Laffaille. Again arguing as in the proof of Proposition 9.5 in [1] we get that 1 and $\bar{\epsilon}$ do not admit any non-trivial infinitesimal Fontaine-Laffaille deformations, so we must have $\chi_1 = 1$ and $\chi_2 = \bar{\epsilon}$. This puts us in the setup of section 6 of [1] with Assumption 6(ii) satisfied. Hence the claim follows from Proposition 7.2 of [1], using Lemma 2.6 above to see that Assumption 6(i) is also satisfied. \square

Let \mathcal{L} be the category of local complete Noetherian \mathbf{Z}_ℓ -algebras with residue field \mathbf{F}_ℓ . Consider deformations $\rho' : G_{\Sigma'} \rightarrow \mathrm{GL}_2(A)$ of $\bar{\rho}$ for A an object of \mathcal{L} which are such that:

- $\det \rho' = \epsilon$;
- ρ' is Fontaine-Laffaille at ℓ .

Since $\bar{\rho}$ has scalar centralizer the above deformation problem is representable (cf. [17], p. 270) by a universal deformation ring R . We write $\sigma : G_{\Sigma'} \rightarrow \mathrm{GL}_2(R)$ for the universal deformation.

Let I be the ideal of reducibility of the universal deformation σ , i.e., I is the smallest ideal $I' \subset R$ such that $\mathrm{tr} \sigma$ is a sum of characters χ_1 and χ_2 mod I' with the property that χ_1 reduces to 1 and χ_2 reduces to $\bar{\epsilon}$ modulo the maximal ideal \mathfrak{m}_R of R .

Theorem 2.9. *Suppose $\mathrm{val}_\ell(\ell_1^2 - 1) = 1$ and $\mathrm{val}_\ell(\ell_i^2 - 1) = 0$ for all $i = 2, 3, \dots, k$. Then $I = \mathfrak{m}_R$.*

Proof. It follows from Proposition 2.1 (and universality of R) that R/I does not admit a surjection to \mathbf{Z}/ℓ^2 . Similarly it follows from Proposition 2.8 that R/I does not admit a surjection to $\mathbf{F}[X]/X^2$. Thus I is the maximal ideal by Lemma 3.5 in [2]. \square

Let us explain one consequence of Theorem 2.9. If A is any object in \mathcal{L} and $\rho : G_{\Sigma'} \rightarrow \mathrm{GL}_2(A)$ is a continuous representation such that

- (i) ρ is Fontaine-Laffaille;
- (ii) $\det \rho = \epsilon$;
- (iii) $\mathrm{tr} \rho = \chi_1 + \chi_2$ for some Galois characters $\chi_1, \chi_2 : G_{\Sigma'} \rightarrow A^\times$ with $\chi_1 \equiv 1 \pmod{\mathfrak{m}_A}$ and $\chi_2 \equiv \bar{\epsilon} \pmod{\mathfrak{m}_A}$;
- (iv) $\rho = \bar{\rho} \pmod{\mathfrak{m}_A}$,

then the \mathbf{Z}_ℓ -algebra map $\phi : R \rightarrow A$ whose existence follows from universality of R factors through (by the definition of I) a \mathbf{Z}_ℓ -algebra map $R \twoheadrightarrow \mathbf{F}_\ell = R/I \xrightarrow{\phi} A$ such that ρ is isomorphic to $\bar{\rho}$ viewed as a $A[G_{\Sigma'}]$ -module via ϕ .

Corollary 2.10. *Let $k = 2$. Suppose $\mathrm{val}_\ell(\ell_1^2 - 1) = 1$ and $\mathrm{val}_\ell(\ell_2^2 - 1) = 0$. Let \mathbf{T} be the Hecke algebra as in Section 1 and \mathfrak{m} a maximal Eisenstein ideal as in Theorem 1.2. Then there does not exist a Galois representation $\rho : G_{\Sigma'} \rightarrow \mathrm{GL}_2(\mathbf{T}/\mathfrak{m}^2)$ such that ρ satisfies (i)-(iv) as above with $A = \mathbf{T}/\mathfrak{m}^2$.*

Proof. Suppose ρ as in the statement exists. Note that $\mathbf{T}/\mathfrak{m}^2$ is an object of \mathcal{L} . Then by universality of R we get a \mathbf{Z}_ℓ -algebra map $\phi : R \rightarrow \mathbf{T}/\mathfrak{m}^2$. Let us first see that this map is surjective. Indeed, viewing \mathbf{T} as the Hecke algebra acting on the space of weight 2 cusp forms of level $\Gamma_0(\ell_1 \ell_2)$ we first complete it at the ideal \mathfrak{m} and note that $\mathbf{T}_\mathfrak{m}$ is an element of \mathcal{L} (since $\mathbf{T}_\mathfrak{m}/\mathfrak{m}\mathbf{T}_\mathfrak{m} = \mathbf{T}/\mathfrak{m}\mathbf{T} = \mathbf{F}_\ell$). For every minimal prime \mathfrak{P} of $\mathbf{T}_\mathfrak{m}$ we have a canonical map $\mathbf{T}_\mathfrak{m} \twoheadrightarrow \mathbf{T}_\mathfrak{m}/\mathfrak{P}$ given by sending operators T_r and U_r to the eigenvalues of the corresponding cusp form. It follows from Proposition A.2.3 and A.2.2(2) in [27] that the algebra $\mathbf{T}_\mathfrak{m}$ is generated by the operators T_r for $r \nmid \ell \ell_1 \ell_2$. Indeed, our assumptions on the valuations of the ℓ_i imply that the Atkin-Lehner signature denoted in [27] by ϵ equals $(-1, 1)$ - this is forced by the condition that the constant term of the relevant Eisenstein series (cf. equation (1.3.1) in [27]) vanishes modulo ℓ . In other words our Hecke algebra $\mathbf{T}_\mathfrak{m}$ equals the Hecke algebra denoted in [27] by $\mathbb{T}_U^{(-1,1),0}$, which in turn equals $\mathbb{T}^{(-1,1),0}$ by

Proposition A.2.3 in [27]. It then follows from Proposition A.2.2 that this last Hecke algebra is generated by T_r for $r \nmid \ell_1 \ell_2$. Thus the intersection of all the minimal primes $\bigcap_{\mathfrak{P}} \mathfrak{P}$ equals 0 as it consists of all the operators T such that $Tf = 0$ for all eigenforms f of \mathbf{T}_m . Hence in particular \mathbf{T}_m injects into $\prod_{\mathfrak{P}} \mathbf{T}_m/\mathfrak{P} = \tilde{\mathbf{T}}_m$, where $\tilde{\mathbf{T}}_m$ is the normalization of \mathbf{T}_m .

We claim that the combined map $R \rightarrow \prod_{\mathfrak{P}} \mathbf{T}_m/\mathfrak{P} = \tilde{\mathbf{T}}_m \supset \mathbf{T}_m$ surjects onto \mathbf{T}_m . This is a standard argument, which we summarize here in our situation. First arguing as in the proof of Proposition 7.13 in [1] using Theorem 2.9 above for the cyclicity of R/I we conclude that R is generated by the set $\{\text{tr } \sigma(\text{Frob}_r) \mid r \notin \Sigma'\}$. Since each of these traces is mapped to T_r under the map $R \rightarrow \tilde{\mathbf{T}}_m$ we see that the image is contained in \mathbf{T}_m . In fact, it equals \mathbf{T}_m as we showed above that \mathbf{T}_m is generated by T_r with $r \nmid \ell_1 \ell_2$.

Having established the surjectivity of $R \rightarrow \mathbf{T}_m$ we now use (iii) above and the definition of I to conclude that the induced surjection $\phi : R \twoheadrightarrow \mathbf{T}/\mathfrak{m}^2$ factors through a \mathbf{Z}_ℓ -algebra map $R \twoheadrightarrow R/I \xrightarrow{\phi} \mathbf{T}/\mathfrak{m}^2$. However, $R/I \cong \mathbf{F}_\ell$ by Theorem 2.9 implying that $\mathfrak{m} = \mathfrak{m}^2$, which is absurd. \square

3. CHARACTER GROUPS OF $J_0(65)$ AS HECKE MODULES

In this section $J := J_0(65)$. In this case, $J = J^{\text{new}}$. Let M_p denote the character group of J at p as defined in the introduction. For $p = 5, 13$, M_p is a free abelian group of rank $\dim(J) = 5$. By the Néron mapping property, the action of the Hecke algebra \mathbf{T} on J extends canonically to an action on the Néron model \mathcal{J} of J over \mathbf{Z}_p . For $p = 5, 13$, \mathbf{T} acts faithfully on $\mathcal{J}_{\mathbf{F}_p}^0$, and hence also on M_p (because J has purely toric reduction at p). The main result of this section is the fact that M_5 and M_{13} are isomorphic as \mathbf{T} -modules. The proof is based on explicit calculations with Brandt matrices; cf. [7].

Remark 3.1. The algebra $\mathbf{T} \otimes \mathbf{Q}$ is semi-simple of dimension 5 over \mathbf{Q} . Since $\mathbf{T} \otimes \mathbf{Q}$ acts faithfully on $M_p \otimes \mathbf{Q}$, $p = 5, 13$, which is also 5-dimensional over \mathbf{Q} , one easily concludes that $M_p \otimes \mathbf{Q}$ is free over $\mathbf{T} \otimes \mathbf{Q}$ of rank 1. Thus, $M_5 \otimes \mathbf{Q} \cong M_{13} \otimes \mathbf{Q}$ as \mathbf{T} -modules, but the isomorphism over \mathbf{Z} is more subtle.

Proposition 3.2. *There are isomorphisms of \mathbf{T} -modules $M_5 \cong M_{13} \cong \mathbf{T}$.*

Proof. The following Magma routine computes the action of T_n on M_5 for a given positive integer n :

```
> B5:= BrandtModule(5, 13);
> M5:= CuspidalSubspace(B);
> Sn:=HeckeOperator(M5, n);
```

The result is an explicit matrix $S_n \in M_5(\mathbf{Z})$. Repeating the same process with the roles of 5 and 13 interchanged, we get another matrix $S'_n \in M_5(\mathbf{Z})$ by which T_n acts on M_{13} (with respect to implicit \mathbf{Z} -bases chosen by the program).

A calculation with discriminants shows that \mathbf{T} , as a free \mathbf{Z} -module of rank 5, is generated by the Hecke operators $T_1, T_2, T_3, T_5, T_{11}$; cf. [10, Sec. 3]. We have

$$S_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad S_2 = \begin{bmatrix} -1 & -1 & 1 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 \\ 2 & -1 & 0 & 0 & -1 \\ -1 & 2 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix},$$

$$S_3 = \begin{bmatrix} 0 & -1 & 0 & 1 & -1 \\ -1 & 0 & 1 & 0 & -1 \\ -1 & 2 & 1 & 0 & -2 \\ 2 & -1 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}, \quad S_5 = \begin{bmatrix} 0 & 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix},$$

$$S_{11} = \begin{bmatrix} 0 & 3 & 0 & -1 & 0 \\ 3 & 0 & -1 & 0 & 0 \\ 1 & -2 & -1 & 2 & 1 \\ -2 & 1 & 2 & -1 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

In Magma, the action of Hecke operators on M_p is defined to be from the right, i.e., as on row vectors. Let $v = [1, 0, 0, 0, 0] \in M_5$, and

$$A := \begin{bmatrix} vS_1 \\ vS_2 \\ vS_3 \\ vS_5 \\ vS_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 & -1 \\ 0 & 3 & 0 & -1 & 0 \end{bmatrix}.$$

One easily verifies that $\det(A) = 1$, hence

$$M_5 = \mathbf{Z}vS_1 + \mathbf{Z}vS_2 + \mathbf{Z}vS_3 + \mathbf{Z}vS_5 + \mathbf{Z}vS_{11} = v\mathbf{T}.$$

Thus, $M_5 \cong \mathbf{T}$ is a free \mathbf{T} -module of rank 1. A similar calculation with M_{13} , gives

$$A' := \begin{bmatrix} vS'_1 \\ vS'_2 \\ vS'_3 \\ vS'_5 \\ vS'_{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & -1 \\ -1 & 0 & 1 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 \\ 1 & -2 & -1 & 0 & 2 \end{bmatrix}.$$

In this case, $\det(A) = -1$, hence again $M_{13} = v\mathbf{T}$. \square

Remark 3.3. The fact that M_5 and M_{13} are free \mathbf{T} -modules is a coincidence (a priori, we don't see a reason for this to happen). To emphasize this point, we note that the dual $M_5^* = \text{Hom}(M_5, \mathbf{Z})$ of M_5 with induces action of \mathbf{T} is not a free \mathbf{T} -module. (On M_5^* the Hecke operator T_n acts by the transpose of the matrix by which it acts on M_5). Indeed, otherwise we get $\mathbf{T} \cong \text{Hom}(\mathbf{T}, \mathbf{Z})$, which implies that the localization of \mathbf{T} at any maximal ideal is Gorenstein in contradiction to [10, Prop. 3.7].

Remark 3.4. The proof of Proposition 3.2 is rather ad hoc. Suppose more generally that we are given two \mathbf{T} -modules M, M' for a Hecke algebra of some level N such that M, M' are free of the same finite rank over \mathbf{Z} and $M \otimes_{\mathbf{Z}} \mathbf{Q} \cong_{\mathbf{T}} M' \otimes_{\mathbf{Z}} \mathbf{Q}$. Also, suppose we are able to compute efficiently the matrices S_n, S'_n by which T_n acts on M and M' , respectively. The question of the integral isomorphism $M \cong_{\mathbf{T}(N)} M'$ is equivalent to the existence of an invertible matrix $S \in \text{GL}_r(\mathbf{Z})$ such that $SS_nS^{-1} = S'_n$ for all $n \geq 1$; here $r = \text{rank}_{\mathbf{Z}}(M)$. In fact, it is enough to find such S that works for all n up to an explicit bound depending on N (the Sturm bound). Despite the elementary nature of this question, computationally it is challenging. The problem of integral conjugacy of matrices is a classical problem related to class groups of orders in number fields (see [11]), and there are algorithms that solve this problem (see [23], [8]), but at the time of writing of this article these

algorithms do not seem to be implemented in any of the standard computational programs, such as `Magma`. (Given two $m \times m$ matrices A and B with rational or integral entries, `Magma` currently can test whether A is conjugate to B in $\mathrm{GL}_m(\mathbf{Z})$ only if $m = 2$.)

Acknowledgements. We are very grateful to Ken Ribet for suggesting that his construction in [21] might lead to a counterexample to Ogg’s conjecture, and for helpful suggestions about the exposition in an earlier version of this paper. We thank Hwajong Yoo for pointing out several misstatements in earlier versions of this paper, and for directing us to the reference [29]. The second author is also grateful to Fu-Tsun Wei for useful discussions related to the topic of this paper.

REFERENCES

1. Tobias Berger and Krzysztof Klosin, *On deformation rings of residually reducible Galois representations and $R = T$ theorems*, *Math. Ann.* **355** (2013), no. 2, 481–518. MR 3010137
2. Frank Calegari, *Eisenstein deformation rings*, *Compos. Math.* **142** (2006), no. 1, 63–83. MR 2196762
3. Seng-Kiat Chua and San Ling, *On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$* , *Proc. Amer. Math. Soc.* **125** (1997), no. 8, 2255–2263. MR 1396972
4. J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. MR 1628193
5. Josep González and Santiago Molina, *The kernel of Ribet’s isogeny for genus three Shimura curves*, *J. Math. Soc. Japan* **68** (2016), no. 2, 609–635. MR 3488137
6. Josep González and Victor Rotger, *Equations of Shimura curves of genus two*, *Int. Math. Res. Not.* (2004), no. 14, 661–674. MR 2038166
7. Benedict H. Gross, *Heights and the special values of L -series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187. MR 894322
8. Fritz J. Grunewald, *Solution of the conjugacy problem in certain arithmetic groups*, Word problems, II (Conf. on Decision Problems in Algebra, Oxford, 1976), *Stud. Logic Foundations Math.*, vol. 95, North-Holland, Amsterdam-New York, 1980, pp. 101–139. MR 579942
9. David Helm, *On maps between modular Jacobians and Jacobians of Shimura curves*, *Israel J. Math.* **160** (2007), 61–117. MR 2342491
10. Krzysztof Klosin and Mihran Papikian, *On Ribet’s isogeny for $J_0(65)$* , *Proc. Amer. Math. Soc.* **146** (2018), no. 8, 3307–3320. MR 3803657
11. Claiborne G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, *Ann. of Math. (2)* **34** (1933), no. 2, 313–316. MR 1503108
12. San Ling and Joseph Oesterlé, *The Shimura subgroup of $J_0(N)$* , *Astérisque* (1991), no. 196–197, 6, 171–203 (1992), *Courbes modulaires et courbes de Shimura* (Orsay, 1987/1988). MR 1141458
13. B. Mazur, *Modular curves and the Eisenstein ideal*, *Inst. Hautes Études Sci. Publ. Math.* (1977), no. 47, 33–186 (1978). MR 488287
14. A. P. Ogg, *Mauvaise réduction des courbes de Shimura*, *Séminaire de théorie des nombres*, Paris 1983–84, *Progr. Math.*, vol. 59, Birkhäuser Boston, Boston, MA, 1985, pp. 199–217. MR 902833
15. Masami Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, *Tokyo J. Math.* **37** (2014), no. 2, 273–318. MR 3304683
16. Mihran Papikian, *On Jacquet-Langlands isogeny over function fields*, *J. Number Theory* **131** (2011), no. 7, 1149–1175. MR 2782835
17. R. Ramakrishna, *On a variation of Mazur’s deformation functor*, *Compositio Math.* **87** (1993), no. 3, 269–286. MR 1227448
18. K. A. Ribet, *On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms*, *Invent. Math.* **100** (1990), no. 2, 431–476. MR 1047143
19. Kenneth Ribet, *Sur les variétés abéliennes à multiplications réelles*, *C. R. Acad. Sci. Paris Sér. A-B* **291** (1980), no. 2, A121–A123. MR 604997

20. Kenneth A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. Math. (2) **101** (1975), 555–562. MR 0371903
21. ———, *Multiplicities of Galois representations in Jacobians of Shimura curves*, Festschrift in honor of I. I. Piatetski-Shapiro on the occasion of his sixtieth birthday, Part II (Ramat Aviv, 1989), Israel Math. Conf. Proc., vol. 3, Weizmann, Jerusalem, 1990, pp. 221–236. MR 1159117
22. Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study. MR 1749177
23. R. A. Sarkisjan, *The conjugacy problem for collections of integral matrices*, Mat. Zametki **25** (1979), no. 6, 811–824, 956. MR 540237
24. E. Urban, *On residually reducible representations on local rings*, J. Algebra **212** (1999), no. 2, 738–742. MR 1676863
25. V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu **4** (2005), no. 2, 281–316. MR 2135139
26. Kestutis Česnavičius, *The Manin constant in the semistable case*, Compos. Math. **154** (2018), no. 9, 1889–1920. MR 3867287
27. Preston Wake and Carl Wang-Erickson, *The Eisenstein ideal with squarefree level*, Preprint (2018), arXiv: 1804.06400.
28. Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575
29. Hwajong Yoo, *On rational Eisenstein primes and the rational cuspidal groups of modular Jacobian varieties*, Trans. Amer. Math. Soc. (to appear).
30. ———, *The index of an Eisenstein ideal and multiplicity one*, Math. Z. **282** (2016), no. 3-4, 1097–1116. MR 3473658
31. ———, *Rational torsion points on Jacobians of Shimura curves*, Bull. Lond. Math. Soc. **48** (2016), no. 1, 163–171. MR 3455760

DEPARTMENT OF MATHEMATICS, QUEENS COLLEGE, CITY UNIVERSITY OF NEW YORK, 65-30
 KISSENA BLVD FLUSHING, NY 11367, USA
E-mail address: `kklosin@qc.cuny.edu`

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA
 16802, USA
E-mail address: `papikian@psu.edu`