

COMPUTING RESIDUAL REPRESENTATIONS OF ABELIAN THREEFOLDS WITH IMAGINARY MULTIPLICATION

SHIVA CHIDAMBARAM AND PIP GOODMAN

ABSTRACT. Let M be an imaginary quadratic field. Let A be a polarised abelian threefold defined over M with geometric endomorphism algebra isomorphic to M . We study residual Galois representations attached to A . In particular, we describe the endomorphism field and the natural restrictions placed on the residual representations by their endomorphisms. We then devise criteria for the image of residual Galois representations to be large, and provide efficient algorithms suitable for large scale calculations.

Subsequently, we apply this algorithm to millions of curves in several families, whose Jacobians are abelian threefolds with imaginary multiplication, and to Sutherland’s dataset of 7-smooth Picard curves. We produce an explicit example of a Picard curve which appears to have an isogeny of degree 13 defined over $\mathbb{Q}(\zeta_3)$. The Jacobians of all other curves, in the range of our computation with endomorphism algebra M , have mod- ℓ image as large as possible for any prime $\ell > 7$. This allows us to realise the group $\Gamma\mathrm{U}_3(\ell)$ of unitary semisimilitudes as a Galois group over $\mathbb{Q}$ for all $\ell \not\equiv 1, 25, 121 \pmod{168}$.

Our algorithms also led us to the discovery of several interesting rational families of Picard curves whose generic members appear to have endomorphism algebra of dimension 6 which is not a CM field. These represent curves on the Picard modular surface and appear to be Shimura curves. Some of them appear to parametrise non-principally polarised abelian surfaces with quaternionic multiplication.

1. INTRODUCTION

Let M be an imaginary quadratic field and fix an algebraic closure $\overline{M}$ of M . In this article we study the residual representations associated to abelian threefolds A defined over M , with a fixed polarisation and geometric endomorphism algebra isomorphic to M , i.e., $\mathrm{End}^0(A_{\overline{M}}) := \mathrm{End}(A_{\overline{M}}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong M$.

The main contribution of this paper is an algorithm which given sufficiently many characteristic polynomials of Frobenius elements for such an abelian variety returns a small set of primes outside of which the residual mod- ℓ representations are as large as possible. Moreover, the algorithm is sufficiently fast that it may be applied to large datasets of such abelian varieties.

The following theorem is obtained as a consequence. Recall that $\Gamma\mathrm{U}_3(\ell)$ denotes the group of semisimilitudes of a non-degenerate hermitian pairing

2020 *Mathematics Subject Classification.* Primary 11F80; 11G10, 11G15, 14K15.

on a 3 dimensional vector space over $\mathbb{F}_{\ell^2}$ [KL90, page 11, page 15 Table 2.1.B].

Theorem 1.1 ($\subseteq$ Theorem 6.2). *Let ℓ be a prime, not congruent to 1, 25 or 121 modulo 168. Then $\Gamma\mathrm{U}_3(\ell)$ is a Galois group over $\mathbb{Q}$.*

The algorithms developed in Section 5 do not require $\mathrm{End}^0(A_{\overline{M}}) \cong M$ and in fact may be applied to any abelian threefold A with imaginary multiplication by M of signature $(2, 1)$ (see Definitions 2.2 and 2.4). However, if $\mathrm{End}^0(A_{\overline{M}}) \not\cong M$, then these algorithms will fail. This turns out to be an effective way to discover such abelian varieties. Indeed, using our algorithms we were able to discover several families of curves whose Jacobians have endomorphism algebras properly containing M .

We let B_d denote the quaternion algebra over $\mathbb{Q}$ with discriminant d .

Theorem 1.2. *Let $a \in \mathbb{Q}$ have height at most 20. Let f_a be one of the polynomials defined in the table below. Suppose f_a is separable. Let A be the Jacobian of the smooth affine curve defined by $y^3 = f_a(x)$. Then $\mathrm{End}^0(A_{\overline{\mathbb{Q}}})$ contains the $\mathbb{Q}$ -algebra listed in the same row as $f_a(x)$ below.*

$f_a(x)$	$\mathbb{Q}$ -algebra
$x(x^3 + 12x^2 + ax + 64)$	$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q})$
$((x+1)^2 - a(5a+1))((x-1)^2 + 27a(a+1))$	$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q})$
$(x^2 - 27a(a-1)(3a^2 - 3a + 32))^2 + 2916a^2(a-1)(x - (a-1)(7a-16))^2$	$\mathbb{Q}(\zeta_3) \times B_{15}$
$(x-3a)((x+a)^3 - a(17a^3 + 6a^2 + 24a + 8)(x+a) + a^2(27a^4 + 14a^3 + 60a^2 + 24a + 32))$	$\mathbb{Q}(\zeta_3) \times B_6$

We believe that for any $a \in \overline{\mathbb{Q}}$ such that f_a is separable, the geometric endomorphism algebra of the Jacobian of $y^3 = f_a(x)$ will always contain the corresponding $\mathbb{Q}$ -algebra listed above and moreover be generically equal to it.

Let us now return to our initial motivation for studying this question. Serre’s Open Image Theorem [Ser72] tells us that a given elliptic curve E without complex multiplication defined over a number field K satisfies $\mathrm{Gal}(K(E[\ell])/K) \cong \mathrm{GL}_2(\ell)$ for all but finitely many primes ℓ . For an elliptic curve $E/\mathbb{Q}$ without complex multiplication it is widely believed that $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \cong \mathrm{GL}_2(\ell)$ for all $\ell > 37$. The truth of this statement is widely known as “Serre’s Uniformity Conjecture”.

Zywina and Sutherland [Zyw20; Sut16] have developed algorithms which, provided with sufficiently many traces of Frobenius for a given elliptic curve $E/\mathbb{Q}$ without complex multiplication, compute $\mathrm{Gal}(\mathbb{Q}(E)/\mathbb{Q})$ as a subgroup of $\mathrm{GL}_2(\ell)$ (up to conjugation) for any prime ℓ . This in turn gives a large amount of data supporting Serre’s Uniformity Conjecture. Moreover, for $\ell \leq 37$, they produce an explicit list of possible small images, i.e., sets of couples (G, ℓ) consisting of a group G and a prime ℓ such that $G \cong \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \subsetneq \mathrm{GL}_2(\ell)$ for some elliptic curve E and conjecture that these are the only non-maximal mod- ℓ images possible. There has been a lot of recent progress on these conjectures coming from studying the associated modular curves, see for example [Bal+19; RSZ22; Bal+23; FL26].

The study of the analogous problem for principally polarised abelian surfaces $A/\mathbb{Q}$ with $\text{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$ was initiated by Dieulefait [Die02]. More specifically, he described an algorithm which given sufficiently many characteristic polynomials of Frobenius, returns a small finite set of primes, outside of which $\text{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}) \cong \text{GSp}_4(\ell)$. His algorithm was recently implemented in SageMath by the authors of [Ban+24]. This implementation is in turn a key input for the main algorithm of [Bom+24] which computes the isogeny class of a given principally polarised abelian surface.

It is a natural question to understand what the possible residual images of principally polarised abelian surfaces are. Determining points on the moduli spaces in question, which have dimension three, seems to be far out of reach from current methods. We seem, however, to be at the dawn of provably determining rational points on surfaces [CP23]. It is our hope that the data provided in Section 6 will aid and inform our understanding of which Picard modular surfaces should have either infinitely or finitely many rational points, thus identifying interesting testing ground for the determination of rational points on surfaces.

Let us now briefly summarise the structure of the paper. In Section 2, we analyse the endomorphism structure of abelian threefolds A over a number field K such that $\text{End}^0(A_{\overline{K}}) \cong M$. Section 3 covers the group theoretic preliminaries we require for determining the restrictions on the images of the residual representations. In Section 4 we then make these restrictions explicit; they allow us in particular to define mod- λ representations and show in Corollary 4.3 that their images are contained in the group $\text{CL}_3^\varepsilon(\ell)$ (see Section 1.1 for the notation). The action of inertia at ℓ on $A[\ell]$ is then studied in Section 4.3. This in particular allows us to prove surjectivity results for the determinants of the mod- λ representations. We begin Section 5 by analysing the maximal subgroups of $\text{CL}_3^\varepsilon(\ell)$ and then go on to give tests for the containment of the images of mod- λ representations in these maximal subgroups. Finally in Section 6, we list the results obtained from our implementation of algorithms developed in Section 5.

Magma [BCP97] implementations of our algorithms, and collected data are available in the GitHub repo [CG26].

1.1. Notation. Our notation for the classical groups is taken to reflect that of [BHR13; KL90]. Let V be a vector space over a field $\mathbb{F}$ and $\langle, \rangle: V \times V \rightarrow \mathbb{F}$ a bilinear map. There is a chain of subgroups associated to $\langle, \rangle$:

$$S \leq I \leq C \leq \Gamma$$

where Γ is the set of semisimilitudes of $(V, \langle, \rangle)$, i.e., semilinear maps which preserve $\langle, \rangle$ up to a constant; C is the set of similitudes of $(V, \langle, \rangle)$, i.e., the linear maps contained in Γ ; I is the set of isometries of $(V, \langle, \rangle)$, i.e., elements of C preserving $\langle, \rangle$; and S is the kernel of $\det: I \rightarrow \mathbb{F}^*$.

If $\langle, \rangle$ is identically zero, then $S = \text{SL}(V)$, $I = C = \text{GL}(V)$. If $\langle, \rangle$ is a non-degenerate Hermitian pairing then $S = \text{SU}(V)$, $I = \text{GU}(V)$, $C = \text{CU}(V)$ and $\Gamma = \Gamma\text{U}(V)$. If $\langle, \rangle$ is a non-degenerate symplectic pairing then $S = I = \text{Sp}(V)$ and $C = \text{GSp}(V)$. We also write $\text{SL}^+ = \text{SL}$, $\text{GL}^+ = \text{CL}^+ = \text{GL}$ as well as $\text{SL}^- = \text{SU}$, $\text{GL}^- = \text{GU}$ and $\text{CL}^- = \text{CU}$.

We write $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_6, \mathcal{C}_8, \mathcal{S}$ for the Aschbacher classes of maximal subgroups as defined in [BHR13, pp. 378-379].

1.2. Acknowledgments: We are grateful to Drew Sutherland for helping start our collaboration and his constant support which has been invaluable for this work. We also thank him for helpful discussions, and for sharing his dataset of 7-smooth Picard curves. We thank Edgar Costa for his help with the endomorphisms package, and his inputs for extending the scope of this work. We are also grateful to Francesc Fit , Davide Lombardo, Bjorn Poonen and Ramin Takloo-Bighash for helpful conversations.

SC was supported by Simons Foundation grant 550033 during part of this project and also partially supported by NSF grant DMS-2301386.

PG was supported the Deutsche Forschungsgemeinschaft (DFG) project grant STO 299/18-2 (AOBJ: 686837), by the Spanish Ministry of Science and Innovation via the grant ‘‘Abelian varieties, L-functions, and rational points’’ (code PID2022-137605NB-I00) and the Max-Planck-Institut f r Mathematik.

The authors thank all the institutions at which they were hosted, whilst they carried out work on this project: Universit t Bayreuth, Universitat de Barcelona, Max-Planck-Institut f r Mathematik, Massachusetts Institute of Technology, and University of Wisconsin-Madison.

2. THE ENDOMORPHISM STRUCTURE

Let g be a positive integer, K a number field and $\overline{K}$ a fixed algebraic closure of K and $M/\mathbb{Q}$ a quadratic extension. The ultimate goal of this section is to define a class of abelian varieties generalising those of Jacobians of Picard curves. Recall that the endomorphism algebra of an abelian variety is a semisimple $\mathbb{Q}$ -algebra. We only wish to consider abelian varieties such that every simple $\mathbb{Q}$ -subalgebra of their geometric endomorphism algebra contains M . For this reason, we make the following definition:

Definition 2.1 (Unital algebra embedding). Given $\mathbb{Q}$ -algebras X, Y with multiplicative identities and a map $\iota: X \rightarrow Y$. We say ι is a unital algebra embedding, if it is injective, is a $\mathbb{Q}$ -linear map, preserves multiplication and sends the multiplicative identity of X to that of Y .

We shall now employ ideas from the theory of CM abelian varieties to study the endomorphism structure of a g -dimensional abelian variety A over K equipped with a unital algebra embedding $\iota: M \hookrightarrow \text{End}^0(A_{\overline{K}}) = \text{End}(A_{\overline{K}}) \otimes \mathbb{Q}$.

We first recall some fundamental notions. For an extension K'/K , we let $\Omega^1(A_K)$ denote the space of invariant differential forms of $A_{K'}$. It is a g -dimensional K' -vector space. An endomorphism f of A acts on $\Omega^1(A_{K'})$ by pullback f^* . Note that pullback reverses composition. This action extends $\mathbb{Q}$ -linearly to a faithful representation

$$\pi_{A, K', \text{an}}: \text{End}^0(A_{K'}) \rightarrow \text{End}_{K'}(\Omega^1(A_{K'})), \quad f \mapsto f^*,$$

which we call the analytic representation.

Let $\varphi, \bar{\varphi}$ denote the two embeddings $M \hookrightarrow \overline{K}$. As $\pi_{A, \overline{K}, \text{an}} \circ \iota$ is a unital algebra embedding and $M \otimes_{\mathbb{Q}} \overline{K} \cong \overline{K} \times \overline{K}$ the space $\Omega^1(A_{\overline{K}})$ is the direct

sum of the two eigenspaces

$\Omega_\varphi = \{\omega : \iota(\alpha)^*\omega = \alpha^\varphi\omega \ \forall \alpha \in M\}$ and $\Omega_{\bar{\varphi}} = \{\omega : \iota(\alpha)^*\omega = \alpha^{\bar{\varphi}}\omega \ \forall \alpha \in M\}$, where we write α^φ for $\varphi(\alpha)$.

Definition 2.2 (Signature). The tuple $(r, s) = (\dim \Omega_\varphi, \dim \Omega_{\bar{\varphi}})$ is called the signature of (A, ι) with respect to the ordering $(\varphi, \bar{\varphi})$. We always assume φ and $\bar{\varphi}$ are chosen such that $r \geq s$.

When the existence of ι is implicit from context, we shall instead refer to the signature of (A, M) .

Equivalently, if we choose an eigenbasis $\omega_1, \dots, \omega_g$ of $\Omega^1(A_{\bar{K}})$, so that for each $1 \leq i \leq g$, M acts on ω_i through an embedding $\varphi_i : M \hookrightarrow \bar{K}$, i.e., $\iota(\alpha)^*\omega_i = \alpha^{\varphi_i}\omega_i$ for all $\alpha \in M$, then φ occurs r times in the multiset $\{\varphi_i | 1 \leq i \leq g\}$ and $\bar{\varphi}$ occurs s times. In other words, the characteristic polynomial of $\iota(\alpha)^*$ is $\prod_{i=1}^g (x - \alpha^{\varphi_i}) = (x - \alpha^\varphi)^r (x - \alpha^{\bar{\varphi}})^s$.

Proposition 2.3. *Let M be any quadratic field. Let $g \geq 1$ be odd, and A/K be a g -dimensional abelian variety equipped with an isomorphism $\iota : M \xrightarrow{\sim} \text{End}^0(A_{\bar{K}})$.*

Then M is imaginary quadratic, and MK is the minimal extension of K over which all endomorphisms of A are defined.

Proof. Let $\mathcal{O} = \text{End}(A_{\bar{K}})$, so that $\mathcal{O}$ is an order in M . Let (r, s) with $r \geq s$ be the signature of A with respect to the embeddings $\varphi, \bar{\varphi}$ of M . Since $r + s = g$ is odd, we have $r \neq s$.

We first show that M is imaginary quadratic. The $2g$ -dimensional $\mathbb{Q}$ -vector space $H_1(A(\mathbb{C}), \mathbb{Q})$ carries a natural action of M through $\iota : M \cong \text{End}^0(A_{\bar{K}})$. Since ι is a unital algebra embedding, this makes $H_1(A(\mathbb{C}), \mathbb{Q})$ a vector space over M of dimension g , so the multiplicity of each of φ and $\bar{\varphi}$ in $H_1(A(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$ is g . On the other hand, by [BL04, Prop. 1.2.3], we know that there is an isomorphism of $\mathbb{C}[\text{End}^0(A_{\bar{K}})]$ -representations between $H_1(A(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$ and the direct sum of the analytic representation $\pi_{A, \mathbb{C}, \text{an}}$ and its complex conjugate $\bar{\pi}_{A, \mathbb{C}, \text{an}}$. If M were real quadratic, both φ and $\bar{\varphi}$ would be real, so that $\bar{\pi}_{A, \mathbb{C}, \text{an}} = \pi_{A, \mathbb{C}, \text{an}}$. This would imply that φ and $\bar{\varphi}$ have multiplicity $2r$ and $2s$ in $H_1(A(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$, giving $2r = g = 2s$, which is absurd.

Let L/K be a finite extension. It is enough to prove that all endomorphisms of A are defined over L if and only if $M \subseteq L$.

Suppose that all endomorphisms of A are defined over L . Since $\iota(\alpha)^*$ is L -linear on $\Omega^1(A_L)$, its trace lies in L . Calculating it over $\bar{K}$ using the signature,

$$\text{Tr}(\iota(\alpha)^*) = r\alpha^\varphi + s\alpha^{\bar{\varphi}} = (r - s)\alpha^\varphi + s\text{Tr}_{M/\mathbb{Q}}(\alpha).$$

Since $r \neq s$, we find that $\alpha^\varphi \in L$. This shows that $M = \varphi(M) \subseteq L$.

Conversely, suppose that $M \subseteq L$. The absolute Galois group G_L acts on $\text{End}^0(A_{\bar{K}}) \cong M$ by ring automorphisms, leading to a homomorphism

$$\varrho : G_L \rightarrow \text{Gal}(M/\mathbb{Q})$$

defined by $\iota(\alpha)^\sigma = \iota(\alpha^{\varrho(\sigma)})$. Consider an eigenbasis $\{\omega_i | 1 \leq i \leq g\}$ of $\Omega^1(A_{\bar{K}})$, with corresponding embeddings φ_i . The group G_L acts on $\Omega^1(A_{\bar{K}}) =$

$\Omega^1(A_L) \otimes_L \overline{K}$ via its action on $\overline{K}$, and $\{\omega_i^\sigma | 1 \leq i \leq g\}$ is another basis for any $\sigma \in G_L$. We have

$$(\iota(\alpha)^\sigma)^* \omega_i^\sigma = (\iota(\alpha)^* \omega_i)^\sigma = \sigma(\alpha^{\varphi_i}) \omega_i^\sigma.$$

Since $\alpha^{\varphi_i} \in \varphi_i(M) = M \subseteq L$, we know $\sigma(\alpha^{\varphi_i}) = \alpha^{\varphi_i}$. So the characteristic polynomial of $(\iota(\alpha)^\sigma)^*$ is $\prod_i (x - \alpha^{\varphi_i})$. But the characteristic polynomial of $(\iota(\alpha^{\varrho(\sigma)}))^*$ is $\prod_i (x - \alpha^{\varrho(\sigma)\varphi_i})$. If $\varrho(\sigma)$ is not the identity, α^φ will be a root with multiplicity r of the first polynomial and multiplicity s of the second. Since $r \neq s$, we deduce that $\varrho(\sigma) = 1 \in \text{Gal}(M/\mathbb{Q})$ for all $\sigma \in G_L$. This shows that all the endomorphisms of A are defined over L . $\square$

Definition 2.4 (Imaginary multiplication). Let A/K be an abelian variety and M an imaginary quadratic field. If there exists a unital algebra embedding $\iota: M \hookrightarrow \text{End}^0(A_{KM})$, then we shall say that A has potential imaginary multiplication by (M, ι) .

Furthermore, we say that A has imaginary multiplication by (M, ι) if $\iota(M) \subseteq \text{End}^0(A)$.

The next proposition is originally due to Shimura [Shi63] as part of a more general result, and is also given as [BL04, Exercise 9.10 (3)]. We provide a concise proof in the specific case we require to aid readability.

Proposition 2.5. *Let M be an imaginary quadratic field, and A/K be a g -dimensional abelian variety with imaginary multiplication by (M, ι) . If the signature of (A, ι) is $(g, 0)$, then A is geometrically isogenous to E^g for an elliptic curve E/M with complex multiplication by M .*

Proof. We may write $A(\mathbb{C}) = \mathbb{C}^g / \Lambda$ some lattice Λ in $\mathbb{C}^g$. Let $\pi := \pi_{A, \mathbb{C}, \text{an}}$ denote the analytic representation of $\text{End}(A)$ with respect to this analytic coordinate system.

After possibly replacing A by an isogenous abelian variety, we may assume $\iota(M) \cap \text{End}(A) = \iota(\mathcal{O}_M)$, where $\mathcal{O}_M$ is the maximal order in M . To simplify notation, let us identify $\iota(\mathcal{O}_M)$ with $\mathcal{O}_M$. The lattice Λ is a finitely generated torsion-free $\mathcal{O}_M$ -module under π . By the structure theorem for such modules over Dedekind domains [Bro24, Prop. 10.2.1], we may write $\Lambda = \pi(I_1)x_1 + \pi(I_2)x_2 + \dots \pi(I_g)x_g$ for some ideals I_n of $\mathcal{O}_M$ and $x_n \in \mathbb{C}^g$ for $1 \leq n \leq g$.

Write $x_n = (x_{n,1}, x_{n,2}, \dots, x_{n,g})$. Since A is of signature $(g, 0)$, there is some embedding $\varphi: M \hookrightarrow \mathbb{C}$ such that for any $\alpha \in \mathcal{O}_M$,

$$\pi(\alpha)x_n = (\varphi(\alpha)x_{n,1}, \varphi(\alpha)x_{n,2}, \dots, \varphi(\alpha)x_{n,g}).$$

Thus $\pi(\alpha)x_n = \varphi(\alpha)x_n$ where $\varphi(\alpha) \in \mathbb{C}$ is a scalar. As $\mathbb{R} \otimes \varphi(I_n) \cong \mathbb{C}$, we see that $(\mathbb{R} \otimes \pi(I_n)x_n) / \pi(I_n)x_n \cong (\mathbb{R} \otimes \varphi(I_n)x_n) / \varphi(I_n)x_n \cong \mathbb{C} / \varphi(I_n)$.

Define a $\mathbb{C}$ -linear map $T: \mathbb{C}^g \rightarrow \mathbb{C}^g$ by $x_n \mapsto e_n$ (where e_n is 1 in the n -th component and zero elsewhere). As Λ is a lattice in $\mathbb{C}^g$, $x_1, x_2, \dots, x_g$ are linearly independent over $\mathbb{C}$ and thus T is invertible. It follows that T induces a biholomorphic map

$$\mathbb{C}^g / \Lambda \rightarrow \mathbb{C} / \varphi(I_1) \times \mathbb{C} / \varphi(I_2) \times \dots \times \mathbb{C} / \varphi(I_g).$$

The $\mathbb{C} / \varphi(I_n)$ are isogenous elliptic curves with CM by $\mathcal{O}_M$ (see for example [Sil94, Chapter II, §1], or [Shi98, Chapter II, Thm. 2] and its corollary). $\square$

Corollary 2.6. *Let M be an imaginary quadratic field and A/K be an abelian threefold with endomorphism algebra $\text{End}^0(A)$ isomorphic to M . Then the signature of (A, M) is $(2, 1)$.*

3. GROUP THEORETIC PRELIMINARIES

Let $g \geq 2$ be an integer and ℓ a prime number. In this section, V denotes a $2g$ -dimensional vector space over $\mathbb{F}_\ell$ equipped with a non-degenerate alternating pairing $\langle, \rangle: V \times V \rightarrow \mathbb{F}_\ell$. We let $\text{GSp}(V)$ denote the similitude group of $\langle, \rangle$. That is, $\text{GSp}(V)$ is the group of $\mathbb{F}_\ell$ -linear maps $V \rightarrow V$ such that for every $\sigma \in \text{GSp}(V)$, there exists a constant $\chi(\sigma)$ such that for any $v, w \in V$, we have:

$$\langle \sigma v, \sigma w \rangle = \chi(\sigma) \langle v, w \rangle.$$

It is easy to check that the map $\chi: \text{GSp}(V) \rightarrow \mathbb{F}_\ell^*$ defined by $\sigma \mapsto \chi(\sigma)$ is a homomorphism. We define $\text{Sp}(V)$ to be the isometry group of $\langle, \rangle$, in other words, the kernel of χ .

We shall now investigate the centralisers of certain elements in $\text{GSp}(V)$ (see Propositions 3.1, 3.3). The results presented here are almost certainly well-known to group theorists, however we were unable to find an adequate reference for them. The reader looking to read more about related questions may wish to consult [Spr51; Wal63; DLO25].

In the following we denote the transpose of a matrix T by T^t and its inverse transpose by T^{-t} .

Proposition 3.1. *Suppose $\alpha \in \text{GSp}(V)$ has a reducible minimal polynomial m_α of degree 2 with distinct roots, and satisfies $m_\alpha(0) = \chi(\alpha)$. Then the centraliser $C_{\text{GSp}(V)}(\alpha)$ of α in $\text{GSp}(V)$ admits an isomorphism:*

$$\varphi: C_{\text{GSp}(V)}(\alpha) \xrightarrow{\sim} \mathbb{F}_\ell^* \times \text{GL}_g(\ell)$$

sending $C_{\text{GSp}(V)}(\alpha) \cap \text{Sp}(V)$ to $\{1\} \times \text{GL}_g(\ell)$.

Furthermore, writing $m_\alpha = \phi\phi'$ with $\deg \phi = \deg \phi' = 1$ and $V_\phi = \ker(\phi(\alpha))$, $V_{\phi'} = \ker(\phi'(\alpha))$:

- i) the natural action of $C_{\text{GSp}(V)}(\alpha)$ on V preserves both V_ϕ and $V_{\phi'}$.
- ii) Both V_ϕ and $V_{\phi'}$ are maximal totally isotropic subspaces of V .
- iii) We may take φ so that the natural action of $C_{\text{GSp}(V)}(\alpha)$ on V translates via φ to the action of $(\mu, T) \in \mathbb{F}_\ell^* \times \text{GL}_g(\ell)$ on V_ϕ as μT and on $V_{\phi'}$ as T^{-t} .

Moreover, taking φ so that it satisfies iii) and letting $\gamma' \in \text{GSp}(V)$ denote an element which exchanges V_ϕ and $V_{\phi'}$, we may extend φ to an isomorphism

$$\langle \gamma', C_{\text{GSp}(V)}(\alpha) \rangle \xrightarrow{\sim} (\mathbb{F}_\ell^* \times \text{GL}_g(\ell)) \rtimes \langle \gamma' \rangle$$

where $\gamma(\mu, T) = (\mu, \mu^{-1}T^{-t})$.

Proof. Suppose first that m_α is reducible. By assumption we may write $m_\alpha(x) = (x - a)(x - \chi(\alpha)a^{-1})$ for some $a \in \mathbb{F}_\ell^*$ with $a \neq \chi(\alpha)a^{-1}$. Let $v, w \in V$ be eigenvectors of α with eigenvalues a, b respectively. We have

$$\chi(\alpha)b^{-1}\langle v, w \rangle = \chi(\alpha)\langle v, \alpha^{-1}w \rangle = \langle \alpha v, w \rangle = a\langle v, w \rangle.$$

Thus either $\langle v, w \rangle = 0$ or $b = \chi(\alpha)a^{-1}$. Hence we see that the restriction of $\langle, \rangle$ to the eigenspace $V_a := \ker(\alpha - a)$ is trivial. Similarly, the restriction of $\langle, \rangle$ to the eigenspace $V_{\chi(\alpha)a^{-1}} := \ker(\alpha - \chi(\alpha)a^{-1})$ is trivial.

It follows that we may take a basis $e_1, \dots, e_g$ of V_a such that $\langle e_i, e_j \rangle = 0$ for all i, j and a basis $f_1, \dots, f_g$ of $V_{\chi(\alpha)a^{-1}}$ such that $\langle f_i, f_j \rangle = 0$ and $\langle e_i, f_j \rangle = \delta_{ij}$ for all i, j where $\delta_{ij} = 1$ if $i = j$ and 0 otherwise.

Let $\sigma \in C_{\mathrm{GSp}(V)}(\alpha)$. Note that as σ commutes with α it preserves its eigenspaces. Write $T \in \mathrm{GL}_g(\ell)$ (resp. $S \in \mathrm{GL}_g(\ell)$) for the matrix obtained by letting σ act on the basis $e_1, \dots, e_g$ (resp. $f_1, \dots, f_g$). The condition that σ is a similitude of $\langle, \rangle$ with similitude factor $\chi(\sigma)$ may then be expressed as:

$$\begin{pmatrix} T^t & 0 \\ 0 & S^t \end{pmatrix} \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \begin{pmatrix} T & 0 \\ 0 & S \end{pmatrix} = \chi(\sigma) \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

From which it follows that if $\chi(\sigma) = 1$, then $S = T^{-t}$. In fact, we deduce that the map $\mathrm{GL}_g(\ell) \rightarrow C_{\mathrm{GSp}(V)}(\alpha) \cap \mathrm{Sp}(V)$ defined by $X \mapsto \begin{pmatrix} X & 0 \\ 0 & X^{-t} \end{pmatrix}$ is an isomorphism. Let $\mu \in \mathbb{F}_\ell^*$. Observe that

$$\begin{pmatrix} \mu I_g & 0 \\ 0 & I_g \end{pmatrix} \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \begin{pmatrix} \mu I_g & 0 \\ 0 & I_g \end{pmatrix} = \mu \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Since $\mathrm{GSp}(V)$ is generated by $\mathrm{Sp}(V)$ and the linear map defined by $e_i \mapsto \mu e_i$, $f_i \mapsto f_i$, we deduce $C_{\mathrm{GSp}(V)}(\alpha) \cong \mathbb{F}_\ell^* \times \mathrm{GL}_g(\ell)$.

We shall now prove the final statement. Let us write γ' as $\begin{pmatrix} 0 & T' \\ S' & 0 \end{pmatrix}$ with respect to the basis $e_1, \dots, e_g, f_1, \dots, f_g$. After possibly multiplying γ' by a matrix of the form $\begin{pmatrix} \mu I_g & 0 \\ 0 & I_g \end{pmatrix}$, we may assume the following equation holds:

$$\begin{pmatrix} 0 & (S')^t \\ (T')^t & 0 \end{pmatrix} \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \begin{pmatrix} 0 & T' \\ S' & 0 \end{pmatrix} = \begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}$$

from which we deduce $S' = (T')^{-t}$. Observing that conjugation by

$$\begin{pmatrix} (T')^{-1} & 0 \\ 0 & (T')^t \end{pmatrix} \begin{pmatrix} 0 & T' \\ (T')^{-t} & 0 \end{pmatrix} = \begin{pmatrix} 0 & I_g \\ I_g & 0 \end{pmatrix}$$

satisfies

$$\begin{pmatrix} 0 & I_g \\ I_g & 0 \end{pmatrix} \begin{pmatrix} \mu T & 0 \\ 0 & T^{-t} \end{pmatrix} \begin{pmatrix} 0 & I_g \\ I_g & 0 \end{pmatrix} = \begin{pmatrix} T^{-t} & 0 \\ 0 & \mu T \end{pmatrix} = \begin{pmatrix} \mu(\mu T)^{-t} & 0 \\ 0 & (\mu T) \end{pmatrix}$$

completes the proof. $\square$

We shall now investigate the case where m_α is irreducible of degree 2. Note that the characteristic polynomial of α is necessarily m_α^g , since it is defined over $\mathbb{F}_\ell$, has degree $2g$, and its only possible irreducible factor over $\mathbb{F}_\ell$ is m_α . We shall then use the isomorphism $\mathbb{F}_\ell[\alpha] \cong \mathbb{F}_\ell[x]/\langle m_\alpha \rangle \cong \mathbb{F}_{\ell^2}$ to view V as a g -dimensional vector space over $\mathbb{F}_{\ell^2}$.

The elements in $C_{\mathrm{GSp}(V)}(\alpha)$ preserve this structure on V . We shall shortly prove that they in fact preserve a non-degenerate Hermitian form on V up to similitude. Our approach is inspired by [Chi91, Section 2], which was in turn inspired by [Del82, Lemmas 4.6, 4.7].

We let Tr denote the trace map $\mathrm{Tr}: \mathbb{F}_{\ell^2} \rightarrow \mathbb{F}_\ell$.

Lemma 3.2. *Suppose $\alpha \in \mathrm{GSp}(V)$ has an irreducible minimal polynomial m_α of degree 2 satisfying $m_\alpha(0) = \chi(\alpha)$.*

Let $\xi \in \mathbb{F}_\ell[\alpha]^*$ be such that $\xi^{\ell-1} = -1$, i.e., $\mathrm{Tr}(\xi) = 0$. Then there exists a unique non-degenerate $\mathbb{F}_\ell[\alpha]$ -Hermitian form $\langle, \rangle_\# : V \times V \rightarrow \mathbb{F}_\ell[\alpha]$ such that $\langle v, w \rangle = \mathrm{Tr}(\xi \langle v, w \rangle_\#)$ for all $v, w \in V$.

Proof. We begin by noting that we may equip V with a second structure of an $\mathbb{F}_{\ell^2}$ -vector space. Indeed, the automorphism $\mathbb{F}_{\ell^2} \rightarrow \mathbb{F}_{\ell^2}$ given by $x \mapsto x^\ell$ allows us to equip V with a $\mathbb{F}_{\ell^2}$ -vector space structure where α acts by $\bar{\alpha} := \alpha^\ell$. We write $\bar{V}$ for V viewed with this alternative $\mathbb{F}_{\ell^2}$ structure.

Let us write $\langle, \rangle'$ for $\langle, \rangle$ viewed as an $\mathbb{F}_\ell$ -bilinear form $V \times \bar{V} \rightarrow \mathbb{F}_\ell$. Note that

$$\langle \alpha v, w \rangle' = \langle \alpha v, w \rangle = \langle v, \chi(\alpha) \alpha^{-1} w \rangle = \langle v, \bar{\alpha} w \rangle = \langle v, \alpha w \rangle'$$

where in the above we have used that m_α is irreducible of degree 2 and $m_\alpha(0) = \chi(\alpha)$. By the universal property of the tensor product, we find that $\langle, \rangle'$ determines an element of $\mathrm{Hom}_{\mathbb{F}_\ell}(V \otimes_{\mathbb{F}_{\ell^2}} \bar{V}, \mathbb{F}_\ell)$. Postcomposing by Tr yields an isomorphism $\mathrm{Hom}_{\mathbb{F}_{\ell^2}}(V \otimes_{\mathbb{F}_{\ell^2}} \bar{V}, \mathbb{F}_{\ell^2}) \rightarrow \mathrm{Hom}_{\mathbb{F}_\ell}(V \otimes_{\mathbb{F}_{\ell^2}} \bar{V}, \mathbb{F}_\ell)$ [Del82, Lemma 4.3]. We thus deduce that there exists a unique non-degenerate $\mathbb{F}_{\ell^2}$ -bilinear form $\langle, \rangle'_0 : V \times \bar{V} \rightarrow \mathbb{F}_{\ell^2}$ such that $\mathrm{Tr} \langle v, w \rangle'_0 = \langle v, w \rangle'$ for all $v \in V, w \in \bar{V}$. Correspondingly, we see that there is a unique non-degenerate sesquilinear form $\langle, \rangle_0 : V \times V \rightarrow \mathbb{F}_{\ell^2}$ such that $\mathrm{Tr} \langle v, w \rangle_0 = \langle v, w \rangle$ for all $v \in V, w \in V$.

Define $\langle, \rangle_\# := \xi^{-1} \langle, \rangle_0$. To prove $\langle, \rangle_\# : V \times V \rightarrow \mathbb{F}_{\ell^2}$ is a non-degenerate Hermitian form it remains to prove that $\overline{\langle v, w \rangle_\#} = \langle w, v \rangle_\#$. To this end, consider

$$\mathrm{Tr}(\xi \langle v, w \rangle_\#) = \langle v, w \rangle = -\langle w, v \rangle = \mathrm{Tr}(\xi \overline{\langle w, v \rangle_\#}).$$

Replacing v by $\xi^{-1} a v$ with $a \in \mathbb{F}_{\ell^2}$, we find $\mathrm{Tr}(a \langle v, w \rangle_\#) = \mathrm{Tr}(a \overline{\langle w, v \rangle_\#})$. Since multiplication followed by Tr yields a non-degenerate bilinear map $\mathbb{F}_{\ell^2} \times \mathbb{F}_{\ell^2} \rightarrow \mathbb{F}_\ell$ and the previous equality holds for all $a \in \mathbb{F}_{\ell^2}$, we deduce $\langle v, w \rangle_\# = \overline{\langle w, v \rangle_\#}$ as required.

If there exist two such Hermitian forms, then their difference is also a Hermitian form $\langle, \rangle_!$, and it satisfies $0 = \mathrm{Tr}(\xi \langle v, w \rangle_!)$ for all $v, w \in V$. Since $\mathrm{Tr}(\xi) = 0$, this can only happen if $\langle, \rangle_!$ is $\mathbb{F}_\ell$ -valued. Since it is $\mathbb{F}_{\ell^2}$ -linear in the first variable, we deduce that $\langle, \rangle_! = 0$. This proves uniqueness. $\square$

We let $\mathrm{CU}(V)$ denote the similitude group of $\langle, \rangle_\#$ and $\mathrm{GU}(V)$ its isometry group. The similitude group $\mathrm{CU}(V)$ is generated by $\mathrm{GU}(V)$ and the invertible scalar matrices over $\mathbb{F}_{\ell^2}$ [KL90, (2.3.3)].

Proposition 3.3. *Suppose $\alpha \in \mathrm{GSp}(V)$ has an irreducible minimal polynomial m_α of degree 2 satisfying $m_\alpha(0) = \chi(\alpha)$. Then the centraliser $C_{\mathrm{GSp}(V)}(\alpha)$ admits an isomorphism:*

$$C_{\mathrm{GSp}(V)}(\alpha) \cong \mathrm{CU}(V)$$

sending $C_{\mathrm{GSp}(V)}(\alpha) \cap \mathrm{Sp}(V)$ to $\mathrm{GU}(V)$ where the $\mathbb{F}_{\ell^2}$ -vector space structure on V is given by the natural action of $\mathbb{F}_\ell[\alpha]$.

Proof. We shall keep the notation introduced in the statement of Lemma 3.2. Let $\sigma \in \mathrm{Aut}_{\mathbb{F}_\ell[\alpha]}(V) = C_{\mathrm{GL}(V)}(\alpha)$. We may thus define the map $(,) : V \times V \rightarrow$

$\mathbb{F}_{\ell^2}$ via $(v, w) := \langle \sigma v, \sigma w \rangle_{\#}$ for any $v, w \in V$. It is easy to see that $(,)$ is a Hermitian pairing on V . Note that

$$\mathrm{Tr}(\xi \langle \sigma v, \sigma w \rangle_{\#}) = \mathrm{Tr}(\xi \langle v, w \rangle_{\#}) \text{ if and only if } \langle \sigma v, \sigma w \rangle = \langle v, w \rangle.$$

In particular, we see that $\mathrm{GU}(V) \hookrightarrow C_{\mathrm{GSp}(V)}(\alpha) \cap \mathrm{Sp}(V)$. Moreover, the uniqueness statement in Lemma 3.2 shows that if $\sigma \in \mathrm{Sp}(V)$, then $\langle \sigma v, \sigma w \rangle_{\#} = \langle v, w \rangle_{\#}$. Hence $\mathrm{GU}(V) \cong C_{\mathrm{GSp}(V)}(\alpha) \cap \mathrm{Sp}(V)$.

Now let $a \in \mathbb{F}_{\ell^2}^*$ and by abuse of notation write a again for the corresponding scalar matrix in $\mathrm{CU}(V)$. We have $\langle av, aw \rangle = \mathrm{Tr}(\xi \langle av, aw \rangle_{\#}) = \mathrm{Tr}(\xi \mathrm{Nm}(a) \langle v, w \rangle_{\#}) = \mathrm{Nm}(a) \mathrm{Tr}(\xi \langle v, w \rangle_{\#}) = \mathrm{Nm}(a) \langle v, w \rangle$. We deduce that $\mathrm{CU}(V) \hookrightarrow C_{\mathrm{GSp}(V)}(\alpha)$. Moreover, since the norm is surjective, we find that this injection is in fact an isomorphism since the index of $\mathrm{Sp}(V)$ in $\mathrm{GSp}(V)$ is $\ell - 1$. $\square$

4. RESIDUAL REPRESENTATIONS OF IM ABELIAN THREEFOLDS

4.1. Restrictions on the residual images. Let A/K be a polarised abelian variety of dimension $g \geq 2$ with potential imaginary multiplication by M . The preimage $\mathcal{O}$ of $\mathrm{End}(A_{KM})$ under ι is well-known to be an order in M . The restrictions on the action of Galois on $A[\ell]$ is influenced by whether or not ℓ divides the degree of our fixed polarisation $A \rightarrow A^{\vee}$ or the index of $\mathcal{O}$ in the maximal order of M . In Section 4.3, it will be important to restrict to primes ℓ such that A has semistable reduction at the primes lying over ℓ in M . For these reasons, we introduce the following definition:

Definition 4.1. We call a prime ℓ *admissible* for A if it satisfies all the conditions below:

- (1) ℓ does not divide the degree of the fixed polarisation.
- (2) ℓ does not divide the discriminant of $\mathcal{O} := \iota^{-1}(\mathrm{End}(A_{KM}))$.

If in addition to the above, A has semistable reduction at every prime above ℓ in M , we say ℓ is a *semistable admissible* prime.

For the rest of this section we assume ℓ is an admissible prime. Recall that the absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on the ℓ -torsion of A , yielding a representation

$$\rho_{\ell}: G_K \rightarrow \mathrm{Aut}(A[\ell]).$$

Since ℓ is coprime to the degree of our fixed polarisation $A \rightarrow A^{\vee}$, there exists a non-degenerate alternating pairing on $A[\ell]$, commonly referred to as the Weil pairing. The action of $\mathcal{O}$ on $A[\ell]$ commutes with that of $\rho_{\ell}(G_{KM})$.

For a prime ideal λ lying above ℓ , we write

$$A[\lambda] := \{P \in A(\overline{K}) \mid \iota(\alpha)P = 0 \forall \alpha \in \lambda\}.$$

Clearly $A[\lambda]$ is a vector space over $\mathbb{F}_{\lambda} := \mathcal{O}/\lambda$ and by [Rib76, Prop. 2.2.1] its dimension over $\mathbb{F}_{\lambda}$ is g . The absolute Galois group G_{KM} acts on $A[\lambda]$ again yielding a representation

$$\rho_{\lambda}: G_{KM} \rightarrow \mathrm{Aut}(A[\lambda]).$$

Note that as G_{KM} is a normal subgroup of G_K , for any $\sigma \in G_K$ we may define a representation ${}^{\sigma}\rho_{\lambda}$ of G_{KM} by ${}^{\sigma}\rho_{\lambda}(\tau) := \rho_{\lambda}(\sigma\tau\sigma^{-1})$. In the following

theorem we describe $\sigma\rho_\lambda$ and give upper bounds on the possible images of ρ_ℓ and ρ_λ .

Conserving the notation of Section 3, we further let $\Gamma U_g(V)$ denote the group of semisimilitudes of $\langle, \rangle_\#$ on V [KL90, Pg. 11].

Theorem 4.2. *Let ℓ be an admissible prime for A . Suppose that either ℓ is odd, or 2 is inert in M .*

If ℓ splits in M as $\lambda\bar{\lambda}$, then $\rho_\ell(G_{KM}) \subseteq \mathbb{F}_\ell^* \times \mathrm{GL}_g(\ell)$, $\rho_\lambda(G_{KM}) \subseteq \mathrm{GL}_g(\ell)$ and $\rho_\ell(G_{KM(\zeta_\ell)}) \subseteq \mathrm{GL}_g(\ell)$. If, furthermore, $M \cong \mathrm{End}^0(A_{KM})$, then $\rho_\ell(G_K) \subseteq (\mathbb{F}_\ell^* \times \mathrm{GL}_g(\ell)) \rtimes \langle \gamma \rangle$ where γ acts by $(\mu, T) \mapsto (\mu, \mu^{-1}T^{-t})$ and for any $\sigma \in G_K \setminus G_{KM}$ we have $\sigma\rho_\lambda = \rho_{\bar{\lambda}}$.

If ℓ is inert in M , then $\rho_\ell(G_{KM}) \subseteq \mathrm{CU}_g(\ell)$ and $\rho_\ell(G_{KM(\zeta_\ell)}) \subseteq \mathrm{GU}_g(\ell)$. If, furthermore, $M \cong \mathrm{End}^0(A_{KM})$, then $\rho_\ell(G_K) \subseteq \Gamma U_g(\ell)$.

Proof. Since $\mathcal{O}$ is an order in a quadratic field, we know that $\mathcal{O} = \mathbb{Z}[f\omega]$ where $\mathcal{O}_M = \mathbb{Z}[\omega]$ is the maximal order and $f = [\mathcal{O}_M : \mathcal{O}]$. As ℓ does not divide the discriminant of $\mathcal{O}$, we know that $\ell \nmid f$. Let $\alpha = f\omega$ and m_α denote the minimal polynomial of α . If $m_\alpha(0) \equiv 0 \pmod{\ell}$, then ℓ splits in M and as $\ell \neq 2$ there exists $n \in \mathbb{Z}$ such that $m_{\alpha+n}(0) \not\equiv 0 \pmod{\ell}$. As $\mathbb{Z}[\alpha+n] = \mathbb{Z}[\alpha]$, we may assume $m_\alpha(0) \not\equiv 0 \pmod{\ell}$.

Let $P, Q \in T_\ell(A)$ and denote by $\langle, \rangle : T_\ell(A) \times T_\ell(A) \rightarrow \mathbb{Z}_\ell$ the Weil pairing. Since ℓ is admissible, the pairing is perfect. Standard properties of the Rosati involution [Mum70, pgs. 189, 192] along with Albert's Classification [Mum70, Thm. 2, pg. 201] give us the following equalities:

$$\langle \iota(\alpha)P, \iota(\alpha)Q \rangle = \langle P, \iota(\bar{\alpha})\iota(\alpha)Q \rangle = \mathrm{Nm}_{M/\mathbb{Q}}(\alpha) \langle P, Q \rangle.$$

Since $\mathrm{Nm}_{M/\mathbb{Q}}(\alpha) = m_\alpha(0) \not\equiv 0 \pmod{\ell}$, it follows that α induces a similarity on $A[\ell]$ with respect to the Weil pairing. The minimal polynomial of $\iota(\alpha)$ acting on the Tate module is given by m_α (combine [Lan83, Chapter II, Thm. 3.6] and [Shi98, Chapter II, Lemma 1]). Thus the minimal polynomial of the induced similarity on $A[\ell]$ is m_α reduced modulo ℓ .

Since $\mathbb{Z}[\alpha]$ is ℓ -maximal, we may apply Dedekind-Kummer factorisation to see $m_\alpha \pmod{\ell}$ is irreducible if ℓ is inert in M and is reducible with distinct roots if ℓ splits in M . In particular, Dedekind-Kummer factorisation tells us that if ℓ splits in M , then writing $m_\alpha = \phi\phi'$ with each of ϕ and ϕ' as degree 1 polynomials we have, up to exchanging ϕ and ϕ' , $\lambda = \langle \ell, \phi(\alpha) \rangle$ and $\bar{\lambda} = \langle \ell, \phi'(\alpha) \rangle$. Thus for ℓ split in M , we have $A[\lambda] = A[\ell] \cap \mathrm{Ker}(\phi(\alpha))$ and $A[\bar{\lambda}] = A[\ell] \cap \mathrm{Ker}(\phi'(\alpha))$. As $\iota(M)$ is contained in $\mathrm{End}^0(A_{KM})$, the action of G_{KM} commutes with that of $\iota(\alpha)$ on $A[\ell]$. Thus the result for G_{KM} follows from applying Proposition 3.1 and Proposition 3.3.

If $\iota(M) \subseteq \mathrm{End}^0(A_K)$, then the result for G_K follows by the same reasoning as that of G_{KM} . Thus let us suppose $\iota(M) \not\subseteq \mathrm{End}^0(A_K)$. Then the action of G_K on $\mathrm{End}^0(A_{KM}) \cong M$ furnishes a surjection $\varrho : G_K \rightarrow \mathrm{Gal}(M/\mathbb{Q})$ with kernel G_{KM} .

In particular, for $\sigma \in G_K$ and $\alpha \in M$ we have $\iota(\alpha)^\sigma = \iota(\alpha^{\varrho(\sigma)})$. For the action on $A[\ell]$, we thus have $\rho_\ell(\sigma)\iota(\alpha) = \iota(\alpha^{\varrho(\sigma)})\rho_\ell(\sigma)$. The result for G_K when ℓ is inert in M is thus clear.

Let us consider the case where ℓ is split in M . Since the minimal polynomial of α has degree two, we see that if $\sigma \in G_K \setminus G_{KM}$, then $\alpha^{\varrho(\sigma)} =$

$\text{Nm}_{M/\mathbb{Q}}(\alpha)\alpha^{-1}$. Thus if $\sigma \in G_K \setminus G_{KM}$ and v is an eigenvector of $\iota(\alpha)$ with eigenvalue a , then

$$\iota(\alpha)\rho_\ell(\sigma)v = \rho_\ell(\sigma)\iota(\alpha^\sigma(\sigma))v = \text{Nm}_{M/\mathbb{Q}}(\alpha)\rho_\ell(\sigma)\iota(\alpha^{-1})v = \text{Nm}_{M/\mathbb{Q}}(\alpha)a^{-1}\rho_\ell(\sigma)v,$$

from which we deduce that σ exchanges the eigenspaces of α . For $\tau \in G_{KM}$, we have ${}^\sigma\rho_\lambda(\tau) := \rho_\lambda(\sigma\tau\sigma^{-1}) = \rho_\ell(\sigma\tau\sigma^{-1})|_{A[\lambda]}$. Since σ gives an isomorphism $A[\bar{\lambda}] \xrightarrow{\sim} A[\lambda]$ of the underlying vector spaces, and the action of τ on $A[\bar{\lambda}]$ is through $\rho_{\bar{\lambda}}(\tau)$, we deduce that ${}^\sigma\rho_\lambda \cong \rho_{\bar{\lambda}}$.

The final result then follows from applying Proposition 3.1. $\square$

As is common in group theory (see [BHR13, Pg. 6] or [KL90, Pg. 15]), we will use the notation $\text{GL}^+ = \text{GL}$ and $\text{GL}^- = \text{GU}$. That is, GL^+ and GL^- denote the isometry group of the zero pairing and a non-degenerate hermitian pairing respectively. It is convenient for us to further extend this notation to the similitude groups, thus writing $\text{CL}^+ = \text{GL}$ and $\text{CL}^- = \text{CU}$.

The following is a direct consequence of Theorem 4.2.

Corollary 4.3. *Let ℓ be an admissible prime for A , and λ a prime above ℓ in M . Writing $\varepsilon = \left(\frac{\Delta_M}{\ell}\right)$, we have*

$$\rho_\lambda(G_{KM}) \subseteq \text{CL}^\varepsilon(A[\lambda])$$

and

$$\rho_\lambda(G_{KM(\zeta_\ell)}) \subseteq \text{GL}^\varepsilon(A[\lambda]).$$

4.2. Background on λ -adic representations. From now on A will denote an abelian threefold defined over M with *imaginary multiplication* by (M, ι) of signature $(2, 1)$.

Let $T_\ell(A) := \varprojlim A[\ell]$ denote the Tate module of A , and $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. The endomorphism algebra $\text{End}^0(A)$ acts faithfully on $V_\ell(A)$ and its action commutes with that of $\mathbb{Q}_\ell$, making $V_\ell(A)$ into an $M \otimes \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} M_\lambda$ module via ι , where here $\lambda|\ell$ runs over all primes above ℓ in M and M_λ is the completion of M at λ . The decomposition $M \otimes \mathbb{Q}_\ell = \prod_{\lambda|\ell} M_\lambda$ allows us to write $1 \in M \otimes \mathbb{Q}_\ell$ as a sum of idempotents $1 = \sum_{\lambda|\ell} e_\lambda$ where e_λ is the multiplicative identity in M_λ and the additive identity in $M_{\lambda'}$ for $\lambda' \neq \lambda$. The vector space $e_\lambda V_\ell(A)$ naturally inherits the structure of an M_λ -vector space, which we denote by $V_\lambda(A)$. Each $V_\lambda(A)$ is a M_λ -vector space of dimension 3 [Rib76]. Furthermore, since $\text{Res}_{\mathbb{Q}_\ell}^{M_\lambda} V_\lambda(A) = e_\lambda V_\ell(A)$ and $M \hookrightarrow \text{End}_{\mathbb{Q}_\ell}(V_\ell)$ is a unital algebra embedding, we have a decomposition

$$V_\ell(A) = \prod_{\lambda|\ell} \text{Res}_{\mathbb{Q}_\ell}^{M_\lambda}(V_\lambda(A)).$$

Thus the representation $\rho_{\ell^\infty}: G_M \rightarrow \text{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$ commutes with the action of $M \otimes \mathbb{Q}_\ell$. This in turn implies each $V_\lambda(A)$ is an $M_\lambda[G_M]$ -module. We denote the corresponding representation by

$$\rho_{\lambda^\infty}: G_M \rightarrow \text{Aut}_{M_\lambda}(V_\lambda(A)).$$

If ℓ is an admissible prime, then we get a corresponding decomposition of the Tate module leading to a lattice $T_\lambda(A)$ inside $V_\lambda(A)$ for every prime $\lambda|\ell$. We then have an isomorphism of $\mathbb{F}_\lambda[G_M]$ -modules $T_\lambda(A)/\lambda \cdot T_\lambda(A) \cong A[\lambda]$.

This family of representations $(\rho_{\lambda^\infty})_\lambda$ is known to form a strictly compatible system [Rib76, Thm 2.12]. It follows that their determinants $(\det \circ \rho_{\lambda^\infty})_\lambda$ also form a strictly compatible system. Such a system of λ -adic representations is known to arise from an algebraic Hecke character Ω of M with values in M and conductor dividing the conductor of A [Sch88, Prop. 1.4, page 25]. That is, the compatible system of λ -adic representations $(\Omega_{\lambda^\infty})_\lambda$ associated to Ω as in [Sch88, Chapter 0, §5] coincides with $(\det \circ \rho_{\lambda^\infty})_\lambda$. Generalising the Shimura-Taniyama formula, Fité has shown that the infinity type of Ω is determined by the action of $\iota(M)$ on $\Omega^1(A)$ [Fit24, Prop. 14]. In particular, as A has imaginary multiplication by M , we deduce that the infinity type of Ω is either $2\varphi^{-1} + \bar{\varphi}^{-1}$ or $\varphi^{-1} + 2\bar{\varphi}^{-1}$.

4.3. Action of inertia at $\ell = p$. Let λ be an unramified prime of M above the rational prime ℓ , k_λ the residue field of M_λ and M_λ^{ur} be the maximal unramified extension of M_λ . For any d with $\ell \nmid d$, we denote by μ_d the d -th roots of unity in M_λ^{ur} , which we identify with their images in $\bar{k}_\lambda$.

Let π be a uniformiser of M_λ^{ur} . Consider the map

$$\theta_{\{d\},\lambda}: \text{Gal}(M_\lambda^{ur}(\pi^{1/d})/M_\lambda^{ur}) \rightarrow \mu_d$$

defined by sending the element $\sigma \in \text{Gal}(M_\lambda^{ur}(\pi^{1/d})/M_\lambda^{ur})$ to the d -th root of unity $\theta_{\{d\},\lambda}(\sigma)$ satisfying

$$\sigma(\pi^{1/d}) = \theta_{\{d\},\lambda}(\sigma)\pi^{1/d}.$$

One may check that $\theta_{\{d\},\lambda}$ does not depend on the choice of uniformiser π nor its d -th root and that it is in fact a group isomorphism.

Clearly the $\theta_{\{d\},\lambda}: I_\lambda^t \rightarrow \bar{k}_\lambda^*$ give characters of the tame inertia group I_λ^t . In fact, they give rise to all characters. Indeed, denoting the localisation of $\mathbb{Z}$ by $\mathbb{Z} \setminus (\ell)$ by $\mathbb{Z}_{(\ell)}$, we have:

Proposition 4.4. [Ser72, Prop. 5] *The map $\mathbb{Z}_{(\ell)}/\mathbb{Z} \rightarrow \text{Hom}(I_\lambda^t, \bar{k}_\lambda^*)$ defined by $\frac{b}{d} \mapsto \theta_{\{d\},\lambda}^b$ is an isomorphism of groups.*

Note that characters $\theta_{\{\ell^n-1\},\lambda}: I_\lambda^t \rightarrow \mathbb{F}_{\ell^n}^*$ are surjective, as are their powers $\theta_{\{\ell^n-1\},\lambda}^s$, for $s \in \mathbb{Z}/n\mathbb{Z}$. We call such a character a fundamental character of level n and write $\theta_{n,\lambda} := \theta_{\{\ell^n-1\},\lambda}$. In fact, when what is meant is clear from context we shall write θ_n in place of $\theta_{n,\lambda}$.

Note also that $\chi_\ell|_{I_\lambda}$, that is, the restriction of the mod- ℓ cyclotomic character $\chi_\ell: G_M \rightarrow \mathbb{F}_\ell^*$, post composed with $\mathbb{F}_\ell^* \hookrightarrow \bar{k}_\lambda^*$ gives rise to an element of $\text{Hom}(I_\lambda^t, \bar{k}_\lambda^*)$ and hence equals $\theta_{1,\lambda}$ by Proposition 4.4. We shall reserve the notation χ_ℓ for the cyclotomic character when viewed as a global representation, i.e., of G_M and write $\theta_{1,\lambda}$ (or θ_1) when viewed as a character of I_λ .

Proposition 4.5. *Let λ be a prime of M above an admissible prime ℓ . If ℓ splits in M , then either $\det \circ \rho_\lambda|_{I_\lambda} = \theta_1$ and $\det \circ \rho_\lambda|_{I_\lambda^-} = \theta_1^2$, or $\det \circ \rho_\lambda|_{I_\lambda} = \theta_1^2$ and $\det \circ \rho_\lambda|_{I_\lambda^-} = \theta_1$.*

If ℓ is inert in M , then either $\det \circ \rho_\lambda|_{I_\lambda} = \theta_2^{2+\ell}$ or $\theta_2^{1+2\ell}$.

Proof. As summarised in Section 4.2, there exists an algebraic Hecke character Ω of M with values in M , conductor dividing that of A and infinity

type either $2\varphi^{-1} + \overline{\varphi}^{-1}$ or $\varphi^{-1} + 2\overline{\varphi}^{-1}$ such that its λ -adic avatars Ω_{λ^∞} coincide with $\det \circ \rho_{\lambda^\infty}$. It is explained in [Ser72, Section 3.4] (see also [Goo25, Section 6.1] for a summary) that we may reduce Ω_{λ^∞} modulo λ to obtain a representation Ω_λ , which coincides with $\det \circ \rho_\lambda$. Furthermore, if I is the inertia group at a prime above ℓ coprime to the conductor of Ω , the restriction of Ω_λ to I is shown to be the product of powers of fundamental characters of level $[\mathbb{F}_\lambda : \mathbb{F}_\ell]$, where the powers are given by the coefficients in the infinity type of Ω (see [Goo25, Eq (6.1)]). $\square$

By definition, a semisimple representation is determined by its simple constituents. We shall make use of this in the following proposition to keep notation light. More precisely, we shall write $(\rho_\lambda|_I)^{ss}$ equal to the sum of three characters for some group I to mean that the simple factors of the semisimplification $(A[\lambda]|_I \otimes_{\mathbb{F}_\lambda} \overline{\mathbb{F}_\lambda})^{ss}$ are given by these characters.

Proposition 4.6. *Let ℓ be a semistable admissible prime for A . Let I be an inertia subgroup corresponding to a prime above ℓ in G_M .*

Suppose ℓ splits in M . Then either $\det \circ \rho_\lambda|_I = \theta_1$ or θ_1^2 . In the former case $(\rho_\lambda|_I)^{ss}$ is given by one of $2\mathbb{1} + \theta_1, \mathbb{1} + \theta_2 + \theta_2^\ell$ and $\theta_3 + \theta_3^\ell + \theta_3^{\ell^2}$. In the latter case $(\rho_\lambda|_I)^{ss}$ is given by one of $\mathbb{1} + 2\theta_1, \theta_1 + \theta_2 + \theta_2^\ell$ and $\theta_3^{1+\ell} + \theta_3^{\ell+\ell^2} + \theta_3^{1+\ell^2}$.

Suppose ℓ is inert in M . Then either $\det \circ \rho_\lambda|_I = \theta_2^{2+\ell}$ or $\theta_2^{1+2\ell}$. In the former case $(\rho_\lambda|_I)^{ss}$ is given by one of $2\theta_2 + \theta_2^\ell, \mathbb{1} + \theta_1 + \theta_2$, or $\theta_6^e + \theta_6^{e\ell^2} + \theta_6^{e\ell^4}$ where $e = 1 + \ell + \ell^2$. In the latter case, $(\rho_\lambda|_I)^{ss}$ is given by one of $\theta_2 + 2\theta_2^\ell, \mathbb{1} + \theta_1 + \theta_2^\ell$, or $\theta_6^e + \theta_6^{e\ell^2} + \theta_6^{e\ell^4}$ where $e = 1 + \ell + \ell^5$.

Proof. Let ψ_1 be an irreducible $\overline{\mathbb{F}_\lambda}[I]$ -submodule of $A[\lambda] \otimes_{\mathbb{F}_\lambda} \overline{\mathbb{F}_\lambda}$. As ℓ -groups act trivially on irreducible modules in characteristic ℓ , the wild inertia subgroup of I acts trivially on ψ_1 . Moreover, as the tame quotient of I is pro-cyclic, the action of I on ψ_1 is via a cyclic group. Hence we deduce that ψ_1 is one dimensional. Repeating the argument, we may write $(\rho_\lambda|_I)^{ss} = \psi_1 + \psi_2 + \psi_3$. Our main goal is to determine the set $\Psi := \{\psi_1, \psi_2, \psi_3\}$.

We shall use the following restrictions on Ψ . First, we clearly have $\psi_1\psi_2\psi_3 = \det \circ \rho_\lambda|_I$. Second, as explained in the proof of [LV14, Lemma 4.9], it follows from [Ray74, Thm. 3.4.3] and [GR72, Exposé IX] that we may write each $\psi_i = \theta_n^e$ for some n and $e = \sum_{j=0}^{n-1} e_j \ell^j$ with $e_j \in \{0, 1\}$.

Suppose ℓ splits in M . As $A[\lambda]$ is a 3-dimensional vector space over $\mathbb{F}_\ell$, each ψ_i is a power of a fundamental character of level at most 3. By Proposition 4.5, we have either $\det \circ \rho_\lambda|_I = \theta_1$ or θ_1^2 . Let us suppose we are in the former case, i.e., $\det \circ \rho_\lambda|_I = \theta_1$. If one of ψ_1, ψ_2, ψ_3 equals θ_1 , then $\Psi := \{\theta_1, \mathbb{1}, \mathbb{1}\}$. Thus let us suppose in the following that $\theta_1 \notin \Psi$. If $\theta_2 \in \Psi$, then so is its conjugate θ_2^ℓ , in which case $\Psi = \{\theta_2, \theta_2^\ell, \mathbb{1}\}$. Thus we may suppose $\theta_3^e \in \Psi$ for some $e = e_0 + e_1\ell + e_0\ell^2 \neq 1 + \ell + \ell^2$, which implies $\Psi = \{\theta_3^e, \theta_3^{e\ell}, \theta_3^{e\ell^2}\}$. As $\theta_1 = \theta_3^e \cdot \theta_3^{e\ell} \cdot \theta_3^{e\ell^2} = \theta_3^{e(1+\ell+\ell^2)} = \theta_1^e$, we find $e \equiv 1 \pmod{\ell-1}$. Thus $\{e_0, e_1, e_2\} = \{1, 0, 0\}$, so $\Psi = \{\theta_3, \theta_3^\ell, \theta_3^{\ell^2}\}$. An analogous argument when $\det \circ \rho_\lambda|_I = \theta_1^2$ determines the possibilities for $(\rho_\lambda|_I)^{ss}$.

Suppose ℓ is inert in M . As $A[\lambda]$ is a 3-dimensional vector space over $\mathbb{F}_{\ell^2}$, the set Ψ must be stable under the action of $G_{\mathbb{F}_{\ell^2}}$, which implies each ψ_i is a power of a fundamental character of level 1, 2, 3, 4, or 6. Moreover, by Proposition 4.5, we have either $\det \circ \rho_\lambda|_I = \theta_2^{2+\ell}$ or $\theta_2^{1+2\ell}$ thus Ψ must contain

a character which is a power of a fundamental character of even level that does not factor through a fundamental character of odd level. In particular, no ψ_i can be a power of a fundamental character of level 3, unless it is θ_1 . Let us first consider the case $\det \circ \rho_\lambda|_I = \theta_2^{2+\ell}$.

Let us first suppose Ψ only contains fundamental characters of level at most 2. If $\theta_1 \in \Psi$, then clearly $\Psi = \{\theta_1, \theta_2, \mathbb{1}\}$. If $\theta_2 \in \Psi$, but $\theta_1 \notin \Psi$, then $\Psi = \{\theta_2, \theta_2, \theta_2^\ell\}$.

Let us now suppose $\theta_4^e \in \Psi$ and θ_4^e is not $\mathbb{1}, \theta_1, \theta_2$ or θ_2^ℓ . Then $\Psi = \{\theta_4^e, \theta_4^{e\ell^2}, \theta_2^{e'}\}$ for some e' . Raynaud's Theorem implies that $e = \sum_{i=0}^3 e_i \ell^i$ and $e' = e'_0 + e'_1 \ell$ for some $e_i, e'_i \in \{0, 1\}$. We deduce that Ψ may be equal to one of the following sets $\{\theta_4^{1+\ell+\ell^2}, \theta_4^{1+\ell^2+\ell^3}, \mathbb{1}\}$, $\{\theta_4, \theta_4^{\ell^2}, \theta_1\}$, $\{\theta_4^{1+\ell}, \theta_4^{\ell^2+\ell^3}, \theta_2\}$, or $\{\theta_4^{1+\ell^3}, \theta_4^{\ell+\ell^2}, \theta_2\}$. It is easy to check in each of these cases that the order inertia at ℓ will contain a element of order $1 + \ell^2$. We shall show this is incompatible with Corollary 4.3. The order of $\text{CU}_3(\ell)$ equals $\ell^3(\ell+1)(\ell^2-1)^2(\ell^3+1)$. Note that 4 does not divide $1 + \ell^2$, since otherwise $\ell \pmod{4}$ would be a square root of 3 $\pmod{4}$. The greatest common divisor of $1 + \ell^2$ with any of $\ell+1, \ell^2-1, \ell^3+1$ is 2 if ℓ is odd and 1 otherwise. Thus $1 + \ell^2$ does not divide the order of $\text{CU}_3(\ell)$. Since the image of ρ_λ is contained in $\text{CU}_3(\ell)$ by Corollary 4.3, we deduce that $\theta_4^e \in \Psi$ if and only if θ_4^e is one of $\mathbb{1}, \theta_1, \theta_2$ or θ_2^ℓ .

We are left to consider the case where $\theta_6^e \in \Psi$ and θ_6^e is not $\mathbb{1}, \theta_1, \theta_2$ or θ_2^ℓ , then $\Psi = \{\theta_6^e, \theta_6^{e\ell^2}, \theta_6^{e\ell^4}\}$. By Raynaud's Theorem, we may write $e = \sum_{i=0}^5 e_i \ell^i$ for some $e_i \in \{0, 1\}$. Since $\theta_2^{2+\ell} = \theta_6^e \cdot \theta_6^{e\ell^2} \cdot \theta_6^{e\ell^4} = \theta_6^{e(1+\ell^2+\ell^4)} = \theta_2^e$, we see $e \equiv (e_0 + e_2 + e_4) + (e_1 + e_3 + e_5)\ell \equiv 2 + \ell \pmod{\ell^2 - 1}$. That is, $\{e_0, e_2, e_4\} = \{1, 1, 0\}$ and $\{e_1, e_3, e_5\} = \{1, 0, 0\}$. It follows that there are at $\binom{3}{2} \cdot \binom{3}{1} / 3 = 3$ possibilities for Ψ in this situation.

By considering the order of $\text{CU}_3(\ell)$, we will, as above, discount 2 of these possibilities, leaving $\Psi = \{\theta_6^e, \theta_6^{e\ell^2}, \theta_6^{e\ell^4}\}$ with $e = 1 + \ell + \ell^2$ as the unique possibility. To do so, it suffices to show the orders of $\theta_6^{1+\ell^2+\ell^3}(I)$ and $\theta_6^{1+\ell^2+\ell^5}(I)$ do not divide the order of $\text{CU}_3(\ell)$.

We begin by proving their orders are a multiple of $\frac{1}{9}(\ell^6 - 1)$. We provide the proof for $\theta_6^{1+\ell^2+\ell^3}(I)$, the other case being similar. Let $e = 1 + \ell^2 + \ell^3$. Again using modular arithmetic, we find $\gcd(e, \ell+1) = 1, \gcd(e, \ell^2 - \ell + 1) = 1$ and $\gcd(e, \ell - 1)$ divides 3. Likewise, we obtain $e \equiv \ell(\ell+1)(\ell-1) \equiv 1 - \ell \pmod{\ell^2 + \ell + 1}$. Thus $\gcd(e, 1 + \ell + \ell^2)$ divides 3. It follows that $\gcd(e, \ell^6 - 1)$ divides 9 and thus the order of θ_6^e is a multiple of $\frac{1}{9}(\ell^6 - 1)$.

The order of $\text{CU}_3(\ell)$ equals $\ell^3(\ell+1)(\ell^2-1)^2(\ell^3+1)$. The gcd of $\# \text{CU}_3(\ell)$ and $1 + \ell + \ell^2$ equals 1 if $\ell \not\equiv 1 \pmod{3}$ and it is equal to 3 if $\ell \equiv 1 \pmod{3}$. For $\ell \geq 7$, we have that $1 + \ell + \ell^2 \geq 57 > 3^3$, thus $\text{CU}_3(\ell)$ cannot contain an element of order $\frac{1}{9}(\ell^6 - 1)$. Hence if $\Psi = \{\theta_6^e, \theta_6^{e\ell^2}, \theta_6^{e\ell^4}\}$ we must have either $e = 1 + \ell + \ell^2$.

An analogous argument when $\det \circ \rho_\lambda|_I = \theta_2^{1+2\ell}$ determines the possibilities for $(\rho_\lambda|_I)^{ss}$. We note that the factorisation $\ell^5 + \ell + 1 = (\ell^2 + \ell + 1)(\ell^3 - \ell^2 + 1)$ is used for the case when Ψ contains a character which is a power of a fundamental character of level 6, not factoring through one of lower level. $\square$

Proposition 4.7. *The homomorphism $\Omega_\lambda = \det \circ \rho_\lambda: G_{M(\zeta_\ell)} \rightarrow \mathbb{F}_\lambda^*$ is surjective if ℓ splits in M and it surjects onto $(\mathbb{F}_\lambda^*)^{\ell-1}$ if ℓ is inert in M .*

Moreover, for ℓ split in M , we have $\rho_\lambda(G_M) = \mathrm{GL}_3(\ell)$ if and only if $\rho_\lambda(G_{M(\zeta_\ell)}) = \mathrm{GL}_3(\ell)$.

Proof. Write $\mathrm{Nm}_{M/\mathbb{Q}}(\lambda) = \ell^f$ where $f \in \{1, 2\}$ is the inertia degree of λ . As M is unramified at ℓ , we have that $\theta_f: I_{\lambda'} \rightarrow \mathbb{F}_\lambda^*$ is surjective, for $\lambda' \in \{\lambda, \bar{\lambda}\}$. In particular, there exists $\sigma' \in I_\lambda$ such that $\theta_f(\sigma')$ has order $\ell + (-1)^f$ and $\sigma'' \in I_{\bar{\lambda}}$ such that $\theta_f(\sigma'') = \theta_f(\sigma')^{-1}$. If ℓ is split in M , let $\sigma := \sigma'\sigma''$. If ℓ is inert in M , let $\sigma := \sigma'$. Using that $\theta_2^{\ell+1} = \theta_1$ and $\chi_\ell|_{I_\lambda} = \theta_1$, we have $\chi_\ell(\sigma) = 1$. Thus $\sigma \in G_{M(\zeta_\ell)}$.

We shall now apply Proposition 4.5 to show $\Omega_\lambda(\sigma)$ has order $\ell + (-1)^f$ in $\mathbb{F}_\lambda^*$. For ℓ split in M , consider $\Omega_\lambda(\sigma) = \Omega_\lambda(\sigma')\Omega_\lambda(\sigma'') = \chi_\ell(\sigma')^{\pm 1}$. For ℓ inert in M , we have $\Omega_\lambda(\sigma) = \theta_2(\sigma)^{\pm 1}$. This completes the proof of the first statement.

Let us now suppose ℓ splits in M and prove the final statement. If $\rho_\lambda(G_{M(\zeta_\ell)}) = \mathrm{GL}_3(\ell)$ then it is clear by Theorem 4.3 that $\rho_\lambda(G_M) = \mathrm{GL}_3(\ell)$. Thus let us suppose $\rho_\lambda(G_M) = \mathrm{GL}_3(\ell)$. As $\mathrm{Gal}(M(\zeta_\ell)/M)$ is abelian, we see that $\rho_\lambda(G_{M(\zeta_\ell)})$ contains the commutator subgroup of $\rho_\lambda(G_M) = \mathrm{GL}_3(\ell)$, that is, $\rho_\lambda(G_{M(\zeta_\ell)}) \supseteq \mathrm{SL}_3(\ell)$ since $\mathrm{SL}_3(\ell)$ is perfect [Gro02, Thm. 1.7]. As $\det \circ \rho_\lambda: G_{M(\zeta_\ell)} \rightarrow \mathbb{F}_\lambda^*$ is surjective, we deduce $\rho_\lambda(G_{M(\zeta_\ell)}) = \mathrm{GL}_3(\ell)$. $\square$

For an admissible prime ℓ which splits in M as $\lambda\bar{\lambda}$, we will now show that surjectivity of the λ -torsion representation ρ_λ implies surjectivity of the ℓ -torsion representation over M . Note that this is a tautological statement for inert primes.

Proposition 4.8. *Let ℓ be an admissible prime for an abelian threefold A/M with imaginary multiplication by M of signature $(2, 1)$, such that ℓ splits in M . Let λ be a prime above ℓ in M . If $\rho_\lambda(G_M) = \mathrm{GL}_3(\ell)$, then $\rho_\ell(G_M) = \mathbb{F}_\ell^* \times \mathrm{GL}_3(\ell)$.*

Proof. By Proposition 4.7, we have $\rho_\lambda(G_{M(\zeta_\ell)}) = \mathrm{GL}_3(\ell)$. Restricting the action of $G_{M(\zeta_\ell)}$ from $A[\ell]$ to $A[\lambda]$, we obtain a surjective homomorphism $\rho_\ell(G_{M(\zeta_\ell)}) \rightarrow \rho_\lambda(G_{M(\zeta_\ell)}) = \mathrm{GL}_3(\ell)$. Moreover, owing to the mod- ℓ cyclotomic character χ_ℓ being the similitude character of the Weil pairing on $A[\ell]$, we have a surjective homomorphism $\rho_\ell(G_M) \rightarrow \chi_\ell(G_M)$ with kernel $\rho_\ell(G_{M(\zeta_\ell)})$. As M is unramified at ℓ , $\chi_\ell(G_M) = \mathbb{F}_\ell^*$. By Theorem 4.3, $\rho_\ell(G_M) \subseteq \mathbb{F}_\ell^* \times \mathrm{GL}_3(\ell)$. Hence for cardinality reasons, we deduce $\rho_\ell(G_M) = \mathbb{F}_\ell^* \times \mathrm{GL}_3(\ell)$. $\square$

Theorem 4.9. *Let $A/\mathbb{Q}$ be an abelian threefold such that $\mathrm{End}^0(A_{\overline{\mathbb{Q}}}) \cong M$. Let ℓ be an admissible prime for A which is either odd, or inert in M . Suppose that $\rho_\lambda(G_M) = \mathrm{CL}^\varepsilon(A[\lambda]) \cong \mathrm{CL}_3^\varepsilon(\ell)$.*

- *If ℓ splits in M , then $\rho_\ell(G_{\mathbb{Q}}) \cong (\mathbb{F}_\ell^* \times \mathrm{GL}_3(\ell)) \rtimes \langle \gamma \rangle$ where γ acts by $(\mu, T) \mapsto (\mu, \mu^{-1}T^{-t})$.*
- *If ℓ is inert in M , then $\rho_\ell(G_{\mathbb{Q}}) \cong \mathrm{GU}_3(\ell)$.*

Proof. By Proposition 4.8, for ℓ split in M , we have $\rho_\ell(G_M) \cong \mathbb{F}_\ell^* \times \mathrm{GL}_3(\ell)$. For ℓ inert in M we have $\rho_\ell(G_M) \cong \mathrm{CU}_3(\ell)$. By [Sil92, Thm. 2.4] and

[Goo26a, Thm. 1.2], M is contained in $\mathbb{Q}(A[\ell])$. Thus for cardinality reasons, we have, by Theorem 4.2, that $\rho_\ell(G_\mathbb{Q})$ is as claimed. $\square$

5. CRITERIA FOR LARGE IMAGES

Let A be an abelian threefold defined over M . Corollary 4.3 shows that for an admissible prime ℓ , the image of G_M under ρ_λ lands in $\mathrm{CL}_3^\varepsilon(\ell)$ where $\varepsilon = (\frac{\Delta_M}{\ell})$. In this section we will develop a practical method for proving $\rho_\lambda(G_M) \cong \mathrm{CL}_3^\varepsilon(\ell)$.

To prove $\rho_\lambda(G_M) \cong \mathrm{CL}_3^\varepsilon(\ell)$, we need to rule out the possibility that $\rho_\lambda(G_M)$ is contained in any maximal subgroup of $\mathrm{CL}^\varepsilon(A[\lambda])$. Thus in Section 5.1 we list the maximal subgroups of $\mathrm{CL}_3^\varepsilon(\ell)$. In Section 5.2, we determine consequences of $\rho_\lambda(G_M)$ being contained in each maximal subgroup, and provide algorithms to check if these consequences are fulfilled. If $\mathrm{End}^0(A_{\overline{M}}) \cong M$, we show under Assumption 5.1 that these algorithms always work. This assumption appears to be known to experts, but not written down anywhere.

Assumption 5.1. Let A/M be an abelian threefold with $\mathrm{End}^0(A_{\overline{M}}) \cong M$. Then there exists a rational prime ℓ split in M and λ a prime of M lying over ℓ such that there is an isomorphism $\rho_\lambda(G_M) \cong \mathrm{GL}_3(\ell)$.

Moreover, ℓ can be chosen to be as large as needed, and satisfying the congruence condition $\ell \equiv 1 \pmod{e}$ for any integer e .

5.1. Maximal subgroups of $\mathrm{CL}_3^\varepsilon(\ell)$. Recall that we write $\mathrm{CL}^+ = \mathrm{GL}$ and $\mathrm{CL}^- = \mathrm{CU}$, which are the similitude groups of the zero pairing and a non-degenerate Hermitian pairing respectively.

The classification of the maximal subgroups of $\mathrm{CL}_3^\pm(\ell)$ may be deduced from the tables found on pages 378 and 379 of [BHR13]. Let us briefly describe how one does so. On page 378 (resp. 379) the maximal subgroups of $\mathrm{SL}_3^+(\ell) := \mathrm{SL}_3(\ell)$ (resp. $\mathrm{SL}_3^-(\ell) := \mathrm{SU}_3(\ell)$) are listed. The maximal subgroups of $\mathrm{SL}_3^\varepsilon(\ell)$ which extend to $\mathrm{GL}_3^\varepsilon(\ell)$ are identified by the presence of the diagonal automorphism δ (viewed as an element of the outer automorphism group of $\mathrm{PSL}_3^\varepsilon(\ell)$, see [BHR13, pages 33, 34]) in the ‘stab’ column. The table also notes the order of the outer automorphism δ to be $d = \gcd(3, \ell - \varepsilon)$. If $d = 1$, then δ is trivial and all rows satisfy the criterion.

To deduce the maximal subgroups of $\mathrm{CU}_3(\ell)$ from those of $\mathrm{GU}_3(\ell)$ note that any maximal subgroup of either group not containing the centre must contain $\mathrm{SU}_3(\ell)$ (see for example [Goo25, Lemma 3.15]). As is a general fact in group theory, the subgroups of $\mathrm{CU}_3(\ell)$ (resp. $\mathrm{GU}_3(\ell)$) containing the centre correspond bijectively to those of their projectivisations via the quotient and inverse image maps. Thus the maximal subgroups of $\mathrm{CU}_3(\ell)$ either contain $\mathrm{SU}_3(\ell)$ or arise from the maximal subgroups of $\mathrm{GU}_3(\ell)$ via adjoining the group of scalar matrices over $\mathbb{F}_{\ell^2}^*$.

One finds that the maximal subgroups of $\mathrm{GL}_3^\varepsilon(\ell)$ not containing $\mathrm{SL}_3^\varepsilon(\ell)$ fall into one of six families. Namely, $\mathcal{C}_1$ reducible subgroups, $\mathcal{C}_2$ imprimitive subgroups, $\mathcal{C}_3$ field extension subgroups, $\mathcal{C}_6$ symplectic type subgroups, $\mathcal{C}_8/\mathcal{C}_5$ -type orthogonal subgroups, or $\mathcal{S}$ -type subgroups. The last two families occur only when the order $d = \gcd(3, \ell - \varepsilon)$ of the automorphism δ is 1, i.e., $\ell \not\equiv \varepsilon \pmod{3}$. So it is worth pointing out that if $M = \mathbb{Q}(\zeta_3)$, then

$\varepsilon = \left(\frac{\Delta_M}{\ell}\right) = \left(\frac{-3}{\ell}\right)$, and no maximal subgroups of $\mathrm{GL}_3^\varepsilon(\ell)$ come from the last two families.

We shall now proceed to describe these maximal subgroups. Whilst doing so, we will make use of a few basic facts from the theory of the classical groups, all of which may be found in [KL90].

5.1.1. $\mathcal{C}_1$ reducible subgroups. The groups in this case are stabilisers of minimal chains of submodules. That is, they stabilise a chain

$$0 \subseteq U \subseteq V$$

where U has dimension one or two.

For $\mathrm{GL}_3(\ell)$ this leads to two conjugacy classes of maximal subgroups in $\mathrm{GL}_3(\ell)$ isomorphic to $\mathbb{F}_\ell^2 \rtimes (\mathrm{GL}_1(\ell) \times \mathrm{GL}_2(\ell))$. We note that these conjugacy classes cannot be distinguished by the characteristic polynomials of their elements. However, the inverse transpose map exchanges these two classes. The description given in §4.1 thus shows that if G_M stabilises a 2-dimensional subspace of $A[\lambda]$, then it must stabilise a 1-dimensional subspace of $A[\bar{\lambda}]$. In this way, we only need to rule out the existence of 1-dimensional subrepresentations to prove the irreducibility of the action of G_M on $A[\lambda]$.

Suppose $H \leq \mathrm{GU}_3(\ell)$ stabilises an irreducible submodule U of V . Then either $U \cap U^\perp = 0$ or U , i.e., either U is non-degenerate or totally isotropic. Suppose the former holds. Then $U^\perp$ is also non-degenerate and $V = U \oplus U^\perp$ as H -modules. It follows that H is contained in $\mathrm{GU}_1(\ell) \times \mathrm{GU}_2(\ell)$.

Otherwise U is totally isotropic, and as V has dimension three, maximal totally isotropic subspaces have dimension one and thus U is one dimensional. It follows $U^\perp$ is two dimensional, and H stabilises a chain $0 \subseteq U \subseteq U^\perp \subseteq V$. An application of Witt's Lemma shows $U^\perp/U$ may be equipped with a non-degenerate Hermitian form. In fact, using further properties of the pairing, one can show H is contained in a group isomorphic to $\ell^{1+2} \rtimes (\mathrm{GU}_1(\ell) \times \mathrm{GL}_1(\ell^2))$ where ℓ^{1+2} denotes a non-abelian group of order ℓ^3 . The eigenvalues of an element in this maximal subgroup are of the form $\alpha, \alpha^{-\ell}, \beta$ where $\alpha, \beta \in \mathbb{F}_{\ell^2}^*$ and $\beta^{1+\ell} = 1$. In particular, up to exchanging α with $\alpha^{-\ell}$, one may assume the eigenvector corresponding to α gives the fixed subspace.

We note that in either situation the semisimplification V^{ss} contains a one dimensional, non-degenerate constituent. There is only one conjugacy class for each of the above types of maximal subgroup in $\mathrm{GU}_3(\ell)$. For $\ell = 2$, the group $\mathrm{GU}_1(2) \times \mathrm{GU}_2(2)$ is not maximal in $\mathrm{GU}_3(2)$.

5.1.2. $\mathcal{C}_2$ imprimitive subgroups. Here we have stabilisers of orthogonal decompositions $V = \bigoplus_{i=1}^3 V_i$, that is the groups falling into this case permute the elements of the set $\{V_1, V_2, V_3\}$.

This leads to subgroups of the form $\mathrm{GL}_1^\varepsilon(\ell)^3 \rtimes S_3$ which are maximal in $\mathrm{GL}_3^\varepsilon(\ell)$ unless $\varepsilon = +1$ and $\ell = 2$. They constitute a unique conjugacy class.

5.1.3. $\mathcal{C}_3$ field extension subgroups. Viewing V as a one dimensional vector space over $\mathbb{F}_{\ell^3}$ for $\varepsilon = +$ (resp. over $\mathbb{F}_{\ell^6}$ for $\varepsilon = -$) gives us an embedding of $\mathrm{GL}_1^\varepsilon(\ell^3)$ into $\mathrm{GL}_3^\varepsilon(\ell)$. Its normaliser, isomorphic to $\mathrm{GL}_1(\ell^3) \rtimes \mathrm{Gal}(\mathbb{F}_{\ell^3}/\mathbb{F}_\ell)$ for $\varepsilon = +1$, and $\mathrm{GU}_1(\ell^3) \rtimes \mathrm{Gal}(\mathbb{F}_{\ell^6}/\mathbb{F}_{\ell^2})$ for $\varepsilon = -1$, is a maximal subgroup

of $\mathrm{GL}_3^\varepsilon(\ell)$, except for $\mathrm{GU}_3(2)$ and $\mathrm{GU}_3(3)$. Groups arising in this manor give a single conjugacy class of maximal subgroups.

5.1.4. *$\mathcal{C}_6$ symplectic type subgroups.* This case only occurs for odd $\ell \equiv 4\varepsilon, 7\varepsilon \pmod{9}$. Here we have a single conjugacy class of maximal subgroups. The image of such a group in $\mathrm{PGL}_3^\varepsilon(\ell)$ is isomorphic to $C_3^2 \rtimes \mathrm{SL}_2(3) \cong \mathrm{ASL}_2(3)$ which has order 6^3 .

5.1.5. *$\mathcal{C}_8/\mathcal{C}_5$ -type orthogonal subgroups.* The maximal subgroups in this class stabilise a non-degenerate symmetric bilinear pairing up to scalars. They are isomorphic to the direct product of the center of $\mathrm{GL}_3^\varepsilon(\ell)$ and $\mathrm{SO}_3(\ell)$. In the notation of [BHR13], these subgroups are of type $\mathcal{C}_8$ if $\varepsilon = +1$, and of type $\mathcal{C}_5$ if $\varepsilon = -1$. For $\ell > 2$, there is a single conjugacy class of such maximal subgroups when $\gcd(3, \ell - \varepsilon) = 1$, i.e., when $\ell \not\equiv \varepsilon \pmod{3}$.

5.1.6. *$\mathcal{S}$ -type subgroups.* There is a family of $\mathcal{S}$ -type maximal subgroups, whose image in $\mathrm{PGL}_3^\varepsilon(\ell)$ is isomorphic to $\mathrm{PSL}_2(7)$, which has order 168. For $\ell > 2$, they form a single conjugacy class exactly when $\ell \not\equiv \varepsilon \pmod{3}$ and $\left(\frac{-7}{\ell}\right) = \varepsilon$. For $\varepsilon = +1$, this is equivalent to $\ell \equiv 2, 8, 11 \pmod{21}$. For $\varepsilon = -1$, this is equivalent to $\ell \equiv 10, 13, 19 \pmod{21}$ or $\ell = 3$.

5.2. **Containment in maximal subgroups.** From now on, let $A/\mathbb{Q}$ be a polarised abelian threefold with potential imaginary multiplication by M of signature $(2, 1)$, and ℓ be an admissible prime for A . While all algorithms and results in this section apply for IM abelian threefolds of signature $(2, 1)$ defined over M , we have chosen to write them specifically for $A/\mathbb{Q}$, because it simplifies the discussion of the algorithms and we have carried out these computations only for such abelian threefolds.

Recall that for a prime λ of M above ℓ , the λ -torsion $A[\lambda]$ is a three dimensional $\mathbb{F}_\lambda$ -vector space [Rib76, Prop 2.2.1], and we know by Corollary 4.3, that the image $\rho_\lambda(G_M)$ of the mod- λ representation $\rho_\lambda: G_M \rightarrow \mathrm{Aut}_{\mathbb{F}_\lambda}(A[\lambda])$ is contained in $\mathrm{CL}_3^\varepsilon(\ell)$ where $\varepsilon = \left(\frac{\Delta_M}{\ell}\right)$. We introduce the following terminology to simplify the discussion ahead.

Definition 5.2. We say an admissible prime ℓ is a $\mathcal{C}_1$ -prime or a *reducible prime* for A , if $A[\lambda]$ is not absolutely irreducible as a G_M -module for some prime λ of M above ℓ , i.e., $A[\lambda] \otimes_{\mathbb{F}_\lambda} \overline{\mathbb{F}_\lambda}$ has a proper $\overline{\mathbb{F}_\lambda}[G_M]$ -submodule.

In particular, ℓ is a $\mathcal{C}_1$ -prime if $\rho_\lambda(G_M)$ is contained in a $\mathcal{C}_1$ -type maximal subgroup of $\mathrm{CL}_3^\varepsilon(\ell)$. The converse is not true though, as $\rho_\lambda(G_M)$ not being contained in a $\mathcal{C}_1$ -type maximal subgroup only implies $A[\lambda]$ is irreducible over $\mathbb{F}_\lambda$, not absolutely irreducible.

Definition 5.3. We say an admissible prime ℓ is a $\mathcal{C}_2$ -prime (respectively $\mathcal{C}_3$ -prime or $\mathcal{C}_6$ -prime) for A , if it is not a $\mathcal{C}_1$ -prime and $\rho_\lambda(G_M)$ is contained in a $\mathcal{C}_2$ -type (respectively $\mathcal{C}_3$ -type or $\mathcal{C}_6$ -type) maximal subgroup of $\mathrm{CL}_3^\varepsilon(\ell)$ for some prime λ of M above ℓ .

Definition 5.4. We say an admissible prime ℓ is a $\mathcal{C}_8/\mathcal{C}_5$ -prime (respectively $\mathcal{S}$ -prime) for A , if $\rho_\lambda(G_M)$ is contained in a $\mathcal{C}_8/\mathcal{C}_5$ -type (respectively $\mathcal{S}$ -type) maximal subgroup of $\mathrm{CL}_3^\varepsilon(\ell)$ for some prime λ of M above ℓ .

The main algorithms in this section are Algorithms 5.15, 5.20, 5.27 and 5.33. If $\text{End}^0(A_{\overline{M}}) \cong M$, these algorithms return finite sets of rational primes which are guaranteed to contain every $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathcal{C}_8/\mathcal{C}_5$ -prime respectively. The returned sets could contain extraneous primes, and the goal of Algorithms 5.22 and 5.29 is to remove any such extraneous $\mathcal{C}_2$ or $\mathcal{C}_3$ -prime. We also show that the only possible $\mathcal{C}_6$ -primes are 5 and 7, and the only possible $\mathcal{S}$ -prime is 3.

We start by setting some notation and recalling simple facts about L -polynomials and characteristic polynomials of Frobenius elements in our setting of abelian threefolds over $\mathbb{Q}$ with potential imaginary multiplication by M of signature $(2, 1)$.

5.2.1. Shape of L -polynomial factorisations. For a polynomial h , and a positive integer n , we denote by $h^{(n)}$ the polynomial whose roots are n -th powers of the roots of h , i.e., $h^{(n)}(x) = \text{Res}_t(h(t), x - t^n)$. Consider a rational prime p of good reduction for the abelian threefold A . Let

$$(5.5) \quad L_{p,A}(x) = 1 + a_p x + b_p x^2 + c_p x^3 + p b_p x^4 + p^2 a_p x^5 + p^3 x^6$$

denote the L -polynomial of A at p . Suppose p is unramified in M and let $\ell \neq p$ be any prime. We define f_p to be the characteristic polynomial of Frob_p (or $\text{Frob}_p^{(2)}$) acting on $T_\ell(A)$ if p splits (or is inert) in M . So in either case, f_p is the characteristic polynomial under ρ_{ℓ^∞} of an element of G_M . Then we know that f_p is independent of ℓ , and furthermore

$$(5.6) \quad f_p(x) = \begin{cases} x^6 L_{p,A}(1/x) & \text{if } p \text{ splits in } M \\ x^6 L_{p,A}^{(2)}(1/x) & \text{if } p \text{ is inert in } M. \end{cases}$$

By taking the resultant of $L_{p,A}(t)$ and $x - t^2$ with respect to t , we note that

$$L_{p,C}^{(2)}(x) = 1 - (a_p^2 - 2b_p)x + \cdots - (a_p^2 - 2b_p)p^4 x^5 + p^6 x^6.$$

Since the Galois action of G_M commutes with the action of $\iota(M) \otimes \mathbb{Q}_\ell$ on $T_\ell(A)$, and we may take ℓ to split in M , i.e., $\iota(M) \otimes \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell \times \mathbb{Q}_\ell$, we deduce that f_p factorises over $\mathcal{O}_M$ as a product $f_{p,1} f_{p,2}$ of cubic polynomials $f_{p,i} = x^3 + a_{p,i}x^2 + b_{p,i}x + c_{p,i}$ that are Galois conjugate, i.e., $f_{p,2} = \overline{f_{p,1}}$.

Remark 5.7. For a prime p that is inert in M , $L_{p,A}(x)$ is a polynomial in x^2 , and hence $f_p(x) = x^6 L_{p,A}^{(2)}(1/x)$ is the square of a cubic polynomial $f_{p,1} = f_{p,2} \in \mathbb{Z}[x]$ such that $x^6 L_{p,A}(1/x) = f_{p,1}(x^2)$. Furthermore $f_{p,1}(x)$ is reducible and has a linear factor $x + p$ (see [AFP22, Lemma 3.8] for the case of Jacobians of Picard curves, and [FG26, Lemma 4.3] for the general case).

5.2.2. $\mathcal{C}_1$ reducible subgroups. Our approach to ruling out $\mathcal{C}_1$ -primes is inspired by Billerey's method for proving the reducibility of the ℓ -torsion representations of elliptic curves over number fields [Bil11]. Forthcoming work [Goo26b] of the second-named author further generalises this to rule out 1-dimensional factors from residual representations of a large class of strictly compatible systems of Galois representations.

Suppose that ℓ is a $\mathcal{C}_1$ -prime. Let λ be a prime of M above ℓ with inertia degree f . Let $\mathbb{F}_\lambda$ denote the corresponding residue field, so that $f = [\mathbb{F}_\lambda : \mathbb{F}_\ell]$. As in Section 4.3, let θ_n denote a fixed fundamental character of level n . As

$A[\lambda] \otimes_{\mathbb{F}_\lambda} \overline{\mathbb{F}}_\lambda$ is a reducible $\overline{\mathbb{F}}_\lambda[G_M]$ -module of dimension 3, the dimensions of its Jordan–Hölder factors are either $(1, 1, 1)$ or $(1, 2)$, so one of the Jordan–Hölder factors is one dimensional. Let us call the corresponding character $\tau: G_M \rightarrow \overline{\mathbb{F}}_\lambda^*$.

Lemma 5.8. *Suppose $\tau: G_M \rightarrow \overline{\mathbb{F}}_\lambda^*$ is a 1-dimensional Jordan–Hölder factor of $A[\lambda]$ for a prime λ of M above ℓ . Then there exist $a, b \in \{0, 1\}$ such that*

- (1) $\tau|_{I_\lambda} = \theta_1^a$ and $\tau|_{I_{\bar{\lambda}}} = \theta_1^b$ if ℓ is split in M ,
- (2) $\tau|_{I_\lambda} = \theta_2^{a+b\ell}$ if ℓ is inert in M .

In case (1), the local characters $\mathcal{O}_{M_\lambda}^*, \mathcal{O}_{M_{\bar{\lambda}}}^* \rightarrow \overline{\mathbb{F}}_\lambda^*$ associated to $\tau|_{I_\lambda}$ and $\tau|_{I_{\bar{\lambda}}}$ by local class field theory are $x \mapsto x^{-a} \pmod{\lambda}$ and $x \mapsto x^{-b} \pmod{\bar{\lambda}} = \bar{x}^{-b} \pmod{\lambda}$ respectively. In case (2), the associated local character is $x \mapsto x^{-a}\bar{x}^{-b} \pmod{\lambda}$.

Proof. Under local class field theory, the decomposition group at λ corresponds to the profinite completion of M_λ^* , and the inertia subgroup at λ corresponds to $\mathcal{O}_{M_\lambda}^*$. Since $\overline{\mathbb{F}}_\lambda^*$ has no element of order ℓ , the character τ is tamely ramified at λ , and hence $\tau|_{I_\lambda}$ factors through $\mathcal{O}_{M_\lambda}^*/1 + \lambda\mathcal{O}_{M_\lambda}^* \simeq \mathbb{F}_\lambda^*$. As the residual degree of ℓ is at most 2, $\tau|_{I_\lambda}$ factors through θ_2 , that is, $\tau|_{I_\lambda} = \theta_2^m$ for some m . Applying Proposition 4.6, we deduce the first statement for $\tau|_{I_\lambda}$. Replacing λ by $\bar{\lambda}$ proves the first statement for $\tau|_{I_{\bar{\lambda}}}$.

The last assertion follows from [Neu99, Chap 5, Prop 3.1 and 3.4] which say that $\theta_f(\text{Art}_\lambda(x)) = x^{-1}$ for $x \in \mathcal{O}_{M_\lambda}^*$, where x is identified with its image in $\mathbb{F}_\lambda$, under the normalisation that the local Artin map sends uniformisers to arithmetic Frobenius. $\square$

Let T denote the finite set of non-admissible primes for A . For a prime $q \geq 3, q \notin T$, let e_q denote the exponent of the group $\text{CL}_3^\varepsilon(q)$, where as usual $\varepsilon = (\frac{\Delta_M}{q})$. Set

$$(5.9) \quad n_M = \text{lcm}_{p \text{ prime}} \text{gcd}_{\substack{q \geq 3 \text{ prime} \\ q \neq p, q \notin T}} e_q.$$

Remark 5.10. Note that even though this definition depends on A through the finite set of excluded primes T , the quantity n_M only depends on the field M . Excluding any finite set of primes from the gcd term does not affect its value, and a simpler alternative definition is $n_M = \text{gcd}_{q \geq 3, q \nmid \text{disc}(M)} e_q$. The

main cases of our computational interest here are $M = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-3})$, for which, the values of n_M are 24, 24 and 72 respectively.

Lemma 5.11. *Let $\tau: G_M \rightarrow \overline{\mathbb{F}}_\lambda^*$ be a 1-dimensional Jordan–Hölder factor of $A[\lambda]$ for a prime λ of M above ℓ . Then τ^{n_M} is unramified at all primes $\mathfrak{p} \nmid \ell$ of M .*

Proof. Let $\mathfrak{p} \nmid \ell$ be a prime of M with residue characteristic p . Let $q \geq 3, q \neq p, q \notin T$ be a prime. Raynaud’s theorem [GR72, Prop. 4.7] says that A attains semistable reduction over $M(A[q])$ at any prime not above q . By Theorem 4.2, we know that the Galois group $\text{Gal}(M(A[q])/M)$ is a subgroup of $\mathbb{F}_q^* \times \text{CL}_3^\varepsilon(q)$ or $\text{CL}_3^\varepsilon(q)$, and hence its exponent divides e_q . Let us fix an

embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{\mathfrak{p}}$. Let w denote the prime of $M(A[q])$ above $\mathfrak{p}$ induced by the chosen embedding. Then the inertia group I_w at w is $I_{\mathfrak{p}} \cap G_{M(A[q])}$. So for any $\sigma \in I_{\mathfrak{p}}$, we have $\sigma^{e_q} \in I_{\mathfrak{p}} \cap G_{M(A[q])} = I_w$. Since A has semistable reduction at w and $w \nmid \ell$, Grothendieck's inertial criterion [GR72, Prop. 3.5] implies that I_w acts unipotently on the Tate module $T_{\ell}(A)$, and hence on $A[\ell]$. Since τ is a 1-dimensional subquotient, we deduce that $\tau|_{I_w} = 1$ and hence $\tau^{e_q}|_{I_{\mathfrak{p}}} = 1$. Therefore the order of $\tau|_{I_{\mathfrak{p}}}$ divides the gcd term in Eq. (5.9) and so it divides n_M . $\square$

Proposition 5.12. *Let ℓ be a semistable admissible prime and λ be a prime of $\mathcal{O}_M$ above ℓ . Suppose that the action of G_M on $A[\lambda]$ is not absolutely irreducible, and let $\tau: G_M \rightarrow \overline{\mathbb{F}}_{\lambda}^*$ be a 1-dimensional Jordan–Hölder factor of $A[\lambda]$. Let $\mathfrak{p}$ be a prime of M of residue characteristic $p \neq \ell$, such that A has good reduction at $\mathfrak{p}$. Suppose $\mathfrak{p}^h = (\gamma)$ for some $\gamma \in \mathcal{O}_M$ and $h \geq 1$. Then there exists $\alpha \in \{1, \gamma, \bar{\gamma}, \gamma\bar{\gamma}\}$ such that*

$$(5.13) \quad \tau^{n_M h}(\text{Frob}_{\mathfrak{p}}) \equiv \alpha^{n_M} \pmod{\lambda}$$

Proof. Let $\psi = \tau^{n_M}$. Since the global Artin reciprocity map is trivial on principal ideles, compatibility of the global and local Artin maps gives $\prod_v \psi(\text{Art}_v(\gamma)) = \psi(\text{Art}(\gamma)) = 1$, where the product ranges over all places v of M and Art_v is the local Artin reciprocity map at v . Using the facts that the Artin map at the complex infinite place is trivial, $\text{ord}_v(\gamma) = 0$ for all $v \neq \mathfrak{p}$, and ψ is unramified outside ℓ by Lemma 5.11, this equality simplifies to:

$$(5.14) \quad \psi(\text{Art}_{\mathfrak{p}}(\gamma)) \prod_{v|\ell} \psi(\text{Art}_v(\gamma)) = 1$$

The first term is $\psi(\text{Art}_{\mathfrak{p}}(\gamma)) = \psi(\text{Frob}_{\mathfrak{p}}^h) = \tau^{n_M h}(\text{Frob}_{\mathfrak{p}})$. By Lemma 5.8, we get that $\prod_{v|\ell} \tau(\text{Art}_v(\gamma)) \equiv \gamma^{-a} \bar{\gamma}^{-b} \pmod{\lambda}$ for some $a, b \in \{0, 1\}$. Raising the last congruence to the n_M -th power, and putting them back into Eq. (5.14), gives $\tau^{n_M h}(\text{Frob}_{\mathfrak{p}}) \equiv (\gamma^a \bar{\gamma}^b)^{n_M} \pmod{\lambda}$, which is the desired result. $\square$

Proposition 5.12 readily yields the following algorithm for detecting all possibly $\mathcal{C}_1$ -primes for an abelian threefold A , given sufficiently many L -polynomials for A .

Algorithm 5.15 (Possibly $\mathcal{C}_1$ -primes).

Input:

- an integer N that is a multiple of all primes of bad reduction for a polarised abelian threefold $A/\mathbb{Q}$.
- an imaginary quadratic field M such that A has potential imaginary multiplication by M of signature $(2, 1)$.
- L -polynomials of $A/\mathbb{Q}$ at each prime in the set S of all primes less than $B > 0$, that split in M and do not divide N .

Output: a finite superset of the semistable $\mathcal{C}_1$ -primes, or 0.

- (1) Compute a positive integer e divisible by n_M using Eq. (5.9).
- (2) For each $p \in S$, choose a prime $\mathfrak{p}$ of $\mathcal{O}_M$ above p . Let h_p be the order of $\mathfrak{p}$ in the class group of M , and γ_p a generator of $\mathfrak{p}^{h_p}$. Calculate $f_p(x) =$

$x^6 L_{p,A}(1/x)$ as in Eq. (5.6) from the given L -polynomial, and use resultants to compute $f_p^{(eh_p)}(x)$. Evaluate at $x = 1, p^{eh_p}, \gamma_p^e$ to compute

$$R_p = f_p^{(eh_p)}(1) \cdot f_p^{(eh_p)}(p^{eh_p}) \cdot \text{Nm}_{M/\mathbb{Q}} \left(f_p^{(eh_p)}(\gamma_p^e) \right).$$

- (3) Calculate $R = \gcd_{p \in S} (pR_p)$. If $R = 0$, return 0. Otherwise return the set of prime numbers dividing R .

Theorem 5.16. *Let $A/\mathbb{Q}$ be a polarised abelian threefold, and M be an imaginary quadratic field such that $M \cong \text{End}^0(A_{\overline{\mathbb{Q}}})$. Suppose Assumption 5.1 holds. Then, for B large enough, Algorithm 5.15 returns a finite superset of the semistable $\mathcal{C}_1$ -primes for A .*

Proof. We work with the notation in Algorithm 5.15. To show that the algorithm does not return 0 for B large enough, we need to produce a single prime p with $R_p \neq 0$. Let h_M denote the class number of M . By Assumption 5.1, choose a rational prime $\ell_0 \equiv 1 \pmod{e}$ splitting in M , and large enough so that $\ell_0^2 + \ell_0 + 1 > h_M$, and $\rho_{\lambda_0}: G_M \rightarrow \text{GL}_3(\mathbb{F}_{\ell_0})$ is surjective for λ_0 above ℓ_0 . Consider a generator g of $\mathbb{F}_{\ell_0}^*$, and let g also denote its image under a fixed natural embedding $\mathbb{F}_{\ell_0}^* \hookrightarrow \text{GL}_3(\mathbb{F}_{\ell_0})$. By applying the Chebotarev density theorem to $M(A[\lambda_0])/M$, we know that there exists a prime $\mathfrak{p}$ of M , lying over a rational prime $p \neq \ell_0$, which splits in M and does not divide N , such that $\rho_{\lambda_0}(\text{Frob}_{\mathfrak{p}})$ is conjugate to g .

Fix a place of $\overline{\mathbb{Q}}$ above λ_0 . We claim that no root of f_p has a reduction whose h_p -th power is in $\mathbb{F}_{\ell_0}$. Since $f_p \pmod{\lambda_0}$ is the product of the characteristic polynomials of $\rho_{\lambda_0}(\text{Frob}_{\mathfrak{p}})$ and of $\rho_{\bar{\lambda}_0}(\text{Frob}_{\mathfrak{p}})$, its roots are $\{g^{\ell_0^i}, pg^{-\ell_0^i} | 0 \leq i \leq 2\}$. Since the smallest power of g to lie in $\mathbb{F}_{\ell_0}$ is the $(\ell_0^2 + \ell_0 + 1)$ -th power, the same is true for all of these elements. Since $h_p \leq h_M < \ell_0^2 + \ell_0 + 1$, the claim follows.

Assume on the contrary that $R_p = 0$. Since every root of f_p has complex absolute value $\sqrt{p}$ because of the Weil conjectures, R_p can be zero only if $f_p^{(eh_p)}(\gamma_p^e) = 0$. That is, there is a root α of f_p such that $\alpha^{eh_p} = \gamma_p^e$. Thus $\alpha^{h_p} = \zeta \gamma_p$ for some root of unity ζ with $\zeta^e = 1$. Consider reduction at the chosen place above λ_0 . Since λ_0 has residue degree 1, and $e|\ell_0 - 1$, we know that the reductions of both γ_p and ζ lie in $\mathbb{F}_{\ell_0}$. This implies that the reduction of α^{h_p} also lies in $\mathbb{F}_{\ell_0}$, contradicting the claim just proven. Therefore $R_p \neq 0$. So, for large enough B , the algorithm returns a finite set of primes.

Let ℓ be a semistable $\mathcal{C}_1$ -prime for A . So $A[\lambda]$ is not absolutely irreducible for some prime λ above ℓ , and let τ be a 1-dimensional Jordan–Hölder factor of $A[\lambda]$. Let $p \in S$. If $p = \ell$, then ℓ clearly divides pR_p . If $p \neq \ell$, then $\tau(\text{Frob}_{\mathfrak{p}})$ is an eigenvalue of $\rho_{\lambda}(\text{Frob}_{\mathfrak{p}})$, thus $f_p(\tau(\text{Frob}_{\mathfrak{p}})) \equiv 0 \pmod{\lambda}$. Proposition 5.12 says that $\tau^{eh_p}(\text{Frob}_{\mathfrak{p}}) \equiv \alpha^e \pmod{\lambda}$ for some $\alpha \in \{1, \gamma_p, \bar{\gamma}_p, \gamma_p \bar{\gamma}_p = \text{Nm}(\mathfrak{p})^{h_p} = p^{h_p}\}$. Hence $f_p^{(eh_p)}(\alpha^e) \equiv 0 \pmod{\lambda}$, which shows that $\ell | R_p$. So ℓ divides R . $\square$

5.2.3. $\mathcal{C}_2$ imprimitive subgroups. We start with the following lemma about characteristic polynomials of certain elements in $\mathcal{C}_2$ -type maximal subgroups.

Lemma 5.17. *Let V be a three dimensional vector space over a finite field $\mathbb{F}$ of characteristic $\ell \geq 5$. Suppose $\sigma \in \mathrm{GL}(V)$ preserves a decomposition $V = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \langle v_3 \rangle$. Write $D(V) = \{\langle v_1 \rangle, \langle v_2 \rangle, \langle v_3 \rangle\}$. The following hold:*

- (1) *if the action of σ on $D(V)$ has order 3, then its characteristic polynomial equals $x^3 + a$ for some $a \in \mathbb{F}^*$;*
- (2) *if the action of σ on $D(V)$ has order 2, then its characteristic polynomial equals $(x + a)(x^2 + b)$ for some $a, b \in \mathbb{F}^*$.*

Moreover if σ acts non-trivially on $D(V)$ and its minimal polynomial equals

- (a) *either $(x - 1)(x - d)$ for some $d \in \mathbb{F}^*$;*
- (b) *or $(x - 1)(x - d)(x - \gamma)$ for some $d \in \mathbb{F}_\ell^*$ and $\gamma \in \mathbb{F} \setminus \mathbb{F}_\ell$;*

then σ acts as a 2-cycle on $D(V)$ and $d = -1$.

Proof. The group of elements which preserve $D(V)$ is isomorphic to $\mathrm{GL}_1(\mathbb{F})^3 \rtimes S_3$. As $\ell \geq 5$, the elements in $\mathrm{GL}_1(\mathbb{F})^3 \rtimes S_3$ act semisimply by Maschke's Theorem, so their minimal polynomials are squarefree. In particular, $d \neq 1$.

Let us suppose $\sigma \in \mathrm{GL}(V)$ acts on $D(V)$ as a 3-cycle. Then there exists $a_1, a_2, a_3 \in \mathbb{F}^*$ such that $\sigma v_i = a_i v_{i+1}$ where the indices are taken modulo 3. In particular, σ has trace zero and the minimal polynomial of σ^3 is $t - a_1 a_2 a_3$, that is, σ^3 is a scalar matrix. Moreover, as $(1, 2, 3)$ is an even permutation, $\det(\sigma) = a_1 a_2 a_3$.

Let us now show that the minimal polynomial of σ cannot be as in (a) or (b). We shall suppose for a contradiction that it is. Then σ has an eigenvalue equal to 1. As σ^3 is a scalar matrix, we find that $a_1 a_2 a_3 = 1$. Thus $\det(\sigma) = 1$ and σ has order 3. However, this is incompatible with the minimal polynomials in (a) and (b). Indeed, if the minimal polynomial of σ was as in (a), the determinant of σ would either equal d or d^2 , both of which are not equal to 1 since d is forced to have order 3 in $\mathbb{F}^*$. The minimal polynomial cannot be as in (b) either, since in this case the determinant is $d\gamma$, which does not belong to $\mathbb{F}_\ell$.

Let us now suppose $\sigma \in \mathrm{GL}(V)$ acts on $D(V)$ as a 2-cycle. Without loss of generality, we may suppose σ fixes $\langle v_3 \rangle$. Then there exists $a_1, a_2, a_3 \in \mathbb{F}^*$ such that $\sigma v_1 = a_1 v_2, \sigma v_2 = a_2 v_1, \sigma v_3 = a_3 v_3$. We immediately verify that the characteristic polynomial of σ is $x^3 - a_3 x^2 - a_1 a_2 x + a_1 a_2 a_3$, which factors as $(x - a_3)(x^2 - a_1 a_2)$.

Let us now show that if the minimal polynomial of σ is as given in (a) or (b), then $d = -1$. As the trace of σ equals a_3 and a_3 is an eigenvalue of σ , we see that the eigenvalues of σ are of the form $c, -c, a_3$ for some c . Since $-\gamma$ is not an eigenvalue of σ , we deduce $\{1, d\} = \{\pm c\}$. $\square$

We now describe consequences of $\rho_\lambda(G_M)$ being contained in a $\mathcal{C}_2$ -type maximal subgroup, using Lemma 5.17, and the characterisation in Proposition 4.6 of the action of inertia at ℓ on $A[\lambda]$.

Proposition 5.18. *Let λ be a prime of $\mathcal{O}_M$ lying above an admissible prime ℓ for A . Suppose that $\rho_\lambda(G_M)$ acts absolutely irreducibly on $A[\lambda]$ and is contained in a $\mathcal{C}_2$ -type maximal subgroup of $\mathrm{CL}_3^\varepsilon(A[\lambda])$.*

Then there exists a non-trivial abelian extension L/M of degree ≤ 3 unramified outside ℓ and the primes of bad reduction for A , such that

- if $[L : M] = 2$ and the image of $\sigma \in G_M$ in $\text{Gal}(L/M)$ is non-trivial then the minimal polynomial of $\rho_\lambda(\sigma)$ equals $x^3 + ax^2 + bx + ab$ for some $a, b \in \mathbb{F}_\lambda^*$;
- if $[L : M] = 3$ and the image of $\sigma \in G_M$ in $\text{Gal}(L/M)$ is non-trivial then $\text{Tr } \rho_\lambda(\sigma) \equiv 0 \pmod{\lambda}$.

If moreover, A has semistable reduction at every prime lying above ℓ and $\ell \geq 5$, then L/M is unramified at ℓ .

Proof. Being contained in a $\mathcal{C}_2$ -type subgroup means $\rho_\lambda(G_M)$ stabilises a decomposition $A[\lambda] = \bigoplus_{i=1}^3 \langle v_i \rangle$. Moreover, as $\rho_\lambda(G_M)$ acts irreducibly on $A[\lambda]$, its action on $D(\lambda) := \{\langle v_1 \rangle, \langle v_2 \rangle, \langle v_3 \rangle\}$ contains a 3-cycle. The extension L' of M cut out by the kernel of the action of $\rho_\lambda(G_M)$ on $D(\lambda)$ has Galois group either C_3 or S_3 . If $\text{Gal}(L'/M) \cong C_3$ we write $L = L'$. If $\text{Gal}(L'/M) \cong S_3$, we let L denote the unique quadratic extension of M contained in L' . Applying the first part of Lemma 5.17, we see that it only remains to prove the final statement.

As $\rho_\lambda(G_M)$ is contained in a $\mathcal{C}_2$ -type subgroup, its order is coprime to ℓ and thus acts semisimply by Maschke's Theorem. In particular, the restriction of ρ_λ to an inertia group I of a prime above ℓ is fully determined by Proposition 4.6. Let us suppose for a contradiction that some $\sigma \in I$ acts non-trivially on $D(\lambda)$. We shall first consider the case that ℓ splits in M and then afterwards that it is inert in M .

If ℓ splits in M then $\rho_\lambda|_I = 2\mathbb{1} + \theta_1$ or $\mathbb{1} + 2\theta_1$. Indeed, the other possibilities described in Proposition 4.6 lead to $\rho_\lambda(I)$ containing a cyclic subgroup of order $\geq \ell^2 - 1$, which is incompatible with the fact that the largest cyclic subgroup of the $\mathcal{C}_2$ -type maximal subgroup of $\text{GL}_3(\ell)$ has order $3(\ell - 1)$. Thus lemma 5.17 implies $\theta_1(\sigma) = -1$. But θ_1 surjects onto $\mathbb{F}_\ell^*$ which has order $\ell - 1 \geq 4$. Thus L/M is unramified at ℓ if ℓ splits in M .

If ℓ is inert in M then $\rho_\lambda|_I = 2\theta_2 + \theta_2^\ell$ or $\mathbb{1} + \theta_1 + \theta_2$ for some fundamental character θ_2 of level 2. Indeed, the other possibilities described in Proposition 4.6 lead to $\rho_\lambda(I)$ containing a cyclic subgroup of order $\geq (\ell - 1)(\ell^3 + 1)$, which is incompatible with the fact that the largest cyclic subgroup of the $\mathcal{C}_2$ -type maximal subgroup of $\text{CU}_3(\ell)$ has order $3(\ell^2 - 1)$. If $\rho_\lambda|_I = \mathbb{1} + \theta_1 + \theta_2$, Lemma 5.17 implies that the image of θ_1 is contained in $\{\pm 1\}$, contradicting $\ell \geq 5$. Thus suppose $\rho_\lambda|_I = 2\theta_2 + \theta_2^\ell$. We may write $\rho_\lambda(\sigma) = \theta_2(\sigma)\sigma'$ for some $\sigma' \in \text{GL}(A[\lambda])$. The action of σ' on $D(\lambda)$ coincides with that of σ . As the minimal polynomial of σ' is $(x - 1)(x - \theta_2^{\ell-1}(\sigma))$, applying Lemma 5.17 we deduce $\theta_2^{\ell-1}(\sigma) = -1$. However, this contradicts the fact that θ_2 surjects onto $\mathbb{F}_{\ell^2}^*$ which has order $\ell^2 - 1 \geq 24$. $\square$

Remark 5.19. Let us now bound the possible conductors of such quadratic or cyclic cubic extensions L/M . Since $L \subseteq M(A[\lambda])$, we know that this conductor divides the conductor of A . But we can say more. Let $\mathfrak{p}$ be a prime ramifying in the extension L/M with residual characteristic p . If p does not divide $[L : M]$, then $\mathfrak{p}$ is tamely ramified and hence the exponent of $\mathfrak{p}$ in the conductor of L/M is 1. If p divides $[L : M]$, then $p = [L : M] \in \{2, 3\}$ and the exponent of $\mathfrak{p}$ in the conductor of L/M is at most $1 + \frac{p}{p-1} \text{ord}_{\mathfrak{p}}(p) \leq 5$, by [Ser87, Corollaire pg 215].

We now adapt Proposition 5.18 to turn it into an algorithm for detecting all possibly $\mathcal{C}_2$ -primes for an abelian threefold A . The first step is to enumerate, using class field theory and Remark 5.19, the finite set of quadratic or cyclic cubic extensions L'/M , that are unramified outside the set of primes of semistable reduction for A . The field extension L/M appearing in Proposition 5.18 must be one of these L' . So, for each of these extensions L' , and for sufficiently many primes p inert in L' , if the L -polynomial of A at p is known, the congruences of Proposition 5.18 will lead to non-trivial divisibility conditions on the $\mathcal{C}_2$ -primes. In Algorithms 5.20 and 5.27, we try to optimize the number of primes to be considered for ensuring the existence of one that is inert in any possible extension L'/M . We do this by working with a basis of homomorphisms from G_M to $\mathbb{F}_2$ or $\mathbb{F}_3$, and making use of linear algebra.

Algorithm 5.20 (Possibly $\mathcal{C}_2$ -primes).

Input:

- an integer N that is a multiple of all primes of bad reduction for a polarised abelian threefold $A/\mathbb{Q}$.
- an imaginary quadratic field M such that A has potential imaginary multiplication by M of signature $(2, 1)$.
- L -polynomials of $A/\mathbb{Q}$ at each prime p , not dividing N , less than some bound B .

Output: a finite superset of the $\mathcal{C}_2$ -primes, or 0.

- (1) Use the conductor exponent bounds from Remark 5.19 to compute a basis $\{\chi_j : 1 \leq j \leq d\}$ for the $\mathbb{F}_2$ -vector space H of Hecke characters of M unramified outside N , and having order dividing 2. We treat these characters as homomorphisms $G_M \rightarrow \mathbb{F}_2$.
- (2) For each prime $p < B, p \nmid N$, use Eq. (5.6) to construct the polynomial $f_p(x) \in \mathbb{Z}[x]$ from the L -polynomial. Write $f_p(x) = f_{p,1}f_{p,2}$ for certain cubic polynomials $f_{p,i}(x) = x^3 + a_{p,i}x^2 + b_{p,i}x + c_{p,i} \in \mathcal{O}_M[x]$, with $\overline{f_{p,1}} = f_{p,2}$, as follows:
 - If p splits in M , factorise $f_p(x)$ over $\mathcal{O}_M$. If it has exactly two irreducible factors of degree 3, call them $f_{p,1}(x)$ and $f_{p,2}(x)$. If not, move to the next prime.
 - If p is inert in M , let $f_{p,1}$ be the cubic polynomial in $\mathbb{Z}[x]$ such that $f_p(x) = f_{p,1}(x)^2$ and let $f_{p,2} = f_{p,1}$.
- (3) Let S denote the set of primes p such that $v_p := a_{p,1}b_{p,1} - c_{p,1} \neq 0$. Let $S = \{p_i : 1 \leq i \leq m\}$. For each prime $p_i \in S$, choose a prime ideal $\mathfrak{p}_i$ above p_i . Construct the $m \times d$ matrix $A \in M_{m,d}(\mathbb{F}_2)$ whose $(i, j)^{th}$ entry is $\chi_j(\mathfrak{p}_i) = \chi_j(\text{Frob}_{\mathfrak{p}_i}) \in \mathbb{F}_2$.
- (4) If $\text{rank}(A) < d$, return 0.
- (5) Return the union of the set of all rational primes outputted by Algorithm 5.27, and the set of rational primes dividing

$$6N \prod_{p \in S} \text{Nm}_{M/\mathbb{Q}}(v_p).$$

Theorem 5.21. *Let $A/\mathbb{Q}$ be a polarised abelian threefold, and M be an imaginary quadratic field such that $M \cong \text{End}^0(A_{\overline{\mathbb{Q}}})$. Suppose Assumption 5.1*

holds. Then, for B large enough, Algorithm 5.20 returns a finite superset of the $\mathcal{C}_2$ -primes for A .

Proof. By Assumption 5.1, choose a rational prime ℓ splitting in M , and λ above ℓ so that $\rho_\lambda(G_M) = \mathrm{GL}_3(\ell)$. Let $M(A[\lambda])$ denote the fixed field of $\ker(\rho_\lambda)$. It contains a unique quadratic extension of M , which corresponds to the quotient $\mathrm{GL}_3(\ell) \xrightarrow{\det} \mathbb{F}_\ell^* \rightarrow \mathbb{F}_\ell^*/\mathbb{F}_\ell^{*2}$.

Let I be the inertia group at λ . By Proposition 4.6, we know that $\det \rho_\lambda|_I = \theta_1$ or θ_1^2 . If it is the latter, we deduce from $\det \rho_\lambda \det \rho_{\bar{\lambda}} = \det \rho_\ell = \chi_\ell^3$ that $\det \rho_{\bar{\lambda}}|_I = \theta_1$. By the last part of Theorem 4.2, we know that $\rho_{\bar{\lambda}} = {}^\sigma \rho_\lambda$ where $\sigma \in G_\mathbb{Q} \setminus G_M$. Therefore $\theta_1 = \det {}^\sigma \rho_\lambda|_I = \det \rho_\lambda|_{\sigma I \sigma^{-1}}$. Hence the restriction of $\det \rho_\lambda$ to the inertia group at $\bar{\lambda}$ is θ_1 . Hence this quadratic extension is ramified at either λ or $\bar{\lambda}$.

Let M_2 denote the compositum of the quadratic extensions cut out by the order 2 Hecke characters χ_j from Step 1 of Algorithm 5.20. Since M_2 is unramified outside N , it is disjoint from $M(A[\lambda])$. Therefore, Chebotarev density theorem applied to the Galois extension $M_2 \cdot M(A[\lambda])$ of M with Galois group $(\mathbb{Z}/2\mathbb{Z})^d \times \mathrm{GL}_3(\ell)$, guarantees the existence of primes $\mathfrak{p}_i|p_i$ in M such that the characteristic polynomial of $\rho_\lambda(\mathrm{Frob}_{\mathfrak{p}_i})$ is irreducible over $\mathbb{F}_\ell$ (so that $f_{p_i,1}$ is irreducible over $\mathbb{Z}_\ell$ and hence $v_{p_i} \neq 0$) and $\chi_j(\mathfrak{p}_i) = \delta_{i,j}$. So for B large enough, the matrix A constructed in Step 3 of Algorithm 5.20 will have full rank. This shows that the algorithm returns a finite set of primes, and not 0.

Let $\ell \geq 5$ be a $\mathcal{C}_2$ -prime for A . If A does not have semistable reduction at ℓ , then $\ell \mid N$ and we are done. So we may assume that ℓ is a semistable prime for A . Then $\rho_\lambda(G_M)$ acts irreducibly on $A[\lambda]$ and is contained in a $\mathcal{C}_2$ -type maximal subgroup for a prime $\lambda|\ell$. Let L/M be the non-trivial abelian extension from Proposition 5.18 unramified outside the bad primes for A .

If $[L : M] = 2$, there exists a non-trivial character $\chi \in H$ which cuts out L . Since the matrix A has full rank, we deduce that there exists a prime $p \in S$ and $\mathfrak{p}|p$ such that $\chi(\mathfrak{p}) \neq 0$. This means that $\mathrm{Frob}_{\mathfrak{p}}$ is non-trivial in $\mathrm{Gal}(L/M)$. Hence Proposition 5.18 implies that either $v_p \equiv 0 \pmod{\lambda}$ or $v_p \equiv 0 \pmod{\bar{\lambda}}$, and therefore $\mathrm{Nm}_{M/\mathbb{Q}}(v_p) \equiv 0 \pmod{\ell}$.

If $[L : M] = 3$, Proposition 5.18 says that $\mathrm{Tr} \rho_\lambda(\sigma) \equiv 0 \pmod{\lambda}$ for every non-trivial $\sigma \in \mathrm{Gal}(L/M)$. Theorem 5.28 then guarantees that ℓ is in the set of primes returned by Algorithm 5.27. $\square$

While Algorithm 5.20 turns the problem of determining $\mathcal{C}_2$ -primes into a finite problem, the output can include false positives, i.e., extraneous primes ℓ for which the image $\rho_\lambda(G_M)$ is not contained in a $\mathcal{C}_2$ -type maximal subgroup. So it is useful to have an algorithm, that can decide for a given prime ℓ , whether ℓ can possibly be a $\mathcal{C}_2$ -prime by inspecting the reductions modulo ℓ of characteristic polynomials of Frobenius elements. Algorithm 5.22 serves this purpose. In particular, it is useful to treat the primes of non-semistable reduction for A , for which Algorithm 5.20 says nothing.

Algorithm 5.22 (Weeding out extraneous primes from possibly $\mathcal{C}_2$ -primes).

Input:

- an imaginary quadratic field M such that the polarised abelian three-fold $A/\mathbb{Q}$ has potential imaginary multiplication by M of signature $(2, 1)$.
- L -polynomials of $A/\mathbb{Q}$ at each prime $p < B$ of good reduction for A that splits in M , for some bound B .
- a rational prime ℓ that is unramified in M .

Output: true or false depending on whether ℓ is possibly a $\mathcal{C}_2$ -prime or not.

- (1) For each prime p , using the given L -polynomial, follow Step 2 of Algorithm 5.20 to construct $f_{p,i}(x) = x^3 + a_{p,i}x^2 + b_{p,i}x + c_{p,i}$, with $\overline{f_{p,1}} = f_{p,2}$.
- (2) Choose a prime λ above ℓ in M , and consider the reduction of $f_{p,1}(x)$ modulo λ . If the reduction does not fully factor in $\mathbb{F}_\lambda[x]$ into linear polynomials, and is not of the form $x^3 - a$, and $v_p \pmod{\lambda} \neq 0$ and $v_p \pmod{\bar{\lambda}} \neq 0$ where $v_p = a_{p,1}b_{p,1} - c_{p,1}$ then return False.
- (3) If no return statement has been executed while running Steps 1 to 2, then return True.

Now we want to show that every extraneous prime ℓ will be weeded out by Algorithm 5.22, if sufficiently many L -polynomials are available. We prove this in Proposition 5.24. The main ingredient for this is an understanding of the intersection of the $\mathcal{C}_2$ and $\mathcal{C}_3$ -type maximal subgroups, which Lemma 5.23 presents in some generality.

Lemma 5.23. *Let $\mathbb{F}$ be a finite field of size q and $\mathbb{F}'/\mathbb{F}$ be an extension of odd prime degree s . Suppose H is a subgroup of $\mathrm{GL}_1(\mathbb{F}') \rtimes \mathrm{Gal}(\mathbb{F}'/\mathbb{F})$ such that $H \cap \mathrm{GL}_1(\mathbb{F}') \leq \{x \in \mathrm{GL}_1(\mathbb{F}') \mid x^s \in \mathrm{GL}_1(\mathbb{F})\}$. Then there exists a decomposition $\mathbb{F}' = \bigoplus_{i=0}^{s-1} V_i$ of $\mathbb{F}$ -vector spaces such that H preserves the set $D = \{V_i \mid 0 \leq i \leq s-1\}$.*

Proof. Let $\sigma = \mathrm{Frob}_q$ be a generator of the cyclic group $\mathrm{Gal}(\mathbb{F}'/\mathbb{F}) \simeq \mathbb{Z}/s\mathbb{Z}$. Since $H/(H \cap \mathrm{GL}_1(\mathbb{F}')) \leq \mathrm{Gal}(\mathbb{F}'/\mathbb{F})$ and s is prime, we know that $H \leq \langle H \cap \mathrm{GL}_1(\mathbb{F}'), \alpha\sigma \rangle$ for some $\alpha \in \mathrm{GL}_1(\mathbb{F}')$. Since $\mathrm{GL}_1(\mathbb{F}')$ is cyclic, its intersection with H is cyclic as well. Let h denote a generator of $H \cap \mathrm{GL}_1(\mathbb{F}')$. We are given that $h^s \in \mathrm{GL}_1(\mathbb{F})$.

Case 1: $h \in \mathrm{GL}_1(\mathbb{F})$. Then the action of $H \cap \mathrm{GL}_1(\mathbb{F}') = \langle h \rangle$ preserves any decomposition of $\mathbb{F}'$ into $\mathbb{F}$ -linear subspaces. So, all we need to find is a decomposition that is preserved by $\alpha\sigma$. If $\alpha \in \mathbb{F}$, a decomposition preserved by σ is also preserved by $\alpha\sigma$, and the normal basis theorem yields a decomposition preserved by σ . Suppose $\alpha \notin \mathbb{F}$. Then the element α generates the field $\mathbb{F}'$ over $\mathbb{F}$ because s is prime, and $(\alpha\sigma)^s = \mathrm{Nm}(\alpha)$. So the minimal polynomial of the $\mathbb{F}$ -linear operator $\alpha\sigma$ is equal to $T^s - \mathrm{Nm}(\alpha)$ and $\mathbb{F}' \simeq \mathbb{F}[T]/(T^s - \mathrm{Nm}(\alpha))$. This isomorphism yields a decomposition $\mathbb{F}' = \bigoplus_{i=0}^{s-1} \mathbb{F} \cdot T^i$, which is preserved by the operator $\alpha\sigma$.

Case 2: $h \notin \mathrm{GL}_1(\mathbb{F})$. Let $a = h^s \in \mathrm{GL}_1(\mathbb{F})$. Since raising to the s^{th} power is not an isomorphism on $\mathbb{F}$, we deduce that $q \equiv 1 \pmod{s}$. The element h generates the field $\mathbb{F}'$ over $\mathbb{F}$ because s is prime, so that $\mathbb{F}' = \mathbb{F}[h] \cong \mathbb{F}[T]/(T^s - a)$ and $\mathrm{Nm}(h) = a$. Let $\omega \in \mathbb{F}$ be a primitive s^{th} root of unity, such that $\sigma(h) = \omega h$.

Since $(\alpha\sigma)^s = \text{Nm}(\alpha) \in H \cap \text{GL}_1(\mathbb{F}) = \langle h^s \rangle = \langle a \rangle$, we deduce that $\text{Nm}(\alpha) = a^n$ for some n . Let $n = ks + m$ for integers k, m . Then the element $\sigma_1 = h^{-m}\alpha\sigma \in H$ satisfies $\sigma_1^s = \text{Nm}(h^{-m}\alpha) = a^{n-m} = a^{ks}$. So, the minimal polynomial of σ_1 over $\mathbb{F}$, which is equal to $T^s - a^{ks}$, completely factors as $\prod_{i=0}^{s-1} (T - a^k \omega^i)$. Let $\mathbb{F}' = \bigoplus_{i=0}^{s-1} V_i$ be the corresponding decomposition into eigenspaces. Since $\sigma_1(hx) = h^{-m}\alpha\sigma(hx) = \sigma(h)\sigma_1(x) = \omega h\sigma_1(x)$, we deduce that the action of h permutes the eigenspaces of σ_1 . Therefore, we conclude that $H \leq \langle h, \alpha\sigma \rangle = \langle h, \sigma_1 \rangle$ preserves the set $D = \{V_i \mid 0 \leq i \leq s-1\}$. $\square$

Proposition 5.24. *Let $A/\mathbb{Q}$ be a polarised abelian threefold, and M be an imaginary quadratic field such that $M \cong \text{End}^0(A_{\overline{\mathbb{Q}}})$. Suppose $\ell > 7$ is a rational prime that is not a $\mathcal{C}_1$ -prime or a $\mathcal{C}_8/\mathcal{C}_5$ -prime for A .*

Suppose B is large enough, i.e., sufficiently many L -polynomials for A are given as input to Algorithm 5.22. Then ℓ is not a $\mathcal{C}_2$ -prime for A if and only if Algorithm 5.22 returns false.

Proof. Let $\lambda|\ell$ be a prime of $\mathcal{O}_M$, and $\mathbb{F} = \mathbb{F}_\lambda$. The if direction follows in a straightforward way from Lemma 5.17, which implies that the characteristic polynomials of elements of the $\mathcal{C}_2$ -type maximal subgroup have one of the following shapes: $\prod_{i=1}^3 (x - a_i)$, $x^3 - a_1$ or $(x - a_1)(x^2 - a_2)$, for some $a_i \in \mathbb{F}$.

Now we prove the converse. Since ℓ is not a $\mathcal{C}_1$ -prime, we know that $\rho_\lambda(G_M)$ acts irreducibly on $\mathbb{F}^3$. We are given that ℓ is not a $\mathcal{C}_2$ -prime or a $\mathcal{C}_8/\mathcal{C}_5$ -prime. Since $\ell > 7$, we know by Sections 5.2.5 and 5.2.7 that $\rho_\lambda(G_M)$ is not contained in a $\mathcal{C}_6$ -type or $\mathcal{S}$ -type maximal subgroup. Therefore, by Proposition 4.7 and the classification in Section 5.1 of maximal subgroups of $\text{CL}_3^\varepsilon(\ell)$ not containing $\text{SL}_3^\varepsilon(\ell)$, we get that either $\rho_\lambda(G_M) = \text{CL}_3^\varepsilon(\ell)$ or $\rho_\lambda(G_M)$ is contained in a $\mathcal{C}_3$ -type maximal subgroup.

If $\rho_\lambda(G_M) = \text{CL}_3^\varepsilon(\ell)$, the Chebotarev density theorem guarantees the existence of primes $\mathfrak{p}|p$ such that the characteristic polynomial of $\rho_\lambda(\text{Frob}_{\mathfrak{p}})$ is an irreducible cubic polynomial over $\mathbb{F}$ not of the form $x^3 - a$. In other words, the reduction in $\mathbb{F}[x]$ of the polynomial $f_{p,1}$ fits the conditions being checked in Step 2 of Algorithm 5.22. So for B large enough, i.e., when sufficiently many L -polynomials for A are given as input, Algorithm 5.22 will return False.

Now suppose $\rho_\lambda(G_M)$ is contained in a $\mathcal{C}_3$ -type maximal subgroup. Let $\mathbb{F}'|\mathbb{F}$ be the degree 3 extension in a fixed algebraic closure.

Case 1: ℓ is split in M . Fix a natural inclusion $\psi: \mathbb{F}'^* \rtimes \text{Gal}(\mathbb{F}'/\mathbb{F}) \hookrightarrow \text{GL}_3(\mathbb{F})$ such that $\rho_\lambda(G_M) \subseteq \text{im}(\psi)$. Let $H = \{x \in \mathbb{F}'^* \mid x^3 \in \mathbb{F}^*\}$. If $\rho_\lambda(G_M) \cap \psi(\mathbb{F}'^*) \leq \psi(H)$, then Lemma 5.23 say that $\rho_\lambda(G_M)$ preserves a decomposition $\mathbb{F}' = \bigoplus_{i=1}^3 \langle v_i \rangle$. This will imply that $\rho_\lambda(G_M)$ is contained in a $\mathcal{C}_2$ -type maximal subgroup, contradicting the assumption that ℓ is not a $\mathcal{C}_2$ -prime. So we deduce that $\rho_\lambda(G_M) \cap \psi(\mathbb{F}'^*) \not\leq \psi(H)$, i.e., there exists $\alpha \in \mathbb{F}'^*$ such that $\alpha^3 \notin \mathbb{F}^*$ and $\psi(\alpha) \in \rho_\lambda(G_M)$.

Case 2: ℓ is inert in M . Then $[\mathbb{F} : \mathbb{F}_\ell] = 2$ and $[\mathbb{F}' : \mathbb{F}_\ell] = 6$. Let $\mathbb{F}'' \subset \mathbb{F}'$ be the degree 3 extension of $\mathbb{F}_\ell$. For any quadratic field extension $l|k$, let l_1 denote the subgroup $\ker(\text{Nm} : l^* \rightarrow k^*)$ of l^* , so that $\text{CL}_1^-(\mathbb{F}'') = \text{CU}_1(\mathbb{F}'') \cong$

$\mathbb{F}'_1$. Fix an inclusion $\psi: \mathbb{F}'_1 \rtimes \text{Gal}(\mathbb{F}'/\mathbb{F}) \hookrightarrow \mathbb{F}'^* \rtimes \text{Gal}(\mathbb{F}'/\mathbb{F}) \hookrightarrow \text{CU}_3(\ell)$ such that $\mathbb{F}'^* \text{im}(\psi)$ is a maximal subgroup of $\text{CU}_3(\ell)$ containing $\rho_\lambda(G_M)$. Let $H = \{x \in \mathbb{F}'_1 \mid x^3 \in \mathbb{F}_1\}$. Lemma 5.23 again implies that the intersection $\rho_\lambda(G_M) \cap \psi(\mathbb{F}'_1)$ is not contained in $\psi(H)$, i.e., there exists $\alpha \in \mathbb{F}'_1$ such that $\alpha^3 \notin \mathbb{F}_1$ and $\psi(\alpha) \in \rho_\lambda(G_M)$.

The characteristic polynomial of $\psi(\alpha)$ is the minimal polynomial over $\mathbb{F}$ of $\alpha \in \mathbb{F}'$, and hence it is irreducible over $\mathbb{F}$ and not of the form $x^3 - a$. Chebotarev density theorem guarantees the existence of primes $\mathfrak{p} \mid p$ such that $\rho_\lambda(\text{Frob}_{\mathfrak{p}})$ is conjugate to $\psi(\alpha)$. Therefore the reduction in $\mathbb{F}[x]$ of the polynomial $f_{p,1}$ fits the conditions being checked in Step 2. So for B large enough, Algorithm 5.22 will return False. $\square$

5.2.4. $\mathcal{C}_3$ field extension subgroups.

Lemma 5.25. *Let $\mathbb{F}$ be a finite field and $\mathbb{F}'/\mathbb{F}$ an extension of prime degree s . Then any element in $\text{GL}_1(\mathbb{F}') \rtimes \text{Gal}(\mathbb{F}'/\mathbb{F})$ of order greater than $s|\mathbb{F}^*|$ is contained in the normal subgroup $\text{GL}_1(\mathbb{F}')$.*

Proof. We may write $\text{GL}_1(\mathbb{F}') \rtimes \text{Gal}(\mathbb{F}'/\mathbb{F}) \cong (\mathbb{F}')^* \rtimes \text{Gal}(\mathbb{F}'/\mathbb{F}) \cong \langle a \rangle \rtimes \langle f \rangle$ where a has order $|\mathbb{F}'| - 1$, f has order s and $f a f^{-1} = a^{|\mathbb{F}'|}$. Let $b \in \text{GL}_1(\mathbb{F}') \rtimes \text{Gal}(\mathbb{F}'/\mathbb{F})$. The relation $f a = a^{|\mathbb{F}'|} f$ allows us to write $b = a^m f^n$ for some m, n .

If $n \equiv 0 \pmod{s}$, then b is a power of a . Thus we may suppose that $n \not\equiv 0 \pmod{s}$ and show that the order of b is at most $s|\mathbb{F}^*|$. It will then follow that any element of order greater than $s|\mathbb{F}^*|$ is contained in $\langle a \rangle$. Considering a as an element of $\mathbb{F}'$, we have

$$b^s = (a^m f^n)^s = \prod_{i=0}^{s-1} f^{in} a^m f^{-in} = \prod_{i=0}^{s-1} f^i a^m f^{-i} = \text{Nm}(a^m) \in \mathbb{F}^*$$

where the penultimate equality follows from the fact that multiplication by n induces an automorphism of $\mathbb{Z}/s\mathbb{Z}$. We deduce that the order of b divides $s|\mathbb{F}^*|$. Hence the result follows as explained above. $\square$

Proposition 5.26. *Let $\ell \geq 5$ be a semistable admissible prime for A and λ a prime of M lying over ℓ . Suppose $\rho_\lambda(G_M)$ is an absolutely irreducible subgroup contained in a $\mathcal{C}_3$ -type subgroup.*

Then there exists an abelian extension L/M of degree 3, unramified outside the primes of bad reduction for A , such that if the image of $\sigma \in G_M$ in $\text{Gal}(L/M)$ is non-trivial then $\text{Tr } \rho_\lambda(\sigma) \equiv 0 \pmod{\lambda}$.

Proof. Suppose ℓ splits in M . The description given in Section 5.1.3 of $\mathcal{C}_3$ -type subgroups of $\text{GL}_3(\ell)$ implies that there exists a injective homomorphism $\psi: \mathbb{F}_{\ell^3}^* \rtimes \text{Gal}(\mathbb{F}_{\ell^3}/\mathbb{F}_\ell) \rightarrow \text{GL}_3(\ell)$ such that $\rho_\lambda(G_M)$ is contained in the image of ψ . Since $\rho_\lambda(G_M)$ is absolutely irreducible by assumption, it cannot be contained in $\psi(\mathbb{F}_{\ell^3}^*)$. Thus $Q := \rho_\lambda(G_M) / (\rho_\lambda(G_M) \cap \psi(\mathbb{F}_{\ell^3}^*))$ is a cyclic quotient of $\rho_\lambda(G_M)$ of order 3. Let L denote the fixed field of $\rho_\lambda(G_M) \cap \psi(\mathbb{F}_{\ell^3}^*)$.

Let a be a generator of $\mathbb{F}_{\ell^3}^*$. Then the eigenvalues of $\psi(a)$ equal a, a^ℓ, a^{ℓ^2} and any generator f of $\psi(\text{Gal}(\mathbb{F}_{\ell^3}/\mathbb{F}_\ell))$ permutes them cyclically. In particular, we find that the trace of such an f must equal zero.

Let I be an inertia group corresponding to a prime above ℓ . As $\ell \neq 3$, the action of I on $A[\lambda]$ factors through its tame quotient and thus acts semisimply. In particular, its action is described by Proposition 4.6.

Suppose for a contradiction that L/M is ramified at ℓ . Then there exists $\sigma \in I$ with non-trivial image in $\text{Gal}(L/M)$. If the order of $\rho_\lambda(\sigma)$ is greater than $3(\ell - 1)$, then $\rho_\lambda(\sigma) \in \psi(\mathbb{F}_{\ell^3}^*)$ by Lemma 5.25. As L is the fixed field of $\rho_\lambda(G_M) \cap \psi(\mathbb{F}_{\ell^3}^*)$, we deduce that the order of $\rho_\lambda(\sigma)$ is less than or equal to $3(\ell - 1)$. Hence Proposition 4.6 combined with $\ell \geq 5$, implies $\rho_\lambda|_I = 2\mathbb{1} + \theta_1$ or $\mathbb{1} + 2\theta_1$. We deduce that the minimal polynomial of $\rho_\lambda(\sigma)$ is of the form $(x - 1)(x - d)$ for some $d \in \mathbb{F}_\ell^*$ of order divisible by 3. Applying Lemma 5.17 with $V = A[\lambda] \otimes \mathbb{F}_{\ell^3}$ and $D(V)$ the decomposition given by the eigenspaces of $\psi(a)$ gives that $\rho_\lambda(\sigma)$ has order 2, a contradiction.

Suppose now ℓ is inert in M . The maximal $\mathcal{C}_3$ -type subgroups of $\text{CU}_3(\ell)$ are isomorphic to $\mathbb{F}_\lambda^*(\text{GU}_1(\ell^3) \rtimes \text{Gal}(\mathbb{F}_{\ell^6}/\mathbb{F}_{\ell^2}))$. More precisely, any such maximal subgroup of $\text{CU}_3(\ell)$ is the image of an injective homomorphism $\psi: \mathbb{F}_\lambda^*(\text{GU}_1(\ell^3) \rtimes \text{Gal}(\mathbb{F}_{\ell^6}/\mathbb{F}_{\ell^2})) \rightarrow \text{CU}_3(\ell)$ such that $\psi(\mathbb{F}_\lambda^*)$ is the scalar matrices in $\text{CU}_3(\ell)$, the image of a generator a of $\text{GU}_1(\ell^3)$ has eigenvalues $a, a^{\ell^2}, a^{\ell^4}$ which are permuted cyclically by the non-trivial elements in $\psi(\text{Gal}(\mathbb{F}_{\ell^6}/\mathbb{F}_{\ell^2}))$. In particular, any non-trivial element in $\psi(\text{Gal}(\mathbb{F}_{\ell^6}/\mathbb{F}_{\ell^2}))$ has trace zero.

Since $\rho_\lambda(G_M)$ is absolutely irreducible by assumption, it cannot be contained in $\psi(\mathbb{F}_\lambda^* \text{GU}_1(\ell^3))$. Thus $Q := \rho_\lambda(G_M)/(\rho_\lambda(G_M) \cap \psi(\mathbb{F}_\lambda^* \text{GU}_1(\ell^3)))$ is a cyclic quotient of $\rho_\lambda(G_M)$ of order 3. Let L denote the fixed field of $\rho_\lambda(G_M) \cap \psi(\mathbb{F}_\lambda^* \text{GU}_1(\ell^3))$.

Let I be an inertia group corresponding to a prime above ℓ . As $\ell \neq 3$, the action of I on $A[\lambda]$ factors through its tame quotient and thus acts semisimply. In particular, its action is described by Proposition 4.6.

Suppose for a contradiction that L/M is ramified at ℓ . Then there exists $\sigma \in I$ with non-trivial image in $\text{Gal}(L/M)$. If the order of $\rho_\lambda(\sigma)$ is greater than $3(\ell^2 - 1)$, then $\rho_\lambda(\sigma) \in \psi(\mathbb{F}_\lambda^* \text{GU}_1(\ell^3))$ by Lemma 5.25. As L is the fixed field of $\rho_\lambda(G_M) \cap \psi(\mathbb{F}_\lambda^* \text{GU}_1(\ell^3))$, we deduce that the order of $\rho_\lambda(\sigma)$ is less than or equal to $3(\ell^2 - 1)$. Hence Proposition 4.6 combined with $\ell \geq 5$, implies $\rho_\lambda|_I = \mathbb{1} + \theta_1 + \theta_2$ or $2\theta_2 + \theta_2^\ell$. In the first case, the minimal polynomial of $\rho_\lambda(\sigma)$ is of the form $(x - 1)(x - d)(x - \gamma)$ for some $d \in \mathbb{F}_\ell^*$ and $\gamma \in \mathbb{F}_\lambda \setminus \mathbb{F}_\ell$. Applying Lemma 5.17 with $V = A[\lambda] \otimes \mathbb{F}_{\ell^3}$ and $D(V)$ the decomposition given by the eigenspaces of $\psi(a)$ gives that $\rho_\lambda(\sigma)$ has order 2, a contradiction. In the second case, i.e., $\rho_\lambda|_I = 2\theta_2 + \theta_2^\ell$, consider $\gamma = \theta_2(\sigma)^{-1} \in \mathbb{F}_\lambda^*$. The minimal polynomial of $\psi(\gamma)\rho_\lambda(\sigma)$ is of the form $(x - 1)(x - d)$ for some $d \in \mathbb{F}_\lambda^*$. Applying Lemma 5.17 again for the decomposition $D(V)$ gives that $\psi(\gamma)\rho_\lambda(\sigma)$ has order 2, i.e., $\rho_\lambda(\sigma)^2 = \psi(\gamma)^2$. This is a contradiction since $\rho_\lambda(\sigma)^2$ has non-trivial image in $\text{Gal}(L/M)$, while $\psi(\gamma)^2$ does not. $\square$

We now adapt Proposition 5.26 to turn it into an algorithm for detecting all possibly $\mathcal{C}_3$ -primes for an abelian threefold A . The exact same idea as in Algorithm 5.20, of working with a basis of homomorphisms from G_M to $\mathbb{F}_3$, is used to optimize the number of primes that need to be considered.

Algorithm 5.27 (Possibly $\mathcal{C}_3$ -primes).

Input: Same as in Algorithm 5.20.

Output: a finite superset of the $\mathcal{C}_3$ -primes, or 0.

- (1) Use the conductor exponent bounds from Remark 5.19 to compute a basis $\{\chi_j : 1 \leq j \leq d\}$ for the $\mathbb{F}_3$ -vector space H of Hecke characters of M unramified outside N , and having order dividing 3. Fix a primitive cube root of unity, and treat these characters as homomorphisms $G_M \rightarrow \mathbb{F}_3$.
- (2) For each prime $p < B, p \nmid N$, follow Step 2 of Algorithm 5.20 to construct $f_{p,i}(x) = x^3 + a_{p,i}x^2 + b_{p,i}x + c_{p,i}$, with $\overline{f_{p,1}} = f_{p,2}$, from the L -polynomial.
- (3) Let S denote the set of primes p such that $a_{p,1} \neq 0$. Let $S = \{p_i : 1 \leq i \leq m\}$. For each prime $p_i \in S$, choose a prime ideal $\mathfrak{p}_i$ above p_i . Construct the $m \times d$ matrix $A \in M_{m,d}(\mathbb{F}_3)$ whose $(i, j)^{th}$ entry is $\chi_j(\mathfrak{p}_i) = \chi_j(\text{Frob}_{\mathfrak{p}_i}) \in \mathbb{F}_3$.
- (4) If $\text{rank}(A) < d$, return 0.
- (5) Return the set of all rational primes dividing

$$6N \cdot \prod_{p \in S} \text{Nm}_{M/\mathbb{Q}}(a_{p,1})$$

Theorem 5.28. *Let $A/\mathbb{Q}$ be a polarised abelian threefold, and M be an imaginary quadratic field such that $M \cong \text{End}^0(A_{\overline{\mathbb{Q}}})$. Suppose Assumption 5.1 holds. Then, for B large enough, Algorithm 5.27 returns a finite superset of the $\mathcal{C}_3$ -primes for A .*

Proof. By Assumption 5.1, choose a rational prime ℓ splitting in M , and λ above ℓ so that $\rho_\lambda(G_M) = \text{GL}_3(\ell)$. Let $M(A[\lambda])$ denote the fixed field of $\ker(\rho_\lambda)$. The maximal abelian sub-extension of $M(A[\lambda])/M$ corresponds to the quotient $\text{GL}_3(\ell) \xrightarrow{\det} \mathbb{F}_\ell^*$. So either there is a unique cyclic cubic sub-extension corresponding to the further quotient $\text{GL}_3(\ell) \twoheadrightarrow \mathbb{F}_\ell^*/\mathbb{F}_\ell^{*3}$ (when $\ell \equiv 1 \pmod{3}$), or there are none (when $\ell \not\equiv 1 \pmod{3}$). Let I denote the inertia group at a prime above ℓ . By Proposition 4.6, we know that $\det \rho_\lambda|_I = \theta_1$ or θ_1^2 . Hence this cyclic cubic sub-extension of $M(A[\lambda])/M$, if it exists, is ramified at both λ and $\bar{\lambda}$.

Let M_3 denote the compositum of the cyclic cubic extensions cut out by the order 3 Hecke characters χ_j from Step 1 of Algorithm 5.27. Since M_3 is unramified outside N , it is disjoint from $M(A[\lambda])$. Therefore, Chebotarev density theorem applied to the Galois extension $M_3 \cdot M(A[\lambda])$ of M with Galois group $(\mathbb{Z}/3\mathbb{Z})^d \times \text{GL}_3(\ell)$, guarantees the existence of primes $\mathfrak{p}_i|p_i$ in M such that $\text{Tr}(\rho_\lambda(\text{Frob}_{\mathfrak{p}_i})) \neq 0 \in \mathbb{F}_\ell$ (so that $a_{p_i,1} \neq 0 \in \mathbb{Z}_\ell$) and $\chi_j(\mathfrak{p}_i) = \delta_{i,j}$. So for B large enough, the matrix A constructed in Step 3 of Algorithm 5.27 will have full rank. This shows that the algorithm returns a finite set of primes, and not 0.

Let $\ell \geq 5$ be a $\mathcal{C}_3$ -prime for A . If A does not have semistable reduction at ℓ , then $\ell \mid N$ and we are done. So we may assume that ℓ is a semistable prime for A . Then $\rho_\lambda(G_M)$ is an absolutely irreducible subgroup contained in a $\mathcal{C}_3$ -type maximal subgroup for a prime ideal $\lambda|\ell$. Let L/M be the cyclic cubic extension given by Proposition 5.26. Since L/M is unramified outside N , there exists a non-trivial character $\chi \in H$ which cuts out L . Since the matrix A has full rank, we deduce that there exists a prime $p \in S$ and $\mathfrak{p}|p$ such that $\chi(\mathfrak{p}) \neq 0$. This means that $\text{Frob}_{\mathfrak{p}}$ is non-trivial in $\text{Gal}(L/M)$.

Hence Proposition 5.26 implies that $\text{Tr } \rho_\lambda(\text{Frob}_{\mathfrak{p}}) \equiv 0 \pmod{\lambda}$, i.e., $a_{p,i} \equiv 0 \pmod{\lambda}$ for $i = 1$ or 2 , which implies that $\text{Nm}_{M/\mathbb{Q}}(a_{p,1}) = a_{p,1}\overline{a_{p,1}} = a_{p,2}\overline{a_{p,2}} \equiv 0 \pmod{\ell}$. $\square$

While Algorithm 5.27 turns the problem of determining $\mathcal{C}_3$ -primes into a finite problem, the output can include false positives, and furthermore it does not say anything about primes of non-semistable reduction for A . Algorithm 5.29 is a simple test to decide for any given prime ℓ , whether it can possibly be a $\mathcal{C}_3$ -prime by inspecting the reductions modulo ℓ of Frobenius polynomials.

Algorithm 5.29 (Weeding out extraneous primes from possibly $\mathcal{C}_3$ -primes).

Input: Same as in Algorithm 5.22.

Output: true or false depending on whether ℓ is possibly a $\mathcal{C}_3$ -prime or not.

- (1) For each prime p , using the given L -polynomial, follow Step 2 of Algorithm 5.20 to construct $f_{p,i}(x) = x^3 + a_{p,i}x^2 + b_{p,i}x + c_{p,i}$, with $f_{p,1} = f_{p,2}$.
- (2) Choose a prime λ above ℓ in M , and consider the reduction of $f_{p,1}(x)$ modulo λ . If this polynomial is reducible in $\mathbb{F}_\lambda[x]$, but not of the form $x^3 - a$ or $(x - a)^3$, then return False.
- (3) If no return statement has been executed while running Steps 1 to 2, then return True.

Proposition 5.30. *Let $A/\mathbb{Q}$ be a polarised abelian threefold, and M be an imaginary quadratic field such that $M \cong \text{End}^0(A_{\overline{\mathbb{Q}}})$. Suppose $\ell > 7$ is a rational prime that is not a $\mathcal{C}_1$ -prime. Then ℓ is not a $\mathcal{C}_3$ -prime for A if Algorithm 5.29 returns false.*

Proof. Let $\lambda|\ell$ be a prime of $\mathcal{O}_M$, and $\mathbb{F} = \mathbb{F}_\lambda$. The characteristic polynomial of an element of the $\mathcal{C}_3$ -type maximal subgroup has one of the following shapes: an irreducible cubic, $(x - a)^3$, or $x^3 - a$ for some $a \in \mathbb{F}^*$. So, if the reduction of $f_{p,1}$ modulo λ is not of these shapes, we can deduce that $\rho_\lambda(\text{Frob}_{\mathfrak{p}})$ does not belong to the $\mathcal{C}_3$ -type maximal subgroup for some prime $\mathfrak{p}|p$. Hence ℓ is not a $\mathcal{C}_3$ -prime for A . $\square$

Remark 5.31. It is worth noting that unlike Algorithm 5.22 which can eliminate any extraneous $\mathcal{C}_2$ -prime given sufficiently many L -polynomials as input (Proposition 5.24), Algorithm 5.29 is not guaranteed to eliminate extraneous $\mathcal{C}_3$ -primes.

5.2.5. $\mathcal{C}_6$ symplectic type subgroups. The description of inertia at primes above ℓ given in Proposition 4.6 shows us that for $\ell > 7$ the projective image of $\rho_\lambda(G_M)$ contains a cyclic element with order greater than 6. As $C_3^2 \rtimes \text{SL}_2(3)$ does not contain such an element, we deduce that $\rho_\lambda(G_M)$ cannot be contained in a $\mathcal{C}_6$ -type maximal subgroup of $\text{CL}_3^\varepsilon(\ell)$ unless $\ell = 5$ and ℓ is inert in M or $\ell = 7$ and ℓ splits in M .

Characteristic polynomials of elements of the $\mathcal{C}_6$ -type maximal subgroup are either reducible or of the form $x^3 - a$ for some $a \in \mathbb{F}$. So exhibiting an irreducible Frobenius characteristic polynomial not of the form $x^3 - a$ is sufficient to rule out $\ell \in \{5, 7\}$ as $\mathcal{C}_6$ -primes. If $\ell \in \{5, 7\}$ is a $\mathcal{C}_1$ -prime, this simple strategy does not work.

5.2.6. $\mathcal{C}_8/\mathcal{C}_5$ -type orthogonal subgroups. Let $\ell > 2$ be an admissible prime for A , λ be a prime of M above ℓ , and $\varepsilon = (\frac{\Delta_M}{\ell})$, and assume $\ell \not\equiv \varepsilon \pmod{3}$. Let $\mathrm{SO}_3(\ell)$ denote the subgroup of $\mathrm{CL}_3^\varepsilon(\ell)$ consisting of the determinant 1 isometries of a non-degenerate symmetric bilinear pairing on the underlying vector space. Then the similitude group of the pairing is $\mathbb{F}_\lambda^* \mathrm{SO}_3(\ell)$, and it is a maximal subgroup of $\mathrm{CL}_3^\varepsilon(\ell)$. We first discuss the shape of characteristic polynomials of elements of this maximal subgroup.

Lemma 5.32. *Let σ be any element in the maximal subgroup $\mathbb{F}_\lambda^* \mathrm{SO}_3(\ell)$ of $\mathrm{CL}_3^\varepsilon(\ell)$, and ϕ be the characteristic polynomial of σ . Then there exists μ in $\mathbb{F}_\ell^*$ if $\varepsilon = +1$ (or in $\mathbb{F}_{\ell^2}^*$ if $\varepsilon = -1$) such that $\phi(x) = \frac{-x^3}{\mu^3} \phi\left(\frac{\mu^2}{x}\right)$, i.e., $\phi(x) = x^3 + ax^2 - a\mu x - \mu^3 = (x - \mu)(x^2 + (a + \mu)x + \mu^2)$ for some a .*

Proof. Let μ denote the scalar, considered as a scalar matrix, such that $\sigma = \mu\tau$ for some $\tau \in \mathrm{SO}_3(\ell)$. Let X be the matrix of the symmetric bilinear pairing. Then ${}^t\tau X \tau = X$, and therefore ${}^t\tau$ and τ^{-1} are conjugate. Therefore the set of eigenvalues of τ is stable under inversion. Since $\det(\tau) = 1$, we deduce that the set of eigenvalues of τ is equal to $\{1, \nu, \nu^{-1}\}$ for some $\nu \in \mathbb{F}_\ell$. Therefore the eigenvalues of σ are $\{\mu, \mu\nu, \mu\nu^{-1}\}$, from which the shape of its characteristic polynomial is evident. $\square$

Algorithm 5.33 (Possibly $\mathcal{C}_8/\mathcal{C}_5$ -primes).

Input: Same as in Algorithm 5.20.

Output: a finite superset of the $\mathcal{C}_8/\mathcal{C}_5$ -primes, or 0.

- (1) For each prime $p < B, p \nmid N$, follow Step 2 of Algorithm 5.20 to construct $f_{p,i}(x) = x^3 + a_{p,i}x^2 + b_{p,i}x + c_{p,i}$, with $\overline{f_{p,1}} = f_{p,2}$, from the L -polynomial.
- (2) Let S denote the set of primes p such that $v_p := b_{p,1}^3 - c_{p,1}a_{p,1}^3 \neq 0$.
- (3) If S is empty, return 0.
- (4) Return the set of all rational primes dividing $\gcd \mathrm{Nm}_{M/\mathbb{Q}}(v_p)_{p \in S}$.

Proposition 5.34. *Let $A/\mathbb{Q}$ be a polarised abelian threefold, and M be an imaginary quadratic field such that $M \cong \mathrm{End}^0(A_{\overline{\mathbb{Q}}})$. Then, for B large enough, Algorithm 5.33 returns a finite superset of the $\mathcal{C}_8/\mathcal{C}_5$ -primes for A .*

Proof. We first show that Algorithm 5.33 does not return 0, if B is large enough, i.e., if sufficiently many L -polynomials are given as input. It is enough to show that there exists some prime p such that the quantity v_p in Step 2 is not zero. By Assumption 5.1, choose a rational prime ℓ splitting in M , and λ above ℓ so that $\rho_\lambda(G_M) = \mathrm{GL}_3(\ell)$. By Chebotarev density theorem there exists a prime $\mathfrak{p}|p$ in M such that the characteristic polynomial of $\rho_\lambda(\mathrm{Frob}_{\mathfrak{p}})$ is irreducible over $\mathbb{F}_\ell$. Therefore $f_{p,1}$ is irreducible over $\mathbb{Z}_\ell$, and hence $v_p = b_{p,1}^3 - c_{p,1}a_{p,1}^3 \neq 0$, so we are done.

Let ℓ be an admissible prime for A , and λ be a prime of M above ℓ . Suppose that $\rho_\lambda(G_M)$ is contained the $\mathcal{C}_8/\mathcal{C}_5$ -type orthogonal maximal subgroup of $\mathrm{CL}_3^\varepsilon(\ell)$. Recall that the reduction of $f_{p,1}(x)$ modulo λ is the characteristic polynomial of $\rho_\lambda(\mathrm{Frob}_{\mathfrak{p}})$ for some prime $\mathfrak{p}$ of M above p . So it should have the shape given in Lemma 5.32. This implies that either $a_{p,1} \equiv b_{p,1} \equiv 0 \pmod{\lambda}$, or $(b_{p,1}/a_{p,1})^3 \equiv c_{p,1} \pmod{\lambda}$. Both cases imply that $v_p := b_{p,1}^3 - c_{p,1}a_{p,1}^3 \equiv 0 \pmod{\lambda}$, which means that ℓ divides $\mathrm{Nm}_{M/\mathbb{Q}}v_p$. Therefore, ℓ is in the set of primes outputted by Algorithm 5.33. $\square$

5.2.7. $\mathcal{S}$ -type subgroups. In Section 5.1.6, we mentioned necessary congruence conditions for the existence of an $\mathcal{S}$ -type maximal subgroup of $\mathrm{CL}_3^\varepsilon(\ell)$ with projective image $\mathrm{PSL}_2(7)$. They force $\ell = 3$ and $\varepsilon = -1$, or $\ell \geq 11$. The description of inertia at primes above ℓ given in Proposition 4.6 shows us that for $\ell \geq 11$ the projective image of $\rho_\lambda(G_M)$ contains a cyclic element of order at least 10. As $\mathrm{PSL}_2(7)$ does not contain such an element, we deduce that $\rho_\lambda(G_M)$ cannot be contained in such an $\mathcal{S}$ -type maximal subgroup of $\mathrm{CL}_3^\varepsilon(\ell)$ unless $\ell = 3$ and ℓ is inert in M .

If 3 is inert in M , to rule out containment of $\rho_3(G_M)$ in the $\mathcal{S}$ -type maximal subgroup, one needs to exhibit a Frobenius characteristic polynomial that does not come from an element of this maximal subgroup.

5.2.8. Semistability criterion. In this section, as before, A denotes an abelian threefold defined over M such that there exists a unital algebra embedding $\iota: M \hookrightarrow \mathrm{End}^0(A_{\overline{M}})$. For a prime $\mathfrak{p}$ of M , let $M_{\mathfrak{p}}$ denote the completion of M at $\mathfrak{p}$ and $\mathcal{O}_{\mathfrak{p}}$ its ring of integers. Let $A_{\mathfrak{p}}$ denote the special fibre of the Néron model of A over $\mathcal{O}_{\mathfrak{p}}$. Let $A_{\mathfrak{p}}^0$ denote the connected component of the identity of $A_{\mathfrak{p}}$. Recall that there exists a short exact sequence

$$0 \rightarrow A_{\mathfrak{p}}^0 \rightarrow A_{\mathfrak{p}} \rightarrow \Phi_{A,\mathfrak{p}} \rightarrow 0$$

where $\Phi_{A,\mathfrak{p}}$ is a finite étale group scheme over $k_{\mathfrak{p}} := \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. Recall that A is said to have semistable reduction at $\mathfrak{p}$ if there exists an exact sequence

$$0 \rightarrow T_{\mathfrak{p}} \rightarrow A_{\mathfrak{p}}^0 \rightarrow B_{\mathfrak{p}} \rightarrow 0$$

where $T_{\mathfrak{p}}$ a torus and $B_{\mathfrak{p}}$ is an abelian variety. The dimension of $T_{\mathfrak{p}}$ is known as the toric rank of $A_{\mathfrak{p}}$. We say that A has bad semistable reduction at $\mathfrak{p}$ if it has semistable reduction and the toric rank of $A_{\mathfrak{p}}$ is positive.

Theorem 5.35. *Suppose A has bad semistable reduction at a prime $\mathfrak{p}$ of M . Let $\ell \notin \mathfrak{p}$ be an odd rational admissible prime not dividing the order of $\Phi_{A,\mathfrak{p}}$ and λ a prime of M lying above ℓ .*

Then either G_M acts reducibly on $A[\lambda]$ or $\rho_\lambda(G_M) \cong \mathrm{CL}_3^\varepsilon(\ell)$.

Proof. By [GR72, Prop. 3.5], for any $\sigma \in I_{\mathfrak{p}}$, we have that $(\sigma - 1)^2$ annihilates $T_\ell(A)$. By [ST68, Lemma 2], we have that $A[\ell]^{I_{\mathfrak{p}}} = A_{\mathfrak{p}}[\ell]$. As the order of $\Phi_{A,\mathfrak{p}}$ is coprime to ℓ , we have $\dim_{\mathbb{F}_\ell} A_{\mathfrak{p}}[\ell] = 6 - t < 6$ where t is the toric rank of $A_{\mathfrak{p}}$ by [ST68, Lemma 1]. Thus $I_{\mathfrak{p}}$ acts non-trivially on $A[\ell]$ and hence also non-trivially on $A[\lambda]$. In particular, there exists $\sigma \in I_{\mathfrak{p}}$ such that $\rho_\lambda(\sigma) \neq 1$ and $(\rho_\lambda(\sigma) - 1)^2 = 0$. Note this means the minimal characteristic polynomial of $\rho_\lambda(\sigma)$ is $(x - 1)^2$.

Suppose $\rho_\lambda(G_M)$ is contained in a $\mathcal{C}_2$ or $\mathcal{C}_3$ -type subgroup. Then $\rho_\lambda(G_M)$ preserves a decomposition $A[\lambda] \otimes_{\mathbb{F}_\lambda} \overline{\mathbb{F}_\lambda} = \bigoplus_{i=1}^3 V_3$. Applying [Goo25, Lemma 5.8], we see this is only possible if $\ell = 2$. Note that for $\ell \geq 5$, order considerations directly make this impossible.

For $\ell = 3$, there are no maximal $\mathcal{C}_6$ -type subgroups in $\mathrm{CL}_3^\varepsilon(\ell)$. Thus let us suppose $\ell \geq 5$. The relation $(\rho_\lambda(\sigma) - 1)^2 = 0$ implies $0 = (\rho_\lambda(\sigma) - 1)^\ell = \rho_\lambda(\sigma)^\ell - 1$, coupling this with $\rho_\lambda(\sigma) \neq 1$, we deduce $\rho_\lambda(\sigma)$ has order ℓ . Since the $\mathcal{C}_6$ -type subgroups do not contain any elements of order ℓ for $\ell \geq 5$, we deduce that $\rho_\lambda(G_M)$ is not contained in a $\mathcal{C}_6$ -type subgroup.

Since the minimal polynomial of $\rho_\lambda(\sigma)$ is $(x-1)^2$ and $A[\lambda]$ has dimension 3 over $\mathbb{F}_\lambda$, we deduce from its Jordan Normal Form that $\ker(\rho_\lambda(\sigma) - 1)$ is of dimension 2. Thus [Gro02, Cor. 6.10] implies $\rho_\lambda(\sigma)$ does not preserve a non-degenerate symmetric pairing.

If $\rho_\lambda(G_M)$ is contained in a $\mathcal{S}$ -type subgroup, then $\rho_\lambda(G_M)$ is contained in a maximal subgroup isomorphic to $\mathbb{F}_\lambda^* \times \mathrm{PSL}_2(7)$. By Section 5.1.6, this can only happen if $\ell = 3$ or $\ell \geq 11$. Since $\rho_\lambda(\sigma)$ has order ℓ and the order of $\mathbb{F}_\lambda^* \times \mathrm{PSL}_2(7)$ is coprime to ℓ for $\ell \geq 11$, we deduce $\ell = 3$ is the only possibility. Examining the representations of $\mathrm{PSL}_2(7)$ over a field of characteristic 3, we find this maximal subgroup does not contain an element with minimal polynomial equal to $(x-1)^2$. Thus $\rho_\lambda(G_M)$ is not contained in a $\mathcal{S}$ -type subgroup.

It follows from the classification in Section 5.1 of maximal subgroups of $\mathrm{CL}_3^\varepsilon(\ell)$ not containing $\mathrm{SL}_3^\varepsilon(\ell)$, that either G_M acts reducibly on $A[\lambda]$ or $\rho_\lambda(G_M) \cong \mathrm{CL}_3^\varepsilon(\ell)$. $\square$

6. RESULTS

In this section we present the results of running the algorithms developed in Section 5 on various families of curves, and a dataset of Picard curves with good reduction outside $\{2, 3, 5, 7\}$.

For hyperelliptic curves, L -polynomials are computed efficiently using the algorithms devised and implemented in [HS14; HS16; KS08]. For Picard curves, L -polynomials are computable in average polynomial time, by combining the work [Sut20] of Sutherland on computing $L_p(C, x) \pmod{p}$ for superelliptic curves, and the work [AFP22] of Asif, Fite and Pentland to lift this to the true integral L -polynomial $L_p(C, x)$ when C is a Picard curve. We use these implementations to obtain L -polynomials efficiently for our computations. For hyperelliptic and Picard curves, we work with L -polynomials at all good primes $p < 2^{12}$. For other smooth plane quartic curves, we work with L -polynomials at all good primes $p < 2^{10}$.

Recall that B_d denotes the quaternion algebra over $\mathbb{Q}$ of discriminant d .

6.1. Hyperelliptic Curves. Consider the family of smooth genus 3 hyperelliptic curves

$$(6.1) \quad y^2 = f(x) = x^7 + ax^5 + bx^3 + cx.$$

The map $(x, y) \mapsto (-x, iy)$ is an automorphism defined over $\mathbb{Q}(i)$. Hence the geometric endomorphism algebra of the Jacobian of a curve in this family contains $\mathbb{Q}(i)$, with equality for a generic curve. We considered the finite set of separable polynomials $f(x) \in \mathbb{Z}[x]$ in the box $\mathcal{B}$ defined by $|a|, |b|, |c| \leq 100$. Note that multiple polynomials may define the same curve upto twist, or even upto isomorphism, and in these cases the results will be identical. But we have not reduced the dataset up to isomorphism/twists.

Among the 8079794 polynomials in this box, Algorithm 5.15 fails for 1052. These define curves that have a bigger geometric endomorphism algebra of Jacobian than $\mathbb{Q}(i)$. Most of these curves are twists of the curve $y^2 = x^7 + x$, or a curve in the family $y^2 = x^7 + ax^5 + ax^3 + x$. Heuristic computations indicate that the generic geometric endomorphism ring in this

family is an order of index 2^5 in $\mathbb{Q}(i) \times M_2(\mathbb{Q})$. Table 1 displays several other non-CM endomorphism algebras, that were observed for a very few curves.

$\text{End}^0(A_{\overline{\mathbb{Q}}})$	Index	$\text{End}^0(A_{\overline{\mathbb{Q}}})$	Index
$\mathbb{Q}(i) \times M_2(\mathbb{Q})$	5^3	$\mathbb{Q}(i) \times M_2(\mathbb{Q})$	$2^2 \cdot 5^3$
$\mathbb{Q}(i) \times M_2(\mathbb{Q}(\sqrt{-2}))$	2^4	$\mathbb{Q}(i) \times M_2(\mathbb{Q}(\sqrt{-3}))$	2^{11}
$\mathbb{Q}(i) \times M_2(\mathbb{Q}(\sqrt{-5}))$	5^4	$\mathbb{Q}(i) \times B_6$	$2 \cdot 3^2$
$M_3(\mathbb{Q}(i))$	3^8		

TABLE 1. Some geometric endomorphism algebras $\text{End}^0(A_{\overline{\mathbb{Q}}})$, along with the index of $\text{End}(A_{\overline{\mathbb{Q}}})$ in a maximal order, that are observed numerically for Jacobians A of a few hyperelliptic curves as in Eq. (6.1).

For the curves defined by the remaining 8 078 742 polynomials, Algorithms 5.15, 5.20, 5.27 and 5.33 succeed. After weeding out extraneous $\mathcal{C}_2$ and $\mathcal{C}_3$ -primes using Algorithms 5.22 and 5.29, the set of primes returned is contained in $\{3\}$. There are no $\mathcal{C}_6$ -type maximal subgroups to worry about since $M = \mathbb{Q}(i)$. We did not rule out containment of $\rho_3(G_M)$ in the $\mathcal{S}$ -type maximal subgroup of $\text{CU}_3(3)$. Thus we find that, for all these curves, the set of non-surjective semistable admissible primes is contained in $\{3\}$. Table 2 gives refined information about the individual outputs of these algorithms, i.e., the admissible primes ℓ at which the mod- λ Galois image for $\lambda|\ell$ is possibly contained in one of the maximal subgroups from Section 5.1.

Superset of	Output	Number of polynomials
Semistable $\mathcal{C}_1$ -primes	$\{\}$	8 078 648
	$\{3\}$	94
$\mathcal{C}_3$ -primes	$\{\}$	8 078 742
$\mathcal{C}_2$ -primes	$\{\}$	8 078 700
	$\{3\}$	42
$\mathcal{C}_8/\mathcal{C}_5$ -primes	$\{\}$	8 078 742

TABLE 2. Output of Algorithms 5.15, 5.20, 5.27 and 5.33, after removing extraneous primes, for polynomials in the box $\mathcal{B}$ defining smooth curves with endomorphism ring $\mathbb{Z}[i]$.

For $d = 2, 3, 4$, there are several 1-dimensional families of hyperelliptic curves C_a over $\mathbb{Q}$ with generic geometric endomorphism ring equal to $\mathbb{Z}[\sqrt{-d}]$. In forthcoming work, we study these families in detail and in particular certify the extra endomorphisms. We consider the 1 216 767 rational numbers of height up to 1000 for values of a . For all but two of these curves, the set of admissible primes returned by Algorithms 5.15, 5.20, 5.27 and 5.33 is empty. The two exceptions give 3 as a possibly reducible prime. Table 3 shows these families and summarises the data.

For the curves in the $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\sqrt{-3}]$ families, we thus find that the mod- λ image is $\text{CL}_3^\varepsilon(\ell)$, for all $\lambda|\ell$ for all semistable admissible primes ℓ . For the curves in the $\mathbb{Z}[\sqrt{-4}]$ families, we did not rule out containment of

$\rho_3(G_M)$ in the $\mathcal{S}$ -type maximal subgroup of $\mathrm{CU}_3(3)$, so the mod- λ image is $\mathrm{CL}_3^\varepsilon(\ell)$, for all $\lambda|\ell$ for all semistable admissible primes $\ell \neq 3$.

Hyperelliptic family	Generic $\mathrm{End}(\mathrm{Jac}(C_a)_{\overline{\mathbb{Q}}})$	Semistable $\mathcal{C}_1$ -primes	Number of curves
$y^2 = (x+2)(x^2-2)$ $(x^4 - 4x^2 + a)$	$\mathbb{Z}[\sqrt{-2}]$	$\{\}$	1 216 763
$y^2 = x((x^2-3)^3 + a(x+2)(x+1)^4)$	$\mathbb{Z}[\sqrt{-4}]$	$\{\}$	1 216 764
$y^2 = (x^4 + ax^2 - \frac{a}{2})$ $(x^4 + 2ax^2 - 2ax + \frac{a}{2})$	$\mathbb{Z}[\sqrt{-4}]$	$\{\}$ $\{3\}$	1 216 762 2
$y^2 = x(x^2 - x - 1/12)$ $((x^2 - x - 1/12)^2 + ax^3)$	$\mathbb{Z}[\sqrt{-3}]$	$\{\}$	1 216 764
$y^2 = (x^2 - x + 1)(x^2 + x + 1)$ $(x(x^3 + 2) + a(2x^3 + 1))$	$\mathbb{Z}[\sqrt{-3}]$	$\{\}$	1 216 765

TABLE 3. Output of Algorithm 5.15 for smooth genus 3 curves in 1-parameter hyperelliptic families C_a , with $a \in \mathbb{Q}$, $\mathrm{ht}(a) \leq 1000$ and given endomorphism ring.

In the theorem below, for $f \in \mathbb{Q}[x]$ separable, we let J_f denote the Jacobian of the smooth projective hyperelliptic curve defined by the affine model $y^2 = f(x)$. We also write $\rho_\ell: G_{\mathbb{Q}} \rightarrow \mathrm{Aut}(J_f[\ell])$ for the associated mod- ℓ representation.

Theorem 6.2. *Let ℓ be a prime, not congruent to 1, 25, 121 modulo 168, then $\Gamma\mathrm{U}_3(\ell)$ is a Galois group over $\mathbb{Q}$. Furthermore,*

- for $\ell \equiv 2 \pmod{3}$, $\ell \neq 2$ and $f(x) = (x^2 - x + 1)(x^2 + x + 1)(x(x^3 + 2) + 3(2x^3 + 1))$, we have $\rho_\ell(G_{\mathbb{Q}}) \cong \Gamma\mathrm{U}_3(\ell)$;
- for $\ell \equiv 3 \pmod{4}$ and $f(x) = x((x^2 - 3)^3 + 5(x + 2)(x + 1)^4)$, we have $\rho_\ell(G_{\mathbb{Q}}) \cong \Gamma\mathrm{U}_3(\ell)$;
- for $\ell \equiv 5, 7 \pmod{8}$ and $f(x) = (x + 2)(x^2 - 2)(x^4 - 4x^2 + 3)$, we have $\rho_\ell(G_{\mathbb{Q}}) \cong \Gamma\mathrm{U}_3(\ell)$.
- for $\ell \equiv 3, 5, 6 \pmod{7}$, and the smooth plane quartic curve $C: 2x^3z + x^2y^2 + x^2yz - xy^2z + 2xyz^2 + xz^3 - y^4 - 2y^3z - 2yz^3 + z^4 = 0$, we have $\rho_\ell(G_{\mathbb{Q}}) \cong \Gamma\mathrm{U}_3(\ell)$.

Proof. The group $\Gamma\mathrm{U}_3(2)$ is soluble and thus a Galois group over $\mathbb{Q}$ by Shafarevich's Theorem for soluble groups [Sha54]. Hence we may assume $\ell > 2$. Thus to prove $\Gamma\mathrm{U}_3(\ell)$ is a Galois group over $\mathbb{Q}$ for ℓ not congruent to 1, 25, 121 modulo 168, it suffices to prove the 'furthermore' claim of the statement.

The last claim is immediate from the computation described in Section 6.3, using the fact that C has good reduction outside $\{2, 7\}$. To prove the given statement for any congruence class of primes, it suffices by Table 3 and the computational results mentioned prior to Table 3 to check that J_f has good reduction at all primes in the given congruence class. To do so, it is enough verify that the given primes ℓ do not divide the discriminant of f . The discriminant of the polynomial $(x^2 - x + 1)(x^2 + x + 1)(x(x^3 + 2) + 3(2x^3 + 1))$

is $-2^{12} \cdot 3^9 \cdot 7^6$, thus for $\ell \equiv 2 \pmod{3}$, $\ell \neq 2$ we have $\rho_\ell(G_{\mathbb{Q}}) \cong \Gamma U_3(\ell)$. The discriminant of the polynomial $x((x^2 - 3)^3 + 5(x + 2)(x + 1)^4)$ is $2^{14} \cdot 5^4 \cdot 17^5$, thus for $\ell \equiv 3 \pmod{4}$ and $\ell > 3$ we have $\rho_\ell(G_{\mathbb{Q}}) \cong \Gamma U_3(\ell)$. For $\ell = 3$, we also compute enough Frobenius characteristic polynomials to rule out containment of $\rho_3(G_{\mathbb{Q}(i)})$ in the $\mathcal{S}$ -type maximal subgroup, thus showing that $\rho_3(G_{\mathbb{Q}(i)}) \cong \text{CU}_3(3)$ and hence $\rho_3(G_{\mathbb{Q}}) \cong \Gamma U_3(3)$. The discriminant of the polynomial $(x + 2)(x^2 - 2)(x^4 - 4x^2 + 3)$ is $2^{13} \cdot 3^3$, thus for $\ell \equiv 5, 7 \pmod{8}$ we have $\rho_\ell(G_{\mathbb{Q}}) \cong \Gamma U_3(\ell)$. $\square$

6.2. Picard curves. We considered the finite set of separable quartic polynomials $f(x) = x^4 + ax^2 + bx + c \in \mathbb{Z}[x]$ lying in the box $\mathcal{B}$ given by $|a|, |b|, |c| \leq 100$ and $b > 0$. Among the 4039833 polynomials in $\mathcal{B}$, Algorithm 5.15 fails for exactly 27, indicating that the Jacobians of the corresponding Picard curves $y^3 = f(x)$ have extra geometric endomorphisms besides $\mathbb{Z}[\zeta_3]$. Heuristic computations confirm that these Jacobians are not simple. All but two of these 27 curves fall into the first family in Table 5 up to twist. The remaining 2 curves fall into the second and fourth families in Table 5 up to twist.

For the remaining 4039806 curves, Algorithms 5.15, 5.20 and 5.27 succeed. Recall that since $M = \mathbb{Q}(\zeta_3)$, there are no $\mathcal{C}_8/\mathcal{C}_5$ -type or $\mathcal{S}$ -type maximal subgroups to worry about. After weeding out using Algorithms 5.22 and 5.29, we find that the set of non-surjective semistable admissible primes is contained in $\{2, 7\}$. Table 4 gives refined information.

Superset of	Output	Number of curves
Semistable $\mathcal{C}_1$ -primes	$\{2\}$	4 039 804
	$\{2, 7\}$	2
$\mathcal{C}_3$ -primes	$\{\}$	4 039 806
$\mathcal{C}_2$ -primes	$\{\}$	2 019 805
	$\{2\}$	2 019 999
	$\{7\}$	2
$\mathcal{C}_6$ -primes	$\{7\}$	2

TABLE 4. Output of Algorithms 5.15, 5.20 and 5.27, after removing extraneous primes, for Picard curves in the box $\mathcal{B}$.

Now we report the results obtained from applying our algorithms on Sutherland's dataset of 3024913 Picard curves of 7-smooth conductor. We note that the dataset includes curves that are twists. Our algorithms succeed for 2413173 curves. The failures consist of bielliptic Picard curves $y^3 = x^4 + ax^2 + c$, curves given by $y^3 = x^4 + bx$, and 13972 other curves for which heuristic computations indicate the presence of extra geometric endomorphisms besides $\mathbb{Z}[\zeta_3]$.

The 13972 failures correspond to 495 curves up to twist. For these curves, we used [Cos+19] to heuristically compute the geometric endomorphism algebra $\text{End}^0(\text{Jac}(C)_{\overline{\mathbb{Q}}})$ and the index of $\text{End}(\text{Jac}(C)_{\overline{\mathbb{Q}}})$ in the maximal order. After sorting them according to this information, we discovered through interpolation of the invariants $a^3/b^2, ac/b^2$, interesting sub-families of Picard curves with generic geometric endomorphism ring strictly bigger than $\mathbb{Z}[\zeta_3]$

(see Table 5). While we had enough data points to obtain the first three families by simple interpolation, for the last one, we needed to look for a short vector in an integer lattice. Table 6 displays several other non-CM endomorphism algebras, that were observed for a very few curves.

For the families in Table 5, we have heuristically verified the endomorphism algebra for all curves corresponding to rational numbers a up to height 20. Therefore, we believe that these represent special subvarieties of the Picard modular surface: the first two are certain rational modular curves $X_0(n)$ for some n dividing 81 and 192 respectively, while the last two are quaternionic rational Shimura curves.

Let C be a smooth Picard curve from one of the last two families in Table 5, corresponding to some generic value of $a \in \mathbb{Q}$. Let $A := \text{Jac}(C)$, and fix an Abel-Jacobi map $C \hookrightarrow A$. Then A contains an elliptic curve E with j -invariant 0, such that the induced map $C \hookrightarrow A \rightarrow E$ does not factor through an isogeny of elliptic curves. Let P denote the Prym variety corresponding to this map, so that P is an abelian surface carrying a natural polarisation; the one obtained by restriction of the principal polarisation on A . The endomorphisms package of [Cos+19] allows us to compute the period matrix of P , using idempotents in the endomorphism algebra. Using this, we verify that $\text{End}(P_{\overline{\mathbb{Q}}})$ is isomorphic to the maximal order in B_{15} or an order of index 3 in the maximal order in B_6 respectively. The latter order precludes principal polarisation. While the former does not, we numerically verify that the natural polarisation on P is not principal.

1-parameter Picard curve family	Generic $\text{End}^0(A_{\overline{\mathbb{Q}}})$ heuristically	Index in maximal order of $\text{End}(A_{\overline{\mathbb{Q}}})$
$y^3 = x(x^3 + 12x^2 + ax + 64)$	$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q})$	$81 = 3^4$
$y^3 = ((x+1)^2 - a(5a+1))((x-1)^2 + 27a(a+1))$	$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q})$	$192 = 2^6 \cdot 3$
$y^3 = (x^2 - 27a(a-1)(3a^2 - 3a + 32))^2 + 2916a^2(a-1)(x - (a-1)(7a-16))^2$	$\mathbb{Q}(\zeta_3) \times B_{15}$	$125 = 5^3$
$y^3 = (x-3a)((x+a)^3 - a(17a^3 + 6a^2 + 24a+8)(x+a) + a^2(27a^4 + 14a^3 + 60a^2 + 24a + 32))$	$\mathbb{Q}(\zeta_3) \times B_6$	$108 = 2^2 \cdot 3^3$

TABLE 5. Picard curve families with generic geometric endomorphism algebra of Jacobian A strictly bigger than $\mathbb{Q}(\zeta_3)$.

Among the 2 413 173 curves, for which our algorithms succeed, the largest possibly non-surjective semistable admissible prime found is 13. It is obtained as a reducible prime for 5 curves, all of which are twists of the curve:

$$(6.3) \quad y^3 = 243x^4 + 338x^3 - 147x^2 - 387x - 142$$

We also obtain a considerable number of curves having 5 and 7 as possibly a reducible prime. Table 7 gives more detailed information.

$\text{End}^0(A_{\overline{\mathbb{Q}}})$	Index	$\text{End}^0(A_{\overline{\mathbb{Q}}})$	Index
$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q})$	$3 \cdot 7^3$	$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q})$	3^7
$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q}(\sqrt{-2}))$	3^7	$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q}(\sqrt{-6}))$	3^4
$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q}(\sqrt{-15}))$	3^4	$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q}(\sqrt{-15}))$	5^4
$\mathbb{Q}(\zeta_3) \times M_2(\mathbb{Q}(\sqrt{-30}))$	5^4	$M_3(\mathbb{Q}(\zeta_3))$	3^{13}
$M_3(\mathbb{Q}(\zeta_3))$	$2^{16} \cdot 3^5$	$M_3(\mathbb{Q}(\zeta_3))$	2^{24}
$\mathbb{Q}(\zeta_3) \times B_{10}$	$2^2 \cdot 3 \cdot 5^2$	$\mathbb{Q}(\zeta_3) \times B_6$	2^8

TABLE 6. Some geometric endomorphism algebras $\text{End}^0(A_{\overline{\mathbb{Q}}})$, along with the index of $\text{End}(A_{\overline{\mathbb{Q}}})$ in a maximal order, that are observed numerically for Jacobians A of a few Picard curves.

Superset of	Output	Number of curves
Semistable $\mathcal{C}_1$ -primes	$\{2\}$	2 412 508
	$\{2, 5\}$	279
	$\{2, 7\}$	381
	$\{2, 13\}$	5
$\mathcal{C}_3$ -primes	$\{\}$	2 413 173
$\mathcal{C}_2$ -primes	$\{\}$	2 406 496
	$\{2\}$	6 559
	$\{7\}$	106
	$\{13\}$	5
	$\{2, 7\}$	7
$\mathcal{C}_6$ -primes	$\{5\}$	279
	$\{7\}$	381

TABLE 7. Output of Algorithms 5.15, 5.20 and 5.27, after removing extraneous primes, for Picard curves from Sutherland’s 7-smooth dataset.

6.3. Other smooth plane quartic curves. As part of the work [FKS25] on classification of Sato-Tate groups of abelian threefolds, Fite, Kedlaya and Sutherland conducted several large-scale enumerations of genus 3 curves over $\mathbb{Q}$, with the aim of realising many Sato-Tate groups through such Jacobians. This was done by extending Sutherland’s original computation [Sut19] of the genus 3 smooth plane quartic database, and retaining all smooth plane quartic models with integer coefficients of absolute value at most 9, and whose discriminants are 7-smooth (divisible only by primes $p \leq 7$), or of absolute value at most 10^9 . In their type B dataset, there are 17 smooth plane quartic curves whose Jacobians appear to have geometric endomorphism algebra isomorphic to $\mathbb{Q}(\sqrt{-7})$. We certify the existence of extra endomorphisms for these 17 curves using the endomorphisms package of [Cos+19], thus showing that there is a subring of $\text{End}^0(\text{Jac}(C)_{\overline{\mathbb{Q}}})$ isomorphic to $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Algorithms 5.20, 5.27 and 5.33 return the empty set on each of these curves, while Algorithm 5.15 returns $\{2\}$ for 5 of these curves and the empty set for the remaining curves. Since Algorithms 5.15, 5.20, 5.27 and 5.33 succeed we conclude that the geometric endomorphism algebra does not merely contain

$\mathbb{Q}(\sqrt{-7})$, but is rather isomorphic to it, in all these cases. The results of the algorithms inform us that the mod- ℓ Galois representations have as large an image as possible for every semistable admissible prime $\ell > 3$.

REFERENCES

- [AFP22] Sualeh Asif, Francesc Fité, and Dylan Pentland. “Computing L -polynomials of Picard curves from Cartier-Manin matrices”. In: *Math. Comp.* 91.334 (2022). With an appendix by A. V. Sutherland, pp. 943–971 (cit. on pp. 20, 36).
- [Bal+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. “Explicit Chabauty-Kim for the split Cartan modular curve of level 13”. In: *Ann. of Math. (2)* 189.3 (2019), pp. 885–944 (cit. on p. 2).
- [Bal+23] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. “Quadratic Chabauty for modular curves: algorithms and examples”. In: *Compos. Math.* 159.6 (2023), pp. 1111–1152 (cit. on p. 2).
- [Ban+24] Barinder S. Banwait, Armand Brumer, Hyun Jong Kim, Zev Klagsbrun, Jacob Mayle, Padmavathi Srinivasan, and Isabel Vogt. “Computing nonsurjective primes associated to Galois representations of genus 2 curves”. In: *LuCaNT: LMFDB, computation, and number theory*. Vol. 796. Contemp. Math. Amer. Math. Soc., 2024, pp. 129–163 (cit. on p. 3).
- [Bil11] Nicolas Billerey. “Critères d’irréductibilité pour les représentations des courbes elliptiques”. In: *Int. J. Number Theory* 7.4 (2011), pp. 1001–1032 (cit. on p. 20).
- [BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*. Second. Vol. 302. Grundlehren der mathematischen Wissenschaften. Springer-Verlag, Berlin, 2004, pp. xii+635 (cit. on pp. 5, 6).
- [Bom+24] Raymond van Bommel, Shiva Chidambaram, Edgar Costa, and Jean Kieffer. “Computing isogeny classes of typical principally polarized abelian surfaces over the rationals”. In: *LuCaNT: LMFDB, computation, and number theory*. Vol. 796. Contemp. Math. Amer. Math. Soc., 2024, pp. 187–214 (cit. on p. 3).
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. “The Magma algebra system. I. The user language”. In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265 (cit. on p. 3).
- [BHR13] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*. Vol. 407. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2013, pp. xiv+438 (cit. on pp. 3, 4, 12, 17, 19).
- [Bro24] Michel Broué. *From rings and modules to Hopf algebras—one flew over the algebraist’s nest*. Springer, Cham, 2024 (cit. on p. 6).

- [CP23] Jerson Caro and Hector Pasten. “A Chabauty-Coleman bound for surfaces”. In: *Invent. Math.* 234.3 (2023), pp. 1197–1250 (cit. on p. 3).
- [Chi91] Wên Chên Chi. “On the l -adic representations attached to simple abelian varieties of type IV”. In: *Bull. Austral. Math. Soc.* 44.1 (1991), pp. 71–78 (cit. on p. 8).
- [CG26] Shiva Chidambaram and Pip Goodman. *Residual representations of IM abelian threefolds*. <https://github.com/shiva-chid/Picard>. 2026 (cit. on p. 3).
- [Cos+19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. “Rigorous computation of the endomorphism ring of a Jacobian”. In: *Math. Comp.* 88.317 (2019), pp. 1303–1339 (cit. on pp. 39–41).
- [DLO25] Giovanni De Franceschi, Martin W. Liebeck, and Eamonn A. O’Brien. *Conjugacy in finite classical groups*. Springer, Cham, 2025 (cit. on p. 7).
- [Del82] Pierre Deligne. “Hodge cycles on abelian varieties (notes by J.S. Milne)”. In: *Hodge Cycles, Motives, and Shimura Varieties*. Springer-Verlag, Berlin Heidelberg, 1982, pp. 9–100 (cit. on pp. 8, 9).
- [Die02] Luis V. Dieulefait. “Explicit determination of the images of the Galois representations attached to abelian surfaces with $\text{End}(A) = \mathbb{Z}$ ”. In: *Experiment. Math.* 11.4 (2002), pp. 503–512 (cit. on p. 3).
- [Fit24] Francesc Fité. “Ordinary primes for some varieties with extra endomorphisms”. In: *Publ. Mat.* 68.1 (2024), pp. 27–40 (cit. on p. 13).
- [FG26] Francesc Fité and Pip Goodman. “Abelian threefolds with imaginary multiplication”. In: *J. Lond. Math. Soc. (2)* 114.1 (2026) (cit. on p. 20).
- [FKS25] Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland. “Sato-Tate groups of abelian threefolds”. In: *Mem. Amer. Math. Soc.* 312.1582 (2025) (cit. on p. 41).
- [FL26] Lorenzo Furio and Davide Lombardo. *On 7-adic Galois representations for elliptic curves over $\mathbb{Q}$* . 2026. arXiv: 2507.17967 [math.NT] (cit. on p. 2).
- [Goo25] Pip Goodman. “Superelliptic curves with large Galois images”. In: *Math. Z.* 309.3 (2025), Paper No. 56, 46 (cit. on pp. 14, 17, 35).
- [Goo26a] Pip Goodman. “Endomorphism algebras of abelian varieties with large cyclic 2-torsion field over a given field”. In: *Res. Number Theory* 12.2 (2026), Paper No. 34, 13 (cit. on p. 17).
- [Goo26b] Pip Goodman. “Ruling out 1 dimensional factors from compatible systems”. In preparation. 2026 (cit. on p. 20).
- [GR72] Alexander Grothendieck and Michel Raynaud. *Modeles de Néron et monodromie*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1972, pp. 313–523 (cit. on pp. 14, 21, 22, 35).
- [Gro02] Larry C. Grove. *Classical groups and geometric algebra*. Vol. 39. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2002, pp. x+169 (cit. on pp. 16, 36).

- [HS14] David Harvey and Andrew V. Sutherland. “Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time”. In: *LMS J. Comput. Math.* 17 (2014), pp. 257–273 (cit. on p. 36).
- [HS16] David Harvey and Andrew V. Sutherland. “Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II”. In: *Frobenius distributions: Lang-Trotter and Sato-Tate conjectures*. Vol. 663. Contemp. Math. Amer. Math. Soc., Providence, RI, 2016, pp. 127–147 (cit. on p. 36).
- [KS08] Kiran S. Kedlaya and Andrew V. Sutherland. “Computing L-Series of Hyperelliptic Curves”. In: *Algorithmic Number Theory*. Springer Berlin Heidelberg, 2008, pp. 312–326 (cit. on p. 36).
- [KL90] Peter Kleidman and Martin Liebeck. *The subgroup structure of the finite classical groups*. Vol. 129. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1990 (cit. on pp. 2, 3, 9, 11, 12, 18).
- [Lan83] Serge Lang. *Complex multiplication*. Vol. 255. Grundlehren der mathematischen Wissenschaften. Springer-Verlag, New York, 1983 (cit. on p. 11).
- [LV14] Eric Larson and Dmitry Vaintrob. “Determinants of subquotients of Galois representations associated with abelian varieties”. In: *J. Inst. Math. Jussieu* 13.3 (2014), pp. 517–559 (cit. on p. 14).
- [Mum70] David Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. Oxford University Press, London, 1970 (cit. on p. 11).
- [Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften. Springer-Verlag, Berlin, 1999 (cit. on p. 21).
- [Ray74] Michel Raynaud. “Schémas en groupes de type $(p, \dots, p)$ ”. In: *Bull. Soc. Math. France* 102 (1974), pp. 241–280 (cit. on p. 14).
- [Rib76] Kenneth A. Ribet. “Galois action on division points of Abelian varieties with real multiplications”. In: *Amer. J. Math.* 98.3 (1976), pp. 751–804 (cit. on pp. 10, 12, 13, 19).
- [RSZ22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. “ ℓ -adic images of Galois for elliptic curves over $\mathbb{Q}$ ”. In: *Forum Math. Sigma* 10 (2022). With an appendix with John Voight, Paper No. e62, 63 (cit. on p. 2).
- [Sch88] Norbert Schappacher. *Periods of Hecke characters*. Vol. 1301. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1988 (cit. on p. 13).
- [Ser72] Jean-Pierre Serre. “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”. In: *Invent. Math.* 15.4 (1972), pp. 259–331 (cit. on pp. 2, 13, 14).
- [Ser87] Jean-Pierre Serre. “Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ”. In: *Duke Math. J.* 54.1 (1987), pp. 179–230 (cit. on p. 25).

- [ST68] Jean-Pierre Serre and John Tate. “Good reduction of abelian varieties”. In: *Ann. of Math. (2)* 88 (1968), pp. 492–517 (cit. on p. 35).
- [Sha54] Igor R. Shafarevich. “Construction of fields of algebraic numbers with given solvable Galois group”. In: *Izv. Akad. Nauk SSSR Ser. Mat.* 18 (1954), pp. 525–578 (cit. on p. 38).
- [Shi63] Goro Shimura. “On analytic families of polarized abelian varieties and automorphic functions”. In: *Ann. of Math. (2)* 78 (1963), pp. 149–192 (cit. on p. 6).
- [Shi98] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*. Vol. 46. Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1998 (cit. on pp. 6, 11).
- [Sil92] Alice Silverberg. “Fields of definition for homomorphisms of abelian varieties”. In: *J. Pure Appl. Algebra* 77.3 (1992), pp. 253–262 (cit. on p. 16).
- [Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994 (cit. on p. 6).
- [Spr51] Tonny A. Springer. *Over Symplectische Transformaties*. Thesis. University of Leiden, 1951, p. 35 (cit. on p. 7).
- [Sut16] Andrew V. Sutherland. “Computing images of Galois representations attached to elliptic curves”. In: *Forum Math. Sigma* 4 (2016), Paper No. e4, 79 (cit. on p. 2).
- [Sut19] Andrew V. Sutherland. “A database of nonhyperelliptic genus-3 curves over $\mathbb{Q}$ ”. In: *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*. Vol. 2. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2019, pp. 443–459 (cit. on p. 41).
- [Sut20] Andrew V. Sutherland. “Counting points on superelliptic curves in average polynomial time”. In: *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*. Vol. 4. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2020, pp. 403–422 (cit. on p. 36).
- [Wal63] Gordon E. Wall. “On the conjugacy classes in the unitary, symplectic and orthogonal groups”. In: *J. Austral. Math. Soc.* 3 (1963), pp. 1–62 (cit. on p. 7).
- [Zyw20] David Zywina. *On the surjectivity of mod ℓ representations associated to elliptic curves*. 2020. arXiv: 1508.07661 [math.NT] (cit. on p. 2).

UNIVERSITY OF WISCONSIN-MADISON, 480 LINCOLN DR, MADISON, WI 53706 USA.

Email address: chidambaram3@wisc.edu

URL: <https://people.math.wisc.edu/~chidambaram3/>

MAX PLANCK INSTITUTE FOR MATHEMATICS, VIVATSGASSE 7, 53111 BONN, GERMANY

Email address: pip.goodman@ub.edu

URL: <https://pipgoodman.github.io/>