

UC San Diego

UC San Diego Previously Published Works

Title

Sato-Tate groups of abelian threefolds: a preview of the classification

Permalink

<https://escholarship.org/uc/item/3dk1n4sz>

Authors

Fité, Francesc
Kedlaya, Kiran
Sutherland, Andrew

Publication Date

2021

DOI

10.1090/conm/770/15432

Peer reviewed

Sato–Tate groups of abelian threefolds: a preview of the classification

Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland

ABSTRACT. We announce the classification of Sato–Tate groups of abelian threefolds over number fields; there are 410 possible conjugacy classes of closed subgroups of $\mathrm{USp}(6)$ that occur. We summarize the key points of the “upper bound” aspect of the classification, and give a more rigorous treatment of the “lower bound” by realizing 33 groups that appear in the classification as maximal cases with respect to inclusions of finite index. Further details will be provided in a subsequent paper.

1. Introduction

The *Sato–Tate group* of an abelian variety A over a number field k is a certain compact Lie group which conjecturally governs the distribution of normalized Euler factors of the L -function of A . For example, if A is an elliptic curve, then the Sato–Tate group is determined by whether or not A has complex multiplication (and if so, whether the field of complex multiplication is contained in k). In the generic case where A has no complex multiplication, its Sato–Tate group is $\mathrm{SU}(2)$ and the usual Sato–Tate conjecture predicts that the distribution of normalized Frobenius traces of A in the interval $[-2, 2]$ is the same as the distributions of traces of random matrices in $\mathrm{SU}(2)$ determined by the Haar measure on $\mathrm{SU}(2)$; this is known when k is a totally real field [BLGG11] or a CM field [AAC...18].

The present paper constitutes an announcement of the classification of Sato–Tate groups of abelian threefolds over number fields, in the style of the classification of Sato–Tate groups of abelian surfaces made in [FKRS12] (building upon [KS08, KS09]). These groups are closed subgroups of $\mathrm{USp}(6)$ that are defined up to conjugacy; we find that there are 410 Sato–Tate groups that occur for abelian threefolds (compared to 3 for elliptic curves and 52 for abelian surfaces).

1991 *Mathematics Subject Classification*. Primary 11M50; Secondary 11G10, 11G20, 14G10, 14K15.

Key words and phrases. Sato–Tate groups, abelian threefolds over number fields.

Fité was supported by the Institute for Advanced Study during 2018–2019 via NSF grant DMS-1638352, and by the Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation (Simons Foundation grant 550033).

Kedlaya was financially supported by the NSF (grant DMS-1802161), UC San Diego (Stefan E. Warschawski professorship), and IAS (visiting professorship 2018–2019).

Sutherland was financially supported by the NSF (grant DMS-1522526) and by the Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation (Simons Foundation grant 550033).

Given the dramatically larger size of the classification in dimension 3, it is not feasible to give a complete account here; we have thus structured this article as a preview of our subsequent paper [FKS] in which we give a complete treatment. Here, we focus on the following steps.

- In §2, we recall some theoretical background needed to make a rigorous definition of the Sato–Tate group; recall a twisting construction that will be needed to realize certain candidate Sato–Tate groups; and formulate some necessary conditions on Sato–Tate groups that reduce the classification to a finite problem (the *Sato–Tate axioms*).
- In §3, we state the classification of closed subgroups of $\mathrm{USp}(6)$ satisfying the Sato–Tate axioms to be obtained in [FKS] (Theorem 3.1); there are 433 such groups. We identify the 14 connected groups that can occur, corresponding to the possible geometric endomorphism \mathbb{R} -algebras of an abelian threefold over an algebraically closed field of characteristic 0. For each such group G^0 , we describe the maximal finite-index overgroups of G^0 that occur; the derivation of this description is given completely in all cases except when G^0 is a one-dimensional torus. In this case, we state a uniform presentation of the maximal overgroups using complex reflection groups, and summarize how the description of finite subgroups of $\mathrm{PSU}(3)$ by Blichfeldt–Dickson–Miller [MBD61] is used to confirm this list in [FKS].
- In §4, we give a complete proof (modulo enumeration of groups; see below) that within the list of 433 groups from Theorem 3.1, exactly 410 occur as Sato–Tate groups (Theorem 4.1). More precisely, we show that exactly 23 groups must be omitted; these groups have identity components containing a factor which is a two-dimensional or three-dimensional torus, and the exclusion of these groups requires a careful study of Shimura’s theory of CM types analogous to [FKRS12, §4.3]. Revising the list of maximal subgroups enumerated in §3 based on this exclusion yields a list of 33 candidate groups which are maximal with respect to inclusions of finite index. Using products and twisting constructions, we show that each maximal group arises from some abelian threefold over \mathbb{Q} or $\mathbb{Q}(\sqrt{3})$; by base extension, we may obtain examples of abelian threefolds (over various number fields) realizing all candidate groups.

We defer to [FKS] the discussion of the following aspects, which for abelian surfaces are treated in [FKRS12].

- Giving a detailed proof of Theorem 3.1. This amounts to confirming that every group that can occur is contained in one of the announced maximal groups.
- Enumerating the finite-index subgroups of the announced maximal groups in order to verify that they represent 433 distinct conjugacy classes within $\mathrm{USp}(6)$. This is needed to confirm that the lower bound in Theorem 3.1 is indeed equal to 410.
- Computation of moment statistics and point densities. For abelian surfaces, all 52 Sato–Tate groups can be distinguished by their moments, but this fails for threefolds.

- Rigorous determination of the Sato–Tate group of an explicitly specified abelian threefold. One approach to this is to compute endomorphism algebras using the method of [CMSV19].
- Large-scale surveys of Sato–Tate groups. With the computational resources and software tools now available [Sut18a, Sut18b], this can now be done at much greater scale than in [FKRS12].
- Distinguishing between Jacobians of curves, principally polarized abelian threefolds, and arbitrary abelian threefolds. For abelian surfaces this does not change the classification of Sato–Tate groups, as was shown in [FKRS12] using a large scale survey of genus 2 curves over \mathbb{Q} . For threefolds the situation is not yet clear.
- Analysis of fields of definition. For abelian surfaces, only 34 of the 52 possible groups occur over \mathbb{Q} ; the situation for abelian threefolds is unclear.

2. Background on Sato–Tate groups

In this section, we recall some of the theoretical results from [FKRS12] that form the basis of the classification of Sato–Tate groups of abelian surfaces, and extend these as required to handle the case of abelian threefolds. We then use these results to classify the possible identity components of Sato–Tate groups of abelian threefolds. See [Sut16] for an overview of this circle of ideas.

2.1. The Mumford–Tate group. We begin by recalling the definition of the Mumford–Tate group of a (polarized) abelian variety A over a number field k . This construction carries enough information to determine the identity component of the Sato–Tate group.

DEFINITION 2.1. Fix an embedding of k into \mathbb{C} and set $V := H^1(A_{\mathbb{C}}^{\text{top}}, \mathbb{Q})$; it carries an alternating pairing ψ given by the cup product. Via the description of $A_{\mathbb{C}}^{\text{top}}$ as a complex torus, we obtain an \mathbb{R} -linear identification of $V \otimes_{\mathbb{Q}} \mathbb{R}$ with the tangent space of $A_{\mathbb{C}}$ at the origin (or equivalently, the dual of the space of holomorphic differentials on $A_{\mathbb{C}}$). The *Mumford–Tate group* of A , denoted $\text{MT}(A)$, is the smallest \mathbb{Q} -algebraic subgroup of $\text{GL}(V)$ whose base extension to \mathbb{R} contains the scalar action of \mathbb{C}^{\times} on $V \otimes_{\mathbb{Q}} \mathbb{R}$; this group is contained in the symplectic group $\text{GSp}(V, \psi)$. It follows from Deligne’s theorem on absolute Hodge cycles (see [DM82]) that the definition of $\text{MT}(A)$ does not depend on the choice of the embedding of k into \mathbb{C} ; it is also clearly invariant under enlargement of k .

DEFINITION 2.2. The *Hodge group* $\text{Hg}(A)$ is the intersection $\text{MT}(A) \cap \text{Sp}(V, \psi)$. The *Lefschetz group* $\text{L}(A)$ is the connected component of the identity in the centralizer of $\text{End}(A_{\bar{k}})_{\mathbb{Q}}$ in $\text{Sp}(V, \psi)$. There is an obvious inclusion $\text{Hg}(A) \subseteq \text{L}(A)$.

PROPOSITION 2.3. For $g \leq 3$, we have $\text{Hg}(A) = \text{L}(A)$. (That is, the Mumford–Tate group is determined by endomorphisms.)

PROOF. See [FKRS12, Theorem 2.16]. □

REMARK 2.4. As shown by Mumford [Mum69], Proposition 2.3 fails for $g = 4$. The case $g = 3$ considered here is the last case where the endomorphism-based methods developed in [FKRS12] and extended here and in [FKS] will suffice.

2.2. Definition of the Sato–Tate group. We continue with the definition of the algebraic Sato–Tate group and Sato–Tate group of an abelian variety A over a number field k in terms of ℓ -adic monodromy, and the statement of the refined Sato–Tate conjecture. This material is taken primarily from [FKRS12, §2.1], but includes some further results from [BaK15, §2] and [BaK16] that we note here.

We denote by $\text{End}(A)$ the ring of endomorphisms of A (defined over k). By the endomorphism field of A , we refer to the minimal extension K of k such that $\text{End}(A_K)$ coincides with the geometric endomorphism ring $\text{End}(A_{\bar{k}})$ of A . Note that K/k is a finite and Galois extension.

DEFINITION 2.5. For each $\tau \in \text{Gal}(K/k)$, define

$$L(A, \tau) := \{\gamma \in \text{Sp}(V, \psi) : \gamma^{-1}\alpha\gamma = \tau(\alpha) \text{ for all } \alpha \in \text{End}(A_K)\}.$$

The *twisted Lefschetz group* $\text{TL}(A)$ is the union of $L(A, \tau)$ over all τ .

PROPOSITION 2.6. For $g \leq 3$, for any prime ℓ , $\text{TL}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$ is the kernel of the symplectic character on the Zariski closure of the image of $\rho_{\ell} : G_k \rightarrow H_{\text{et}}^1(A_{\bar{k}}, \mathbb{Q}_{\ell})$.

PROOF. This amounts to the statement that the Mumford–Tate conjecture holds for A whenever $g \leq 3$. See for example [BaK15, Theorem 6.11]. \square

DEFINITION 2.7. In light of Proposition 2.3 and Proposition 2.6, for $g \leq 3$, we define the *Sato–Tate group* $\text{ST}(A)$ to be a maximal compact subgroup of $\text{TL}(A) \otimes_{\mathbb{Q}} \mathbb{C}$.

LEMMA 2.8. For $g \leq 3$, there is a canonical isomorphism $\text{ST}(A)/\text{ST}(A)^0 \rightarrow \text{Gal}(K/k)$. In particular, this isomorphism is compatible with base change: for any finite extension k' of k , $\text{ST}(A_{k'})$ is the inverse image of $\text{Gal}(k'K/k') \subseteq \text{Gal}(K/k)$ in $\text{ST}(A)$.

PROOF. This is again a consequence of [BaK15, Theorem 6.11]. \square

REMARK 2.9. In the definition of the Sato–Tate group, we are implicitly using the fact that for $g \leq 3$, the Mumford–Tate group of A is determined by endomorphisms. For general g , it is expected that the role of $\text{TL}(A)$ in Proposition 2.6 can be filled by a certain algebraic group over \mathbb{Q} , the *motivic Sato–Tate group*, whose definition involves algebraic cycles on $A \times A$ of all codimensions, not just endomorphisms [BaK16]. There is still a canonical surjection $\text{ST}(A)/\text{ST}(A)^0 \rightarrow \text{Gal}(K/k)$, but it is not in general an isomorphism.

2.3. Twisting and the Sato–Tate group.

DEFINITION 2.10. For L/k a finite Galois extension and ξ a 1-cocycle of $\text{Gal}(L/k)$ valued in $\text{Aut}(A_L)$, there exists a unique (up to unique isomorphism) abelian variety A_{ξ} over k and an isomorphism $\theta : A_{\xi, L} \rightarrow A_L$ such that

$$\xi(\sigma) = \theta^{\sigma} \circ \theta^{-1} \quad (\text{for all } \sigma \in \text{Gal}(L/k)).$$

Moreover, A_{ξ} depends only on the class of ξ in the pointed set $H^1(\text{Gal}(L/k), \text{Aut}(A_L))$.

EXAMPLE 2.11. Let E be an elliptic curve without complex multiplication defined over \mathbb{Q} and let L/\mathbb{Q} be a Galois extension. Let $A = E^d$, and fix an isomorphism $\text{Aut}(A_L) \simeq \text{GL}_d(\mathbb{Z})$ for some integer $d \geq 1$. For every rational degree d Artin representation ρ , there is a choice of a basis for which the image of ρ lies in $\text{GL}_d(\mathbb{Z})$. We may thus regard a rational degree d representation of $\text{Gal}(L/\mathbb{Q})$ as a 1-cocycle

$$\xi : \text{Gal}(L/\mathbb{Q}) \rightarrow \text{Aut}(A_L).$$

The endomorphism field of the abelian d -fold A_ξ defined above is the field cut out by the representation $\rho \otimes \rho^\vee$. The Galois group of the endomorphism field is thus isomorphic to the projective image of the original degree d rational representation ρ of $\text{Gal}(L/\mathbb{Q})$. We will use this construction in §4.2.4.

EXAMPLE 2.12. Similarly, let E be an elliptic curve over \mathbb{Q} with complex multiplication by the maximal order of the imaginary quadratic field M (which must have class number one, since E is defined over \mathbb{Q}). Let L/\mathbb{Q} be a Galois extension containing M for which the extension

$$1 \rightarrow \text{Gal}(L/M) \rightarrow \text{Gal}(L/\mathbb{Q}) \rightarrow \text{Gal}(M/\mathbb{Q}) \rightarrow 1$$

is split. Let $A = E^d$, and fix an isomorphism $\text{Aut}(A_L) \simeq \text{GL}_d(\mathcal{O}_M)$ for some integer $d \geq 1$. For the action of C_2 on $\text{GL}_d(M)$ via complex conjugation on M , suppose that $\tilde{\rho} : \text{Gal}(L/\mathbb{Q}) \rightarrow \text{GL}_d(M) \rtimes C_2$ is a representation whose restriction ρ to $\text{Gal}(L/M)$ factors through $\text{GL}_d(M)$. Since \mathcal{O}_M has class number 1, there is a choice of basis of M^d for which ρ factors through a representation $\rho_0 : \text{Gal}(L/M) \rightarrow \text{GL}_d(\mathcal{O}_M)$.

Suppose further that the basis of M^d can be chosen so that $\tilde{\rho}$ factors through $\text{GL}_d(\mathcal{O}_M) \rtimes C_2$ (see Remark 2.13). We then obtain from $\tilde{\rho}$ a cocycle

$$\xi : \text{Gal}(L/\mathbb{Q}) \rightarrow \text{Aut}(A_L)$$

and again the Galois group of the endomorphism field of A_ξ is isomorphic to the projective image of $\text{Gal}(L/\mathbb{Q})$. We will use this construction in §4.2.5.

REMARK 2.13. In Example 2.11, the condition that $\tilde{\rho}$ can be factored through $\text{GL}_d(\mathcal{O}_M) \rtimes C_2$ is equivalent to requiring the existence of a choice of ρ_0 for which

$$(2.1) \quad \rho_0 \cong c_M \circ \rho_0 \circ c,$$

where c denotes the action of $\text{Gal}(M/\mathbb{Q})$ on $\text{Gal}(L/M)$ while c_M denotes complex conjugation on \mathcal{O}_M^d . The following considerations will be useful.

- (i) We automatically have (2.1) if ρ_0 is uniquely determined by ρ . (This can only occur if ρ is absolutely irreducible.)
- (ii) We also have (2.1) if $\tilde{\rho}$ descends to $\text{GL}_d(\mathbb{Z}) \times C_2$ and $\text{Gal}(M/\mathbb{Q})$ acts on $\text{Gal}(L/M)$ as an inner automorphism.
- (iii) When ρ_0 is not uniquely determined by ρ , the choices for ρ_0 will be distinguished by their reductions modulo some $\alpha \in \mathcal{O}_M$. Using this, we can sometimes track the effects of c and c_M and thus detect whether or not (2.1) holds.

REMARK 2.14. We will encounter a small number of cases where (2.1) fails. In these cases, we have an isomorphism $\rho \cong c_M \circ \rho \circ c$ which does not descend to ρ_0 ; that is, the image of ρ_0 is normalized by some matrix of $\text{GL}_d(M) \setminus \text{GL}_d(\mathcal{O}_M)$.

In general, such cases correspond to twists not of E^d but of an isogenous abelian variety (which by [Kan11, Theorem 2] is itself a product of elliptic curves isogenous to E). We work out two specific constructions of this type. (Compare [SM74, §4] or [Ma11, Example 5.15].)

- Let E be the elliptic curve $y^2 = x^3 - 1$; E has CM by the maximal order $\mathbb{Z}[\zeta_3]$ and contains the rational 2-torsion point $Q = (1, 0)$, with the other two 2-torsion points Q_1, Q_2 being defined over M . Let A be the quotient of the Weil restriction of E_M from M to \mathbb{Q} by the rational subgroup of

order 2 corresponding to $\langle Q_1 \rangle$; then

$$\begin{aligned} \text{End}(A_M) &\cong M_2(\mathcal{O}_M) \cap \begin{pmatrix} 2^{-1} & 0 \\ 0 & 1 \end{pmatrix} M_2(\mathcal{O}_M) \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathcal{O}_M) : b \equiv 0 \pmod{2} \right\} \end{aligned}$$

with the action of $\text{Gal}(M/\mathbb{Q})$ given by

$$g \mapsto \begin{pmatrix} 2^{-1} & 0 \\ 0 & 1 \end{pmatrix} \bar{g} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

(Note that $A_M \cong E_M \times E'_M$ where $E'_M = E_M/\langle Q_1 \rangle$ has CM by the nonmaximal order $\mathbb{Z}[2\zeta_3]$.)

- Put $k = \mathbb{Q}(\sqrt{3})$. Let E be the elliptic curve over $\mathbb{Q}(\sqrt{3})$ with LMFDB label [2.2.12.1-9.1-a3](#); it has CM by $\mathbb{Z}[i]$ and has a rational point Q of order 3. Let A be the product $E \times E/\langle Q \rangle$; then

$$\begin{aligned} \text{End}(A) &\cong M_2(\mathcal{O}_M) \cap \begin{pmatrix} 3^{-1} & 0 \\ 0 & 1 \end{pmatrix} M_2(\mathcal{O}_M) \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathcal{O}_M) : b \equiv 0 \pmod{3} \right\} \end{aligned}$$

with the action of $\text{Gal}(M/\mathbb{Q})$ given by

$$g \mapsto \begin{pmatrix} 3^{-1} & 0 \\ 0 & 1 \end{pmatrix} \bar{g} \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}.$$

(Note that $E/\langle Q \rangle$ has CM by the nonmaximal order $\mathbb{Z}[3i]$.)

2.4. Axioms for Sato–Tate groups. A key tool used to classify Sato–Tate groups in [\[FKRS12\]](#) is a list of necessary conditions called the *Sato–Tate axioms*. The formulation in [\[FKRS12, Definition 3.1\]](#) is applicable to arbitrary motives; we state here a restricted form of the three original Sato–Tate axioms applicable to the 1-motives associated to abelian threefolds. We also add a fourth axiom coming from the fact that the Sato–Tate group of an abelian threefold is determined by endomorphisms ([Proposition 2.3](#)).

DEFINITION 2.15. For a subgroup G of $\text{GL}_6(\mathbb{C})$ with identity connected component G^0 , the *Sato–Tate axioms (for abelian threefolds)* are as follows.

- (ST1) The group G is a closed subgroup of $\text{USp}(6)$. For definiteness, we take the latter to be defined with respect to the symplectic form given by the block matrix

$$J = \begin{pmatrix} 0 & I_3 \\ -I_3 & 0 \end{pmatrix},$$

where I_3 denotes a 3×3 identity matrix, unless otherwise specified.

- (ST2) (Hodge condition) There exists a homomorphism $\theta: \text{U}(1) \rightarrow G^0$ such that $\theta(u)$ has eigenvalues u, u^{-1} of multiplicity 3. The image of such a θ is a *Hodge circle*, and the set of all Hodge circles must generate a dense subgroup of G^0 .
- (ST3) (Rationality condition) For each component H of G and each irreducible character χ of $\text{GL}_6(\mathbb{C})$, the expected value (under the Haar measure) of $\chi(\gamma)$ over $\gamma \in H$ is an integer. In particular, for any positive integers m and n , the expectation $\text{E}[\text{Trace}(\gamma, \wedge^m \mathbb{C}^6)^n : \gamma \in H]$ is an integer.

(ST4) (Lefschetz condition) The subgroup of $\mathrm{USp}(6)$ fixing $\mathrm{End}(\mathbb{C}^6)^{G^0}$ is G^0 .

PROPOSITION 2.16. Let A be an abelian threefold over k . Then $G = \mathrm{ST}_A$ satisfies the Sato–Tate axioms.

PROOF. For (ST1), (ST2), (ST3), this is [FKRS12, Proposition 3.2] except that the density condition in (ST2) is not stated therein; that statement is a consequence of the definition of the Mumford–Tate group [FKRS12, Definition 2.11]. For (ST4), apply Proposition 2.3. \square

3. Classification: an overview

This section is mainly expository. We report on several aspects of the following theorem, whose proof will appear in the upcoming work [FKS].

THEOREM 3.1 ([FKS]). *Up to conjugacy, at most 433 subgroups of $\mathrm{GL}_6(\mathbb{C})$ satisfy the Sato–Tate axioms for an abelian threefold. Among these, 30 are maximal with respect to finite index inclusions.*

REMARK 3.2. In §4, we will show that all 433 groups of the above theorem satisfy the Sato–Tate axioms (see Remark 4.7).

We will describe the possible connected components of these groups (§3.1), explain their connection to the possible geometric endomorphism rings of abelian threefolds (§3.2), and for each identity component present the extensions that are maximal with respect to the relation of inclusion of finite index up to conjugacy (§3.3). We should nevertheless emphasize that §3.1 and §3.2 contain complete proofs; only §3.3 depends on results in [FKS].

3.1. Connected component of the identity. We first identify the connected groups that satisfy the Sato–Tate axioms (ST1), (ST2), (ST4). Note that condition (ST3) is vacuous for a connected group, as the expected value in question is simply the dimension of the fixed subspace of the representation with character χ .

Let G^0 be a connected group satisfying the Sato–Tate axioms and let T be a maximal torus of G^0 . Let \mathfrak{h} denote the Lie algebra of G^0 and let $\mathfrak{h}_{\mathbb{C}}$ be the complexification of \mathfrak{h} . Since T is contained in a maximal torus of $\mathrm{USp}(6)$, which is 3-dimensional, $\mathfrak{h}_{\mathbb{C}}$ has rank at most 3.

The set of Lie algebras of rank at most 3 can easily be determined from the classification of Dynkin diagrams:

r	Lie algebras of rank r
1	$\mathfrak{t}_1, \mathfrak{sl}_2 = \mathfrak{so}_3$
2	$\mathfrak{t}_2, \mathfrak{t}_1 \times \mathfrak{sl}_2, \mathfrak{sl}_2 \times \mathfrak{sl}_2 = \mathfrak{so}_4, \mathfrak{sl}_3, \mathfrak{sp}_4 = \mathfrak{so}_5, \mathfrak{g}_2$
3	$\mathfrak{t}_3, \mathfrak{t}_2 \times \mathfrak{sl}_2, \mathfrak{t}_1 \times \mathfrak{sl}_2 \times \mathfrak{sl}_2, \mathfrak{t}_1 \times \mathfrak{sl}_3, \mathfrak{t}_1 \times \mathfrak{sp}_4, \mathfrak{t}_1 \times \mathfrak{g}_2, \mathfrak{sl}_2 \times \mathfrak{sl}_2 \times \mathfrak{sl}_2, \mathfrak{sl}_2 \times \mathfrak{sl}_3, \mathfrak{sl}_2 \times \mathfrak{sp}_4, \mathfrak{sl}_2 \times \mathfrak{g}_2, \mathfrak{sl}_4 = \mathfrak{so}_6, \mathfrak{so}_7, \mathfrak{sp}_6$

The standard representation of $\mathrm{USp}(6)$ gives rise to a faithful 6-dimensional unitary symplectic self-dual representation of \mathfrak{h} . This eliminates some Lie algebras from the above list.

- There are no 6-dimensional symplectic representations of \mathfrak{sp}_4 except if we allow some trivial summands, but these violate (ST2).

- The smallest dimension of a nontrivial representation of \mathfrak{g}_2 is $7 > 6$; this also rules out $\mathfrak{t}_1 \times \mathfrak{g}_2$ and $\mathfrak{sl}_2 \times \mathfrak{g}_2$.
- The only nontrivial self-dual representation of \mathfrak{sl}_3 of dimension at most 6 is the sum of the standard 3-dimensional representation and its dual. This rules out $\mathfrak{sl}_2 \times \mathfrak{sl}_3$.
- The only nontrivial self-dual representation of \mathfrak{so}_6 is the standard representation, which is not symplectic.
- The smallest dimension of a nontrivial representation of \mathfrak{so}_7 is $7 > 6$.

The above considerations, together with an additional argument to rule out the group $U(2)$ (see [FKS16, Rem. 2.3]), allow us to conclude that G^0 must correspond to one of the following groups (the subscripts in the notation are defined below):

$\dim(T)$	Connected groups satisfying (ST1) and (ST2)
1	$U(1)_3, SU(2)_3, SO(3)$
2	$U(1) \times U(1)_2, U(1) \times SU(2)_2, SU(2) \times U(1)_2, SU(2) \times SU(2)_2, SU(3)$
3	$U(1) \times U(1) \times U(1), U(1) \times U(1) \times SU(2), U(1) \times SU(2) \times SU(2), U(3), U(1) \times USp(4), SU(2) \times SU(2) \times SU(2), SU(2) \times USp(4), USp(6)$

Each group comes equipped with a 6-dimensional representation, which may be inferred from the preceding table using the following considerations:

- The groups $SU(2)$, $USp(4)$, $USp(6)$ carry their standard representations.
- For $d = 2, 3$, the notations $U(1)_d, SU(2)_d$ refer to the d -fold diagonal representations of $U(1), SU(2)$.
- The groups $U(1), U(3)$ are embedded into $SU(2), USp(6)$ by the formula

$$(3.1) \quad A \mapsto \begin{pmatrix} A & 0 \\ 0 & \bar{A} \end{pmatrix}.$$

- The groups $SO(3)$ and $SU(3)$ are viewed in $USp(6)$ via the above embedding of $U(3)$.
- Note that the abstract group $U(1) \times SU(2)$ is considered twice: once as a subgroup of $U(1) \times U(1) \times SU(2)$ via the diagonal embedding of $U(1)$, and once as a subgroup of $U(1) \times SU(2) \times SU(2)$ via the diagonal embedding of $SU(2)$.

In the case $USp(6)$ and all of the product cases, one easily verifies that (ST4) is satisfied by following the methods of [FKRS12, §4]. This leaves the cases of $SO(3)$, $SU(3)$, and $U(3)$, which we work out by hand. Recall that $U(3)$ is embedded into $USp(6)$ via (3.1). As a result, we see that the endomorphisms of \mathbb{C}^6 commuting with $SO(3)$ or $SU(3)$ are those given by block scalar matrices, all of which also commute with $U(3)$. It follows that $SO(3)$ and $SU(3)$ do not satisfy (ST4).

The possible values for a connected G satisfying the Sato–Tate axioms are listed in the fourth column of Table 1.

3.2. Geometric endomorphism algebras. In this section we recover the possible geometric \mathbb{R} -algebras of endomorphisms of abelian threefolds from our classification of identity components of Sato–Tate groups. We then describe the possible geometric \mathbb{Q} -algebras of endomorphisms they correspond, by using Shimura’s refinement of Albert’s classification of division algebras equipped with a positive involution.

3.2.1. *Geometric endomorphism \mathbb{R} -algebras.* For an abelian threefold A defined over a number field k , we can recover the geometric endomorphism \mathbb{R} -algebra $\text{End}(A_{\bar{k}})_{\mathbb{R}} := \text{End}(A_{\bar{k}}) \otimes \mathbb{R}$ by first finding the subalgebra of $\text{End}(\mathbb{C}^6)$ commuting with $\text{ST}(A)^0$, then picking out the maximal positive definite subspace of this algebra under the Rosati form [FKRS12, Prop. 2.19].

In the case of $\text{USp}(6)$ and all the other product cases, the above computation is easily carried out with the methods of [FKRS12, §4]. In the case of $\text{U}(3)$ the Rosati form is given up to scalars by

$$\begin{pmatrix} uI_3 & 0 \\ 0 & vI_3 \end{pmatrix} \mapsto 6uv = \frac{3}{2}((u+v)^2 - (u-v)^2),$$

so the maximal positive definite subspace consists of those matrices for which $u+v \in \mathbb{R}$, $u-v \in i\mathbb{R}$, or equivalently $v = \bar{u}$. Therefore $\text{End}(A_{\bar{k}})_{\mathbb{R}} \simeq \mathbb{C}$. We assign letters **A**, **B**, \dots , **N** to each of the possibilities for $\text{End}(A_{\bar{k}})_{\mathbb{R}}$. We refer to this letter as the *absolute type* of A . The absolute types together with the possible values for $\text{End}(A_{\bar{k}})_{\mathbb{R}}$ are listed in the first and second columns of Table 1.

3.2.2. *Geometric endomorphism \mathbb{Q} -algebras.* For a simple abelian variety A of dimension $g \leq 3$, the work of Albert and Shimura leaves the following possibilities for the geometric \mathbb{Q} -algebra of endomorphisms $\text{End}(A_{\bar{k}})_{\mathbb{Q}} := \text{End}(A_{\bar{k}}) \otimes \mathbb{Q}$. Note that for a fixed $g \leq 3$, each possibility is distinguished by the \mathbb{Q} -dimension d of $\text{End}(A_{\bar{k}})_{\mathbb{Q}}$ (equal to the \mathbb{R} -dimension of $\text{End}(A_{\bar{k}})_{\mathbb{R}}$). (See for example [Oo87].)

g	d	Albert type	\mathbb{Q} -algebra
1	1	I(1)	\mathbb{Q}
	2	IV(1,1)	imaginary quadratic field
2	2	I(1)	real quadratic field
	4	I(2)	indefinite quaternion algebra
	6	IV(2,1)	quartic CM field
3	1	I(1)	\mathbb{Q}
	2	IV(1,1)	imaginary quadratic field
	3	I(3)	totally real cubic field
	6	IV(3,1)	sextic CM field

From the list of geometric \mathbb{Q} -algebra endomorphism types for simple abelian varieties of dimension $g \leq 3$ one can determine all possibilities for $g = 3$ by taking all possible products (including self products) that yield an abelian variety of dimension 3; there are 22 ways to do this. Each yields a distinct type of \mathbb{Q} -algebra, but only 14 distinct \mathbb{R} -algebras (for example, taking three non-isogenous elliptic curves of type I(1) yields the same \mathbb{R} -algebra $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ as a single RM abelian threefold of type I(3)). This leads to the following description of absolute types in terms of the the isogeny decomposition of $A_{\bar{k}}$ (compare with [Sut16, §4, Table 2]):

- (A) $A_{\bar{k}}$ is simple of type I(1);
- (B) $A_{\bar{k}}$ is simple of type IV(1,1);
- (C) $A_{\bar{k}}$ is isogenous to the product of an elliptic curve without CM and a simple abelian surface of type I(1);
- (D) $A_{\bar{k}}$ is isogenous to the product of an elliptic curve with CM and a simple abelian surface of type I(1);
- (E) $A_{\bar{k}}$ is either
 - simple of type I(3), or

- isogenous to the product of an elliptic curve without CM and a simple abelian surface of type I(2), or
 - isogenous to the product of three pairwise non-isogenous elliptic curves without CM;
- (F) $A_{\bar{k}}$ is either
- isogenous to the product of an elliptic curve with CM and two non-isogenous elliptic curves without CM, or
 - isogenous to the product of an elliptic curve with CM and a simple abelian surface of type I(2);
- (G) $A_{\bar{k}}$ is either
- isogenous to the product of an elliptic curve without CM and two nonisogenous elliptic curves with CM, or
 - isogenous to the product of an elliptic curve without CM and a simple abelian surface of type IV(2,1);
- (H) $A_{\bar{k}}$ is either
- simple of type IV(3,1), or
 - isogenous to the product of an elliptic curve with CM and a simple abelian surface of type IV(2,1), or
 - isogenous to the product of three pairwise non-isogenous elliptic curves with CM;
- (I) $A_{\bar{k}}$ is either
- isogenous to the product of an elliptic curve without CM and a simple abelian surface of type II(1), or
 - isogenous to the product of an elliptic curve E without CM and the square of an elliptic curve without CM nonisogenous to E ;
- (J) $A_{\bar{k}}$ is either
- isogenous to the product of an elliptic curve with CM and the square of an elliptic curve without CM, or
 - isogenous to the product of an elliptic curve with CM and a simple abelian surface of type II(1);
- (K) $A_{\bar{k}}$ is isogenous to the product of an elliptic curve without CM and the square of an elliptic curve with CM;
- (L) $A_{\bar{k}}$ is isogenous to the product of an elliptic curve E with CM and the square of an elliptic curve with CM nonisogenous to E ;
- (M) $A_{\bar{k}}$ is isogenous to the cube of an elliptic curve without CM;
- (N) $A_{\bar{k}}$ is isogenous to the cube of an elliptic curve with CM.

REMARK 3.3. The third column of Table 1 summarizes the discussion above. In the table one can see that absolute types are ordered according to the lexicographic ordering of pairs (r, d) where r is the rank of the Néron-Severi group of $A_{\bar{k}}$ and d is the \mathbb{R} -dimension of $\text{End}(A_{\bar{k}})_{\mathbb{R}}$. See [CFS19] for an interpretation of r and d in terms of the moments of the Sato–Tate group.

3.3. Extensions. Let G^0 be one of the connected groups obtained in §3.1. Let N and Z denote the normalizer and centralizer of G^0 within $\text{USp}(6)$. The general strategy in [FKS] to prove Theorem 3.1 exploits the bijection between:

- The set of (conjugacy classes of) closed subgroups G of $\text{USp}(6)$ with identity component G^0 that satisfy (ST3);

Type	$\text{End}(A_{\bar{k}})_{\mathbb{R}}$	Splitting of $A_{\bar{k}}$	$\text{ST}(A)^0$
A	\mathbb{R}	T	$\text{USp}(6)$
B	\mathbb{C}	S_{IM}	$\text{U}(3)$
C	$\mathbb{R} \times \mathbb{R}$	$E \times S$	$\text{SU}(2) \times \text{USp}(4)$
D	$\mathbb{C} \times \mathbb{R}$	$E_{\text{CM}} \times S$	$\text{U}(1) \times \text{USp}(4)$
E	$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	T_{RM} $E \times S_{\text{RM}}$ $E \times E' \times E''$	$\text{SU}(2) \times \text{SU}(2) \times \text{SU}(2)$
F	$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	$E_{\text{CM}} \times E' \times E''$ $E_{\text{CM}} \times S_{\text{RM}}$	$\text{U}(1) \times \text{SU}(2) \times \text{SU}(2)$
G	$\mathbb{C} \times \mathbb{C} \times \mathbb{R}$	$E_{\text{CM}} \times E'_{\text{CM}} \times E''$ $S_{\text{CM}} \times E$	$\text{U}(1) \times \text{U}(1) \times \text{SU}(2)$
H	$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	T_{CM} $E_{\text{CM}} \times S_{\text{CM}}$ $E_{\text{CM}} \times E'_{\text{CM}} \times E''_{\text{CM}}$	$\text{U}(1) \times \text{U}(1) \times \text{U}(1)$
I	$\mathbb{R} \times \text{M}_2(\mathbb{R})$	$E \times (E')^2$ $E \times S_{\text{QM}}$	$\text{SU}(2) \times \text{SU}(2)_2$
J	$\mathbb{C} \times \text{M}_2(\mathbb{R})$	$E_{\text{CM}} \times (E')^2$ $E_{\text{CM}} \times S_{\text{QM}}$	$\text{U}(1) \times \text{SU}(2)_2$
K	$\mathbb{R} \times \text{M}_2(\mathbb{C})$	$E \times (E'_{\text{CM}})^2$	$\text{SU}(2) \times \text{U}(1)_2$
L	$\mathbb{C} \times \text{M}_2(\mathbb{C})$	$E_{\text{CM}} \times (E'_{\text{CM}})^2$	$\text{U}(1) \times \text{U}(1)_2$
M	$\text{M}_3(\mathbb{R})$	E^3	$\text{SU}(2)_3$
N	$\text{M}_3(\mathbb{C})$	E_{CM}^3	$\text{U}(1)_3$

TABLE 1. Real endomorphism algebras and connected parts of Sato–Tate groups of abelian threefolds. We describe the decomposition up to isogeny of $A_{\bar{k}}$; when doing so, we denote by E , S , T simple abelian varieties over \bar{k} of respective dimensions 1, 2, 3. Given E , we denote by E' an elliptic curve not isogenous to E (a similar convention applies to E''). For $B \in \{E, S, T\}$, we write B_{CM} to indicate that B has complex multiplication by a CM field of degree $2 \dim(B)$ and B_{RM} to indicate that B has real multiplication by a field of degree $\dim(B)$. The lack of a subindex indicates that B has trivial endomorphism ring. We write S_{IM} (resp. S_{QM}) to indicate that S has multiplication by an imaginary quadratic field (resp. by an indefinite quaternion algebra over \mathbb{Q}).

- The set of (conjugacy classes of) finite subgroups H of N/G^0 such that HG^0 satisfies (ST3).

In this section we report on some aspects of this proof of Theorem 3.1. We will organize the discussion into four cases depending on the structure of the normalizer N . We say that G^0 is *decomposable* if there is a subgroup G_1^0 of $\text{SU}(2)$ and a subgroup G_2^0 of $\text{USp}(4)$ such that

$$(3.2) \quad G^0 = G_1^0 \times G_2^0.$$

The indecomposable cases correspond to $G^0 = \text{USp}(6), \text{U}(3)$. Suppose that G^0 is decomposable and let N_1 (resp. N_2) denote the normalizer of G_1^0 (resp. G_2^0) in $\text{SU}(2)$ (resp. $\text{USp}(4)$). We say that that G^0 is a *split product* (resp. a *non-split*

product) if

$$N = N_1 \times N_2, \quad (\text{resp. } N \supsetneq N_1 \times N_2).$$

Eight of the possibilities for G^0 happen to be split products. The non-split product cases include the *triple products* $SU(2) \times SU(2) \times SU(2)$ and $U(1) \times U(1) \times U(1)$, and also the *diagonal products* $SU(2)_3$ and $U(1)_3$.

REMARK 3.4. We will only impose (ST3) explicitly in the case of diagonal products (and, in fact, only a relaxed version of (ST3)). However, it should be noted that (ST3) will be imposed in an implicit way for the split products. We will postpone to §4 the verification that (ST3) is satisfied for all the extensions described in this section. In particular, it will follow from the discussion in §4 that, when G^0 is indecomposable or a triple product, any closed subgroup G of N with identity component G^0 automatically satisfies (ST3).

The main purpose of this section is to describe the 30 group extensions that potentially satisfy the Sato–Tate axioms and are maximal with respect to finite index inclusions (up to conjugacy). The distribution of these groups among the possibilities for G^0 will be discussed below and it is summarized in Table 3.

3.3.1. *Indecomposable cases.* In case $G^0 = \mathrm{USp}(6)$ (type **A**), it is clear that $G = G^0$, which is obviously maximal. In case $G^0 = U(3)$ (type **B**), we have $Z = U(1)_3 \subset G^0$ and $N = G^0 \cup JG^0$. Consequently, $N/G^0 \simeq C_2$, so G equals either G^0 or N , which is the only maximal group for the identity component $G^0 = U(3)$.

3.3.2. *Split products.* Note that in this case

$$G = G_1 \times G_2,$$

where G_1 is a subgroup of N_1 with identity component G_1^0 and G_2 is a subgroup of N_2 with identity component G_2^0 . Here G_i^0 is as in (3.2). We start with the cases where we must have $G_i = G_i^0$ for one i , in which case the options come directly from the other factor.

- In the case $G^0 = SU(2) \times \mathrm{USp}(4)$ (type **C**), we must have $G_i = G_i^0$ for $i = 1, 2$, so $G = G^0$. This yields a maximal group.
- In the case $G^0 = U(1) \times \mathrm{USp}(4)$ (type **D**), we must have $G_2 = G_2^0$, so $G = G_1 \times \mathrm{USp}(4)$ for $G_1 \in \{U(1), N(U(1))\}$. Then $G_1 = N(U(1))$ yields a maximal group.
- In the case $G^0 = SU(2) \times SU(2)_2$ (type **I**), we must have $G_1 = G_1^0$, so $G = SU(2) \times G_2$ for some G_2 among the groups of dimension $d = 3$ in [FKRS12, Table 8]. Among these groups, the maximal ones are $J(E_4)$ and $J(E_6)$. For this identity component we find 10 extensions, among which two are maximal, namely $SU(2) \times J(E_4)$ and $SU(2) \times J(E_6)$.
- In the case $G^0 = SU(2) \times U(1)_2$ (type **K**), we must have $G_1 = G_1^0$, so $G = SU(2) \times G_2$ for some G_2 among the groups of dimension $d = 1$ in [FKRS12, Table 8]. Among these groups, the maximal ones are $J(D_6)$ and $J(O)$. For this identity component we find 32 extensions, among which two are maximal, namely $SU(2) \times J(D_6)$ and $SU(2) \times J(O)$.
- In the case $G^0 = U(1) \times U(1) \times SU(2)$ (type **G**), take $G_1^0 = SU(2)$ and $G_2^0 = U(1) \times U(1)$; we must have $G_1 = G_1^0$, so $G = SU(2) \times G_2$ for some G_2 among the groups with dimension $d = 2$ in [FKRS12, Table 8]. Among these groups, only $F_{a,b,c}$ is maximal. For this identity component we find 8 extensions, of which one is maximal: $SU(2) \times F_{a,b,c}$ (we will return to this case in §4.1).

REMARK 3.5. As indicated by the asterisks that appear in [FKRS12, Table 8], the subgroup $F_{a,b,c}$ of $\mathrm{USp}(4)$ is one of three subgroups that satisfy the Sato–Tate axioms for abelian surfaces but do not arise as the Sato–Tate group of an abelian surface. This explains the discrepancy between the counts 55 and 52 in [FKRS12] of groups that satisfy the Sato–Tate axioms and groups that arise as Sato–Tate groups, and it increases the number of maximal Sato–Tate groups with identity component $\mathrm{U}(1) \times \mathrm{U}(1)$ (two of the maximal subgroups of $F_{a,b,c}$ arise as Sato–Tate groups). A similar phenomenon occurs here, as explained in Remark 4.6 below.

We next consider cases where $G_1^0 = \mathrm{U}(1)$. In such cases, $G_1 \in \{\mathrm{U}(1), N(\mathrm{U}(1))\}$, so for any given G there exists a group G_2 with connected part G_2^0 such that either $G = \mathrm{U}(1) \times G_2$, $G = N(\mathrm{U}(1)) \times G_2$, or G is the fiber product $N(\mathrm{U}(1)) \times_{\mathrm{C}_2} G_2$ with respect to the unique nontrivial homomorphism $N(\mathrm{U}(1)) \rightarrow \mathrm{C}_2$ and some nontrivial homomorphism $G_2 \rightarrow \mathrm{C}_2$. The latter may be characterized by the group G_2 and the index-2 subgroup K which is the kernel of the homomorphism.

- In the case $G^0 = \mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$ (type **F**), take $G_1^0 = \mathrm{U}(1)$ and $G_2^0 = \mathrm{SU}(2) \times \mathrm{SU}(2)$; then $G_2 \in \{\mathrm{SU}(2) \times \mathrm{SU}(2), N(\mathrm{SU}(2) \times \mathrm{SU}(2))\}$ and there is a unique fiber product in the latter case. For this identity component we find 5 extensions, of which one is maximal: $N(\mathrm{U}(1)) \times N(\mathrm{SU}(2) \times \mathrm{SU}(2))$.
- In the case $G^0 = \mathrm{U}(1) \times \mathrm{SU}(2)_2$ (type **J**), G_2 must be taken from the groups with $d = 3$ in [FKRS12, Table 8]. Unique fiber products occur for $G_2 = E_2, E_4, E_6, J(E_1), J(E_3)$. Multiple fiber products occur for $G_2 = J(E_{2n})$ for $n = 1, 2, 3$, as we may take the kernel to be either E_{2n} or one of the two copies of $J(E_n)$. (The latter are conjugate to each other via the normalizer of $J(E_{2n})$, and so give rise to conjugate fiber products.) For this identity component we find 31 extensions, of which two are maximal: $N(\mathrm{U}(1)) \times J(E_4)$ and $N(\mathrm{U}(1)) \times J(E_6)$.
- In the case $G^0 = \mathrm{U}(1) \times \mathrm{U}(1)_2$ (type **L**), we find the maximal extensions $N(\mathrm{U}(1)) \times J(D_6)$ and $N(\mathrm{U}(1)) \times J(O)$. We defer to [FKS] the discussion yielding 122 extensions in this case.

3.3.3. *Triple products.* We next classify the options for G assuming that $G^0 \simeq \mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$ (type **E**). In this case, $N/G^0 \simeq \mathrm{S}_3$; more precisely, N is generated by G^0 plus the permutation matrices. We find four options for G in this case, corresponding to the subgroups of S_3 up to conjugacy, which we may identify with $\mathrm{S}_1, \mathrm{S}_2, \mathrm{A}_3, \mathrm{S}_3$. We obtain a unique maximal extension in this case.

We next classify the options for G assuming that $G^0 \simeq \mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$ (type **H**). In this case, $Z = G^0$ and N/G^0 is isomorphic to the wreath product $\mathrm{C}_2 \wr \mathrm{S}_3$. We find 33 options for G in this case, all contained in a unique maximal extension (we will return to this case in §4.1).

3.3.4. *The diagonal product $\mathrm{SU}(2)_3$.* We next classify the options for G assuming that $G^0 \simeq \mathrm{SU}(2)_3$ (type **M**). In this case, Z equals the group $\mathrm{O}(3)$ realized as a block matrix with scalar entries, $Z \cap G^0 = \{\pm 1\}$, and $N = ZG^0$, so $N/G^0 \simeq \mathrm{SO}(3)$. We first bound the order of a cyclic subgroup of $\mathrm{SO}(3)$ satisfying (ST3). Any cyclic subgroup of $\mathrm{SO}(3)$ of order n is conjugate to

$$\langle A \rangle, \quad A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos 2\pi/n & \sin 2\pi/n \\ 0 & -\sin 2\pi/n & \cos 2\pi/n \end{pmatrix}.$$

By (ST3) the average of the trace of the representation $\wedge^2 \mathbb{C}^6$ on the coset of G^0 containing A , which is given by

$$E[\text{Trace}(\gamma, \wedge^2 \mathbb{C}^6) : \gamma \in AG^0] = |\text{Trace}(A)|^2 = (1 + 2 \cos 2\pi/n)^2,$$

must be an integer; this happens if and only if $n \in \{1, 2, 3, 4, 6\}$. Since every finite subgroup of $\text{SO}(3)$ is either cyclic, dihedral, or one of the three exceptional groups (tetrahedral, octahedral, icosahedral), we obtain component groups isomorphic to

$$C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, A_4, S_4.$$

For this identity component we find 11 extensions, among which two are maximal, namely those with component groups D_6 and S_4 , which we denote by $\text{SU}(2)_3[D_6]$ and $\text{SU}(2)_3[S_4]$.

3.3.5. *The diagonal product* $U(1)_3$. We finally report on the classification for the options for G achieved in [FKS] assuming that $G^0 \simeq U(1)_3$ (type **N**). In this case, $Z = U(3)$ embedded as in §3.1, $G^0 \subset Z$, and $N = Z \cup JZ$, so $N/G^0 \simeq \text{PSU}(3) \rtimes C_2$ for the action of C_2 on $\text{PSU}(3)$ via complex conjugation.

As in the case $G^0 \simeq \text{SU}(2)_3$, if the cyclic subgroup of $\text{PSU}(3)$ generated by $A \in Z$ satisfies (ST3), then $|\text{Trace}(A)|^2$ is an integer (and similarly for every power of A). It will suffice to apply (ST3) in this form, which we denote by (ST3'), as we will show *a posteriori* in §4 that every group we obtain also satisfies (ST3) in full.

We first focus on subgroups of $\text{PSU}(3)$. Since $\text{SU}(3)$ surjects onto $\text{PSU}(3)$ with kernel μ_3 , we may identify finite subgroups of $\text{PSU}(3)$ with finite subgroups of $\text{SU}(3)$ containing μ_3 ; for the latter, we use the classification by Blichfeldt–Dickson–Miller [MBD61, Chapter XII].

LEMMA 3.6. *Every finite subgroup of $\text{SU}(3)$ containing μ_3 is conjugate to a subgroup which is either*

- contained in the diagonal torus,
- contained in $\text{SU}(3) \cap (U(1) \times U(2))$,
- a semidirect product of A_3 acting on a diagonal abelian group,
- a (not necessarily split) extension of S_3 by a diagonal abelian group, or
- one of seven exceptional cases whose images in $\text{PSU}(3)$ have orders 36, 72, 216 (the Hessian group), 60 (the group A_5), 360 (the group A_6), or 168 (the group $\text{PSL}(2, 7)$).

To reduce the classification to a finite problem, we study the abelian case in detail. In what follows, let $D(u, v, w)$ denote the 3×3 diagonal matrix with diagonal entries $e^{2\pi i u}, e^{2\pi i v}, e^{2\pi i w}$.

LEMMA 3.7. *Let H be a finite cyclic subgroup of $\text{SU}(3)$ containing μ_3 and satisfying (ST3'). Then $\#(H/\mu_3)$ divides one of 7, 8, 12.*

PROOF. By conjugating, we may ensure that H is generated by some matrix of the form $D(u, v, w)$ with $u, v, w \in \mathbb{Q}$ and $u + v + w \in \mathbb{Z}$, and the problem is to bound the least common denominator of u, v, w subject to the condition that

$$e^{2\pi i(u-v)} + e^{2\pi i(u-w)} + e^{2\pi i(v-u)} + e^{2\pi i(v-w)} + e^{2\pi i(w-u)} + e^{2\pi i(w-v)} \in \mathbb{Z}.$$

This amounts to finding the cyclotomic points on a certain algebraic curve (i.e., solving a multiplicative Manin–Mumford problem), which can be done by following either Conway–Jones [CJ76] or Beukers–Smyth [BS02]; we defer to [FKS] for further details. \square

REMARK 3.8. By Lemma 3.7, the only primes that can divide the order of a finite subgroup of $\mathrm{PSU}(3)$ satisfying (ST3') are 2, 3, 7; in particular, the exceptional subgroups A_5, A_6 are excluded. We may moreover classify all of the cases in which 7 divides the order as follows.

Up to conjugation, there is a unique copy H_0 of C_7 in $\mathrm{PSU}(3)$ satisfying (ST3'); it is generated by the image of $D(\frac{1}{7}, \frac{2}{7}, \frac{4}{7})$. By Lemma 3.7, H_0 is not contained in any larger abelian group satisfying (ST3'); it is also not contained in any conjugate of $\mathrm{SU}(2)$. By Lemma 3.6 plus a direct verification that $\mathrm{PSL}(2, 7)$ satisfies (ST3'), it follows (after checking that these cases do all work) that up to conjugacy, the finite subgroups of $\mathrm{PSU}(3)$ satisfying (ST3') of order divisible by 7 are

$$H_0, H_0 \rtimes A_3, \mathrm{PSL}(2, 7).$$

Having addressed the subgroups of $\mathrm{PSU}(3)$ of order divisible by 7, we henceforth restrict our attention to finite subgroups of $\mathrm{PSU}(3)$ with 3-smooth order.

REMARK 3.9. Let H be a finite subgroup of $\mathrm{SU}(3)$ of 3-smooth order containing μ_3 and satisfying (ST3'). If H is a diagonal abelian group, then it must be isomorphic to $C_m \times C_n$ for some integers m, n with $\mathrm{lcm}(3, m)$ dividing n . It is straightforward to exhaustively consider all choices of m, n consistent with Lemma 3.7 to identify cases satisfying (ST3'); we find that in all cases, $m \in \{1, 2, 3, 4, 6\}$.

If H is an extension of A_3 by a diagonal abelian group H_0 , then H_0 cannot be cyclic (because no cyclic group of order dividing 8 or 12 has a faithful automorphism of order 3). It must thus have the form $C_m \times C_n$ with $m \in \{2, 3, 4, 6\}$. It is straightforward to identify the cases from the previous paragraph which are stable under A_3 ; each of these cases is in fact stable under S_3 .

REMARK 3.10. Using Lemma 3.7, Remark 3.8, and Remark 3.9, the classification of finite subgroups of $\mathrm{SU}(3)$ containing μ_3 and satisfying (ST3') reduces to the case of a nonabelian subgroup H of $\mathrm{SU}(3) \cap (\mathrm{U}(1) \times \mathrm{U}(2))$. The latter group admits $\mathrm{U}(1) \times \mathrm{SU}(2)$ as a double cover via the map $(u, A) \mapsto (u^2, u^{-1}A)$. For \tilde{H} the preimage of H in this cover, the projection of \tilde{H} to $\mathrm{SU}(2)$ cannot be an abelian group of odd order; it must therefore be the inverse image of a dihedral, tetrahedral, or octahedral subgroup of $\mathrm{SO}(3)$. Meanwhile, the projection of \tilde{H} to $\mathrm{U}(1)$ has order dividing 16 or 24. One may thus obtain a bound on such groups by testing (ST3') for each finite subgroup (up to conjugacy) of each of the subgroups

$$C_{96} \times 2D_{48}, C_{96} \times 2O.$$

We were not able to completely automate this calculation; the classification in [FKS] is human-readable, although we did cross-check several steps by numerical computation.

It remains to classify finite subgroups of $\mathrm{PSU}(3) \rtimes C_2$ not contained in $\mathrm{PSU}(3)$ whose intersection with $\mathrm{PSU}(3)$ equals a fixed group H known to satisfy (ST3'); we call each such subgroup a *double cover* of H . (In general, not all double covers are semidirect products of H by C_2 , but the maximal groups all are.) In most cases, we work with a conjugacy representative of H which is stable under the action $g \mapsto \bar{g}$ of complex conjugation; under this condition, the double covers of H are the groups of the form $\langle H, Jg \rangle$ for some $g \in N_H$ satisfying $\bar{g}g \in H$. The last condition means that the image of g in N_H/H maps to its inverse under complex conjugation; the values in N_H/H corresponding to the same double cover as g are the images of $\bar{h}^{-1}gh$ for all $h \in N_H$.

REMARK 3.11. One complicating feature is that not every double cover of a given H extends to every overgroup. In particular, the intersection of a maximal finite subgroup of $\mathrm{PSU}(3) \rtimes \mathrm{C}_2$ satisfying (ST3') with $\mathrm{PSU}(3)$ need not be a *maximal* finite subgroup of $\mathrm{PSU}(3)$ satisfying (ST3').

THEOREM 3.12. *Up to conjugacy, there are 12 maximal subgroups of $\mathrm{PSU}(3) \rtimes \mathrm{C}_2$ satisfying (ST3'), as listed in Table 2. (See below for explanation of the table entries.)*

The maximal subgroups in Theorem 3.12 are described in Table 2. In each row, M is an imaginary quadratic field of class number 1, \tilde{H} is a subgroup of $\mathrm{GL}_3(M)$, H is the projective image of \tilde{H} , and $H \rtimes \mathrm{C}_2$ is a particular choice of semidirect product (to be discussed in more detail in Lemma 4.10). The notation for \tilde{H} is to be interpreted as follows.

- The labels $G(m, n, p)$ and G_i refer to the Shephard-Todd notation [ST54] for complex reflection groups. In these cases, M is the field of traces of \tilde{H} as per [MM10, Table 1].
- The notation $[G_8 : 4]$ refers to a non-normal index-4 subgroup of $G(1, 1, 1) \times G_8$. It is not a complex reflection group.
- The notation G'_4 refers to a copy of G_4 embedded via its two-dimensional irreducible representation with rational traces (a cubic twist of the reflection representation). That representation has a nontrivial Schur index: it can only be realized over fields that split the quaternion algebra $(-1, -1)_{\mathbb{Q}}$ (compare [FG18, Proposition 3.5]). By convention, we do not regard G'_4 as a complex reflection group.

The action of C_2 on H is induced by an action of C_2 on \tilde{H} specified as follows.

- For $c \in \mathrm{C}_2$ and $c_M \in \mathrm{Gal}(M/\mathbb{Q})$ generators and $\rho : \tilde{H} \rightarrow \mathrm{GL}_3(M)$ the implied representation, we have $\rho \cong c_M \circ \rho \circ c$.
- In the cases where \tilde{H} is written as a product, the action of c respects this decomposition.
- The actions on $G(n, 1, 1)$, $G(4, 4, 3)$, $G(6, 2, 3)$, G_4 , G_8 , G_{12} , G_{24} , G_{25} are all outer, represented by the action of c_M on a c_M -stable presentation [MM10, Theorem 1.7].
- The action on $[G_8 : 4]$ is outer, but this leaves two possibilities for the semidirect product. One of these extends to G_8 ; we take the other one.
- The action on $G(3, 3, 2)$ is trivial.
- The actions on $G(2, 1, 2)$, $G(6, 6, 2)$ are outer.
- The action on G'_4 is outer, but this leaves two possibilities for the semidirect product. One of these recovers $\langle 144, 125 \rangle$; we take the other one.

REMARK 3.13. Since we are only interested in H rather than \tilde{H} , some variation in the choice of complex reflection groups is possible in Table 2. For the most part, we have made choices to minimize $\#\tilde{H}/\#H$.

REMARK 3.14. By choosing explicit presentations of the groups in Table 2, it is possible to verify by computer calculations that the subgroups of these groups account for 171 distinct extensions of $\mathrm{U}(1)_3$, and that there are no containment relations among the groups in the table. The difficult part of the classification, which we defer to [FKS], is to check that every possible extension is accounted for

H	$H \times C_2$	\tilde{H}	$\#\tilde{H}/\#H$	M
$\langle 24, 1 \rangle$	$\langle 48, 15 \rangle$	$G(1, 1, 1) \times [G_8 : 4]$	1	$\mathbb{Q}(i)$
$\langle 24, 10 \rangle$	$\langle 48, 15 \rangle$	$G(3, 1, 1) \times G(2, 1, 2)$	1	$\mathbb{Q}(\zeta_3)$
$\langle 24, 5 \rangle$	$\langle 48, 38 \rangle$	$G(4, 1, 1) \times G(3, 3, 2)$	1	$\mathbb{Q}(i)$
$\langle 24, 5 \rangle$	$\langle 48, 41 \rangle$	$G(4, 1, 1) \times G(6, 6, 2)$	2	$\mathbb{Q}(i)$
$\langle 48, 29 \rangle$	$\langle 96, 193 \rangle$	$G(1, 1, 1) \times G_{12}$	1	$\mathbb{Q}(\sqrt{-2})$
$\langle 72, 25 \rangle$	$\langle 144, 125 \rangle$	$G(3, 1, 1) \times G_4$	1	$\mathbb{Q}(\zeta_3)$
$\langle 72, 25 \rangle$	$\langle 144, 127 \rangle$	$G(3, 1, 1) \times G'_4$	1	$\mathbb{Q}(\zeta_3)$
$\langle 96, 67 \rangle$	$\langle 192, 988 \rangle$	$G(1, 1, 1) \times G_8$	1	$\mathbb{Q}(i)$
$\langle 96, 64 \rangle$	$\langle 192, 956 \rangle$	$G(4, 4, 3)$	1	$\mathbb{Q}(i)$
$\langle 168, 42 \rangle$	$\langle 336, 208 \rangle$	G_{24}	2	$\mathbb{Q}(\sqrt{-7})$
$\langle 216, 92 \rangle$	$\langle 432, 523 \rangle$	$G(6, 2, 3)$	3	$\mathbb{Q}(\zeta_3)$
$\langle 216, 153 \rangle$	$\langle 432, 734 \rangle$	G_{25}	3	$\mathbb{Q}(\zeta_3)$

TABLE 2. Maximal extensions of $U(1)_3$.

in this manner; in other words, that there are no maximal subgroups missing from the table below.

$ST(A)^0$	$\dim ST(A)^0$	Extensions	Maximal
$USp(6)$	21	1	1
$U(3)$	9	2	1
$SU(2) \times USp(4)$	13	1	1
$U(1) \times USp(4)$	11	2	1
$SU(2) \times SU(2) \times SU(2)$	9	4	1
$U(1) \times SU(2) \times SU(2)$	7	5	1
$U(1) \times U(1) \times SU(2)$	5	8	1
$U(1) \times U(1) \times U(1)$	3	33	1
$SU(2) \times SU(2)_2$	6	10	2
$U(1) \times SU(2)_2$	4	31	2
$SU(2) \times U(1)_2$	4	32	2
$U(1) \times U(1)_2$	2	122	2
$SU(2)_3$	3	11	2
$U(1)_3$	1	171	12

TABLE 3. For each connected Sato–Tate group, we list the number of extensions satisfying the Sato–Tate axioms and the number of those which are maximal.

4. Realization

The goal of this section is to provide a proof of the following result, assuming Theorem 3.1.

THEOREM 4.1. *Up to conjugacy, there are 410 closed subgroups of $USp(6)$ that occur as Sato–Tate groups of abelian threefolds over number fields. Among these, the 33 that are maximal with respect to finite index inclusions arise as Sato–Tate groups of abelian threefolds. (Hence by base extension, all 410 groups occur for abelian threefolds over number fields.)*

The proof of the theorem has two parts. On the one hand, when the identity component contains $U(1) \times U(1)$ as a factor, we refine the group-theoretic argument by making a further analysis of CM types that rules out 23 of the groups satisfying the Sato–Tate axioms (§4.1). In particular, the set of maximal groups among those satisfying the refined analysis of CM types differs from the set of maximal groups satisfying the Sato–Tate axioms (see Remark 4.6).

On the other hand, we realize the remaining 410 groups as Sato–Tate groups of certain abelian threefolds (§4.2). Crucially, it will suffice to realize the 33 maximal groups among these, as then their subgroups of finite index can be achieved by considering base extensions (by Lemma 2.8). As an aside, we note that at present we do not know exactly which groups can occur over \mathbb{Q} (certainly not all of them: no connected group with a unique factor isomorphic to $U(1)$ can arise over \mathbb{Q} , since this would require a CM elliptic curve to have all its endomorphisms defined over \mathbb{Q}).

We note in passing that all of the examples of types other than \mathbf{N} will carry a principal polarization. The analysis of polarizations in the type \mathbf{N} case is more subtle, and is not included here.

4.1. Upper bound. Let A be an abelian threefold with $\text{ST}(A) = G$ and suppose that G^0 contains $U(1) \times U(1)$ as a factor.

Suppose first that $G^0 = \text{SU}(2) \times U(1) \times U(1)$. Then A must split up to isogeny as the product of an elliptic curve without CM and an abelian surface whose Sato–Tate group has identity component $U(1) \times U(1)$. By [FKRS12, §4.3, §4.4], of the 8 options for G described in §3.3.2, we may omit the 3 for which G_2 cannot occur for abelian surfaces.

Suppose next that $G^0 = U(1) \times U(1) \times U(1)$ so that N/G^0 is isomorphic to the wreath product $C_2 \wr S_3$. Let a, b, c be representatives of the nontrivial cosets in the three factors of $N(U(1))$, and set t, s correspond to the permutations $(12), (123)$ in S_3 .

If A is not simple, then it splits as a product of a CM elliptic curve and a CM abelian surface; this means that up to conjugacy, $\text{ST}(A)$ is contained in the product of a subgroup of $\langle a, b, t \rangle$ and a subgroup of $\langle c \rangle$. By the analysis from [FKRS12, §4.3], the former must be a subgroup of either $\langle a, b \rangle$ or $\langle at \rangle$.

To handle the case where A is simple, we recall some basic facts about abelian varieties with complex multiplication, following [Dod84, §1] and [Kil16, §1] (and ultimately [Shi71, §5.5]). For future reference, we temporarily allow A to have arbitrary dimension.

DEFINITION 4.2. A *CM field* is a totally imaginary quadratic extension of a totally real number field. A *CM type* is a pair (M, Φ) consisting of a CM field M and a section Φ of the map grouping the complex embeddings of M into conjugate pairs.

Given a CM type (M, Φ) , for any \mathbb{Z} -lattice \mathfrak{m} in M , we may use Φ to specify a complex structure on $M \otimes_{\mathbb{Q}} \mathbb{R}$, and thus view $(M \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{m}$ as a complex torus. Changing the choice of \mathfrak{m} gives rise to an isogenous torus [Shi71, Proposition 5.13]; consequently, we may associate a polarization to this torus using the trace pairing on M , and thus obtain an abelian variety A over \mathbb{C} with complex multiplication by some order in M . Note that if M has degree $2n$, then A has dimension n .

DEFINITION 4.3. Given a CM type (M, Φ) , let L be the Galois closure of M in \mathbb{C} , which is again a CM field. The action of $\text{Gal}(L/\mathbb{Q})$ on the complex embeddings of M by postcomposition acts on the CM types for M . The *reflex field* of (M, Φ) is the fixed field M^* of the stabilizer of Φ in $\text{Gal}(L/\mathbb{Q})$; note that M^* is defined as a subfield of L (and hence of \mathbb{C}), whereas M does not come with a distinguished embedding into L . (There is also a CM type associated to M^* , the *reflex type*, which we will not discuss here.)

LEMMA 4.4. *Fix an embedding of k into \mathbb{C} . Let A be a simple polarized abelian variety of dimension n over k with CM type (M, Φ) .*

- (a) *The field M^* is Galois over $k \cap M^*$.*
- (b) *The field kM^* is the endomorphism field of A .*
- (c) *The group $\text{Gal}(kM^*/k)$ is canonically isomorphic to a subgroup of $\text{Aut}(M/\mathbb{Q})$.*

PROOF. For (a), (b), see [Shi71, Theorem 5.15, Proposition 5.17]. For (c), the action from (b) gives an action of $\text{Gal}(kM^*/k)$ on $\text{End}(A_{\mathbb{C}})_{\mathbb{Q}} = M$. \square

REMARK 4.5. To trace the effect of the previous discussion on Sato–Tate groups, we identify $\text{ST}(A)/\text{ST}(A)^0$ with a subgroup of $C_2 \wr S_n$ using the embedding of M into $\text{End}(A_K)_{\mathbb{R}}$ to fix the identification of $U(1) \times \cdots \times U(1)$ with $\prod_{\tau \in \Phi} \mathbb{C}^{\times}$. Then the subgroup $\text{ST}(A)/\text{ST}(A)^0$ is contained in $\text{Gal}(L/(k \cap M^*))$ and the composition

$$\text{ST}(A)/\text{ST}(A)^0 \rightarrow \text{Gal}(L/(k \cap M^*)) \rightarrow \text{Gal}(M^*/(k \cap M^*)) \cong \text{Gal}(kM^*/k)$$

is the canonical map (see Remark 2.9).

We now specialize back to the case where A is a simple CM abelian threefold. In this case, as per [Dod84, §5.1.1], the sextic field M must be one of the following.

- A cyclic Galois extension of \mathbb{Q} . In this case, we must have $G/G^0 \subseteq \langle abc, s \rangle$ as this is the unique copy of C_6 in $C_2 \wr S_3$.
- A compositum of an imaginary quadratic field M_0 and a non-Galois totally real cubic field M_1 . In this case, $\text{Aut}(M/\mathbb{Q}) = \text{Gal}(M_0/\mathbb{Q})$ and so $G/G^0 \subseteq \langle abc \rangle$.
- A non-Galois extension of \mathbb{Q} whose Galois closure has group $C_2 \wr A_3$ or $C_2 \wr S_3$. In this case, $\text{Aut}(M/\mathbb{Q})$ is trivial, as then is G/G^0 .

To summarize, we list the 33 conjugacy classes of subgroups of N/G^0 (as may be verified using GAP or MAGMA) in Table 4. In the table, \star indicates a normal subgroup, while an underline denotes a group that is permitted by the previous analysis to occur as a Sato–Tate group of an abelian threefold; we will see later that these groups all do occur (see §4.2.3).

REMARK 4.6. The above discussion eliminates, in particular, the groups $\text{SU}(2) \times F_{a,b,c}$ and $N(U(1) \times U(1) \times U(1))$. These are the maximal groups among those satisfying the Sato–Tate axioms for the absolute types \mathbf{G} and \mathbf{H} as seen in §3.3.2 and §3.3.3, respectively. In their place, five groups become maximal among the list of groups satisfying the above refined analysis. The groups $\text{SU}(2) \times F_{a,b}$ and $\text{SU}(2) \times F_{ac}$ become maximal for the absolute type \mathbf{G} , and the groups with groups of connected components $\langle a, b, c \rangle$, $\langle at, c \rangle$, and $\langle abc, s \rangle$ become maximal for the absolute type \mathbf{H} . The refined analysis thus yields 33 maximal groups in total.

Order	Isom type	Groups	Total
1	C_1	$\langle e \rangle$	1
2	C_2	$\langle a \rangle, \langle ab \rangle, \langle abc \rangle \star, \langle t \rangle, \langle ct \rangle$	5
3	C_3	$\langle s \rangle$	1
4	C_4	$\langle at \rangle, \langle act \rangle$	2
4	C_2^2	$\langle a, b \rangle, \langle a, bc \rangle, \langle ab, bc \rangle \star, \langle c, t \rangle, \langle ab, t \rangle, \langle ab, ct \rangle, \langle abc, t \rangle$	7
6	C_6	$\langle abc, s \rangle$	1
6	S_3	$\langle s, t \rangle, \langle abct, s \rangle$	2
8	$C_2 \times C_4$	$\langle c, at \rangle$	1
8	C_2^3	$\langle a, b, c \rangle \star, \langle ab, c, t \rangle$	2
8	D_4	$\langle a, b, t \rangle, \langle ab, bc, t \rangle, \langle a, b, ct \rangle, \langle ab, bc, ct \rangle$	4
12	D_6	$\langle abc, s, t \rangle$	1
12	A_4	$\langle ab, bc, s \rangle \star$	1
16	$C_2 \times D_4$	$\langle a, b, c, t \rangle$	1
24	$C_2 \wr A_3$	$\langle a, b, c, s \rangle \star$	1
24	S_4	$\langle ab, bc, s, t \rangle \star, \langle ab, bc, at, s \rangle \star$	2
48	$C_2 \wr S_3$	$\langle a, b, c, s, t \rangle \star$	1

TABLE 4. Conjugacy classes of subgroups of N/G^0 for $G^0 \simeq U(1) \times U(1) \times U(1)$. The starred groups are normal; the underlined groups can be realized by Sato–Tate groups.

REMARK 4.7. Recall from Remark 3.2 that Theorem 3.1 gives only an upper bound on the set of conjugacy classes of subgroups of $GL_6(\mathbb{C})$ satisfying the Sato–Tate axioms for an abelian threefold. The lower bound is not obtained in this argument because we only verify (ST3) for some choices of the character χ .

However, it can be shown that all 433 conjugacy classes that occur do in fact satisfy (ST3) in full. For the 410 groups that occur in Theorem 4.1, the realizations of these groups as Sato–Tate groups of abelian threefolds will *a posteriori* confirm (ST3). To settle the remaining cases, it suffices to check (ST3) for the full normalizers of $U(1) \times U(1) \times SU(2)$ and $U(1) \times U(1) \times U(1)$ in $USp(6)$. For G equal to one of these groups, we can write G as $G_0 \rtimes K$ where K is a finite subgroup of $USp(6) \cap GL_6(\mathbb{Q})$; this means that (ST3) holds for every χ which is the base extension of a \mathbb{Q} -linear representation of $GL_6(\mathbb{Q})$, and this covers all χ by virtue of the usual description of irreducible representations of $GL_6(\mathbb{C})$ via Schur functors.

4.2. Lower bound. We next exhibit examples of abelian threefolds defined over \mathbb{Q} realizing each of the 33 maximal groups described in Remark 4.6.

4.2.1. *Indecomposable cases.* The unique group of absolute type **A** is realized by any abelian threefold with trivial endomorphism ring, and in particular by the Jacobian of a generic genus-3 curve. For a concrete example of absolute type **A**, by a theorem of Zarhin [Za00, Theorem 2.1], the Jacobian of the hyperelliptic curve $y^2 = x^7 - x + 1$ has trivial endomorphism ring.

The unique maximal group of absolute type **B** is realized by the Jacobian of a generic Picard curve. For a concrete example of absolute type **B**, we take an example of Upton [Upt09, §6.1.3]: the Jacobian of the Picard curve $C : y^3 = x^4 + x + 1$ has maximal 67-adic Galois image. Note that Upton’s result uses a calculation of Frobenius traces plus a big image criterion in the manner of [Vas04]; in general, we do not know of a good way to compute directly with the mod- ℓ

Galois representation for any prime ℓ other than 2, for which the Galois action on bitangents provides a computable model.

4.2.2. *Split products.* Note that the maximal split products are all of the form $G = G_1 \times G_2$, where $G_1 = N(U(1))$ or $SU(2)$, and

$$G_2 = \mathrm{USp}(4), N(\mathrm{SU}(2) \times \mathrm{SU}(2)), F_{ac}, F_{a,b}, J(E_4), J(E_6), J(D_6), \text{ or } J(O).$$

Fix one such G_2 . As shown by [FKRS12, Table 11], there exists a principally polarized abelian surface S defined over \mathbb{Q} with $\mathrm{ST}(S) \simeq G_2$. If $G_1 = \mathrm{SU}(2)$, then G is realized by the product of S with an elliptic curve without CM defined over \mathbb{Q} ; if $G_1 = N(U(1))$, then G is realized by the product of S with an elliptic curve defined over \mathbb{Q} with CM by a quadratic imaginary field not contained in the endomorphism field of S . One readily verifies that examples of elliptic curves satisfying this condition can be easily found.

4.2.3. *Triple products.* The unique maximal group for the absolute type **E** can be realized in the following manner. Let E be an elliptic curve without CM defined over a non Galois cubic extension F/\mathbb{Q} which is not a \mathbb{Q} -curve (that is, there exists $\sigma \in G_{\mathbb{Q}}$ such that E and σE are not $\overline{\mathbb{Q}}$ -isogenous). It immediately follows that if σ and σ' are different embeddings of F into $\overline{\mathbb{Q}}$, then σE and $\sigma' E$ are not $\overline{\mathbb{Q}}$ -isogenous, and therefore the maximal group for the absolute type **E** is realized by taking the Weil restriction of scalars of E from F down to \mathbb{Q} .

We next realize the maximal groups of absolute type **H**:

- The product of three elliptic curves defined over \mathbb{Q} with CM by pairwise non-isomorphic imaginary quadratic fields realizes the maximal group with group of components $\langle a, b, c \rangle$.
- Let S be a principally polarized abelian surface over \mathbb{Q} with CM by a quartic CM field (as the example given in [FKRS12, Table 11] realizing the group F_{ac} , for example). Let E be an elliptic curve defined over \mathbb{Q} with CM by a quadratic imaginary field not contained in the endomorphism field of S . Then $E \times S$ realizes the maximal group with group of components $\langle at, c \rangle$.
- As discussed in §4.1, the maximal group with group of components $\langle abc, s \rangle$ is realized by a principally polarized abelian threefold with CM by a cyclic CM field of degree 6. As a concrete example, we may take the Jacobian of the curve $y^2 = x^7 + 1$, which has CM by the field $\mathbb{Q}(\zeta_7)$.

4.2.4. *The diagonal product $\mathrm{SU}(2)_3$.* We next realize the two maximal groups of absolute type **M**. We will use the construction of Example 2.11, but this does not yield examples carrying a principal polarization; we thus supplement the discussion with some explicit examples that are principally polarized.

In order to realize $\mathrm{SU}(2)_3[\mathrm{S}_4]$, let L/\mathbb{Q} denote a Galois extension with Galois group S_4 and let

$$\xi: \mathrm{Gal}(L/\mathbb{Q}) \rightarrow \mathrm{GL}_3(\mathbb{Z})$$

denote a faithful integral degree 3 representation. Let E be an elliptic curve without complex multiplication defined over \mathbb{Q} and let A be the twist of E^3 by ξ . From the fact that ξ has projective image S_4 , we easily deduce that A has Sato–Tate group $\mathrm{SU}(2)_3[\mathrm{S}_4]$.

Alternatively, note that this group occurs for the Jacobian of a generic twist of the curve $y^2 = x^8 + 14x^4 + 1$, which has an automorphism group of order 48. See for example [ACLLM18, Table 4, row 11].

In order to realize $SU(2)_3[D_6]$, let L/\mathbb{Q} denote a Galois extension with Galois group D_6 and let

$$\xi: \text{Gal}(L/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z})$$

denote a faithful integral degree 2 representation. Let E be an elliptic curve without complex multiplication defined over \mathbb{Q} , set $S = E^2$, and let S_ξ be the twist of S by ξ . Since the projective image of ξ is D_3 , the endomorphism field of S_ξ has Galois group D_3 . Then $SU(2)_3[D_6]$ is realized by the product of S_ξ and a nontrivial quadratic twist E' of E over a quadratic field not contained in the endomorphism field of S .

Alternatively, let C_2 be the curve $y^2 = x^6 + x^3 + 4$, which is given in [FKRS12, Table 11] as an example with Sato-Tate group $J(E_3)$. The curve C_2 is a twist of $y^2 = x^6 + x^3/2 + 1$, whose quotient by the involution

$$(x, y) \mapsto (1/x, y/x^3)$$

may be identified with the curve $C_1 : y^2 = (x+2)(x^3 - 3x + 1/2)$ via the map $(x, y) \mapsto (x+1/x, y(x+1)/x^2)$; taking the product of $\text{Jac}(C_2)$ with a generic quadratic twist of $\text{Jac}(C_1)$ yields an abelian threefold with Sato-Tate group $SU(2)_3[D_6]$.

REMARK 4.8. Note that in both of the constructions realizing $SU(2)_3[D_6]$, we use an abelian surface with Sato-Tate group $J(E_3)$. One may wonder whether it is possible to construct an abelian threefold A defined over \mathbb{Q} with $\text{ST}(A) = SU(2)_3[D_6]$ such that A is the product of an elliptic curve E over \mathbb{Q} and an abelian surface S over \mathbb{Q} with $\text{ST}(S) = J(E_6)$. This seemingly natural construction is ruled out by [FS14, §3D], which shows that an elliptic factor of such an S never admits a model up to isogeny defined over \mathbb{Q} .

4.2.5. *The diagonal product* $U(1)_3$. We finally realize the twelve maximal groups of absolute type \mathbf{N} . We do this in a uniform fashion using the presentations given in Table 2. Hereafter, let H, \tilde{H} correspond to a row of the table.

We first verify that the construction of Example 2.12 is applicable. In the cases where \tilde{H} is written as a product, we apply Remark 2.13 to the two-dimensional factor. Using the results of [Fei03], we see the following.

- For the factors G_{12}, G_8 , the integral representation ρ_0 is uniquely determined by ρ , so point (i) of Remark 2.13 applies.
- For the factor $G(3, 3, 2)$, point (ii) of Remark 2.13 applies.

To handle the remaining factors, take $\alpha = 3$ if $M = \mathbb{Q}(i)$ or $\alpha = 2$ if $M = \mathbb{Q}(\zeta_3)$. In Table 5, we give explicit generators for the image of one choice of ρ_0 , presented so that the reduction modulo α becomes lower triangular. One may check easily that while the reduction modulo α is manifestly reducible, the reduction modulo α^2 admits no invariant vector not divisible by α . We may thus apply [Fei03, Corollary 1.5] to see that there are exactly two choices for ρ_0 , and that these two are exchanged by conjugation by $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$. Consequently, either these two choices are preserved by $\rho_0 \mapsto c_M \circ \rho_0 \circ c$, in which case Example 2.12 applies directly; or they are exchanged and Remark 2.14 applies.

REMARK 4.9. Although it is not necessary for our present discussion, for future reference we resolve the ambiguity in the previous discussion.

Factor	Generators
$[G_8 : 4]$	$\begin{pmatrix} -1-i & -3 \\ i & 1+i \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$
$G(2, 1, 2)$	$\begin{pmatrix} -1 & -2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}$
$G(6, 6, 2)$	$\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix}$
G_4	$\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -2 \\ 0 & \zeta_3 \end{pmatrix}$
G'_4	$\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -\zeta_3 & -2\zeta_3 \\ 0 & \zeta_3^2 \end{pmatrix}$

TABLE 5. Presentations of two-dimensional factors of \tilde{H} .

- For the factors $[G_8 : 4], G(2, 1, 2), G(6, 6, 2)$, we are in a situation similar to point (ii) of Remark 2.13: the choices for ρ_0 are fixed by c_M and exchanged by c , so we must apply Remark 2.14 rather than Example 2.12.
- For the factor G'_4 , we argue as in point (ii) of Remark 2.13. The group $G'_4 \cong \langle 24, 3 \rangle$ has a unique 2-Sylow subgroup

$$P = \left\langle \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -2\zeta_3^3 \\ \zeta_3 & -1 \end{pmatrix} \right\rangle.$$

The two choices of ρ_0 , restricted to P , have reductions modulo 2 which factor through the quotient $C_2 \times C_2$ of P ; by labeling the elements of P and of \mathbb{F}_4 and keeping track of signs of permutations, we see that the reductions are interchanged by c_M .

For the extension by $\text{Gal}(M/\mathbb{Q})$ in question, the 2-Sylow subgroup is $\langle 16, 13 \rangle$. The quotient of this group by the center of P is abelian, so the reductions are preserved by c .

Putting this together, we see that the two choices for ρ_0 must be exchanged by $\rho_0 \mapsto c_M \circ \rho_0 \circ c$, so we must apply Remark 2.14 rather than Example 2.12.

- For the factor G_4 , recall from the explanation of Table 2 that we get the same projective image by taking the factor G'_4 and modifying the action of c ; we may thus reuse the previous analysis. In this case, the 2-Sylow subgroup is $\langle 16, 8 \rangle$. The quotient of this group by the center of P is D_4 , so the reductions are interchanged by c . Consequently, the two choices for ρ_0 are preserved by $\rho_0 \mapsto c_M \circ \rho_0 \circ c$, so we may apply Example 2.12 directly.

In the cases where \tilde{H} is three-dimensional, we again apply the results of [Fei03]. The only case where ρ_0 is not uniquely determined by ρ is $\tilde{H} = G_{25}$, in which case there are two choices for ρ_0 which are reducible modulo $1 - \zeta_3$. However, the two reductions have invariant subspaces of different dimensions, so the map $\rho_0 \mapsto c_M \circ \rho_0 \circ c$ fixes them both and Example 2.12 applies directly.

From the previous analysis, it follows that we can apply the construction of Example 2.12 to obtain an abelian threefold A over \mathbb{Q} with $\text{ST}(A)^0 \simeq \text{U}(1)_3$ and $\text{ST}(A)/\text{ST}(A)^0 \simeq H \rtimes C_2$ provided that we can solve the Galois embedding problem

for the pair $(\tilde{H} \rtimes C_2, \tilde{H})$ and the extension M/\mathbb{Q} . We first give a uniform solution for the complex reflection groups.

LEMMA 4.10. *Consider any row of Table 2 for which \tilde{H} is a complex reflection group (that is, $\tilde{H} \neq G(1, 1, 1) \times [G_8 : 4], G(3, 1, 1) \times G'_4$). Let $V = M^3$ be the representation space on which $\mathrm{GL}_3(M)$ acts.*

- (a) *The invariant ring $R = (\mathrm{Sym} V^\vee)^{\tilde{H}}$ is a polynomial ring in 3 variables over M .*
- (b) *The ring R^c is a polynomial ring in 3 variables over \mathbb{Q} .*

PROOF. To check (a), apply the Chevalley–Shephard–Todd theorem, which is valid for arbitrary complex reflection groups [ST54, §7], [Ben11, Theorem 7.2.1]. We may deduce (b) from (a) by Galois descent. \square

For those rows of Table 2 to which Lemma 4.10 applies, the affine space corresponding to R^c contains a Zariski-dense open subspace every point of which defines a solution of the desired embedding problem.

REMARK 4.11. For the various choices of \tilde{H} subsumed in the previous argument, one can also give more direct solutions of the Galois embedding problem that may be better suited for generating small examples. This is perhaps least obvious when H is the Hessian; in this case, one has (as pointed out by Noam Elkies) an isomorphism $\tilde{H} \cong \mathrm{U}(3, \mathbb{F}_4)$ via which \tilde{H} occurs as the 2-division field of a generic Picard curve over \mathbb{Q} .

To deal with the remaining cases, we give more direct solutions of the Galois embedding problems in question.

- For the case $\tilde{H} = G(1, 1, 1) \times [G_8 : 4]$, we find a Galois extension L of \mathbb{Q} containing $\mathbb{Q}(i)$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong \langle 48, 15 \rangle$, $\mathrm{Gal}(L/\mathbb{Q}(i)) \cong \langle 24, 1 \rangle$. By way of motivation, note that the second row of Table 2 also represents the abstract group $\langle 48, 15 \rangle$ but with a different presentation: in that case, one takes the semidirect product of $C_3 \times D_4$ by C_2 acting by an outer automorphism of each factor. It therefore suffices to take L to be the compositum of two Galois extensions $L_1/\mathbb{Q}, L_2/\mathbb{Q}$ in which L_1/\mathbb{Q} is an S_3 -extension, L_2/\mathbb{Q} is a D_8 -extension containing $\mathbb{Q}(i)$ as the fixed subfield of one copy of D_4 , and the fixed field of the other copy of D_4 coincides with the quadratic subfield of L_1/\mathbb{Q} .

To confirm that this can be achieved, we give an explicit example. The degree-8 number field 8.2.85525504.1 contains $\mathbb{Q}(\sqrt{17})$, its discriminant is -1 times a square, and its Galois group is D_8 ; we may thus take L_2 to be the Galois closure of this field. The degree-3 number field 3.3.2057.1 has discriminant which is 17 times a square and its Galois group is S_3 ; we may thus take L_1 to be the Galois closure of this field.

- For the case $\tilde{H} = G(3, 1, 1) \times G'_4$, we find a Galois extension L of \mathbb{Q} containing $\mathbb{Q}(\zeta_3)$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong \langle 144, 125 \rangle$, $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3)) \cong \langle 72, 25 \rangle$. It suffices to take L to be the compositum of two Galois extensions $L_1/\mathbb{Q}, L_2/\mathbb{Q}$ in which L_1/\mathbb{Q} is an S_3 -extension containing $\mathbb{Q}(\zeta_3)$ and L_2/\mathbb{Q} is an extension containing $\mathbb{Q}(\zeta_3)$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong \langle 48, 33 \rangle$, $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3)) \cong \langle 24, 3 \rangle$.

To confirm that this can be achieved, we give an explicit example. We take $L_1 = \mathbb{Q}(\zeta_3, 2^{1/3})$. To choose L_2 , we consult the Klüners-Malle

database [KM01], which includes the polynomial

$$x^{16} - x^{15} - 2x^{14} + 8x^{13} + 10x^{12} - 19x^{11} - 4x^{10} + 64x^9 + 12x^8 - 94x^7 + 38x^6 + 119x^5 - 64x^4 - 97x^3 + 48x^2 + 11x + 1$$

as an entry for the permutation representation 16T60 (in GAP notation). Using MAGMA, one may confirm that this polynomial is irreducible with Galois group $\langle 48, 33 \rangle$, and that the unique quadratic subfield of the splitting field is $\mathbb{Q}(\zeta_3)$.

References

- [AAC...18] P.B. Allen, F. Calegari, A. Caraiani, T. Gee, D. Helm, B.V. Le Hung, J. Newton, P. Scholze, R. Taylor, and J.A. Thorne, [Potential automorphy over CM fields](#), arXiv:1812.09999v1 (2018).
- [ACLLM18] S. Arora, V. Cantoral-Farfán, A. Landesman, D. Lombardo, and J.S. Morrow, [The twisting Sato-Tate group of the curve \$y^2 = x^8 - 14x^4 + 1\$](#) , *Math. Z.* **290** (2018), 991–1022.
- [BaK15] G. Banaszak and K.S. Kedlaya, [An algebraic Sato-Tate group and Sato-Tate conjecture](#), *Indiana Univ. Math. J.* **64** (2015), 245–274.
- [BaK16] G. Banaszak and K.S. Kedlaya, [Motivic Serre group, algebraic Sato-Tate group and Sato-Tate conjecture](#), in *Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures*, Contemporary Math. 663, Amer. Math. Soc., 2016, 11–44.
- [BLGG11] T. Barnet-Lamb, T. Gee, and D. Geraghty, [The Sato-Tate conjecture for Hilbert modular forms](#), *J. Amer. Math. Soc.* **24** (2011), 411–469.
- [Ben11] D. Benson, *Polynomial Invariants of Finite Groups*, Cambridge Univ. Press, Cambridge, 2011.
- [BS02] F. Beukers and C. Smyth, [Cyclotomic points on curves](#), in *Number theory for the millennium, I (Urbana, IL, 2000)*, A.K. Peters, Natick, 2002, 67–85.
- [CJ76] J.H. Conway and A.J. Jones, [Trigonometric Diophantine equations \(On vanishing sums of roots of unity\)](#), *Acta Arith.* **30** (1976), 229–240.
- [CFS19] Edgar Costa, Francesc Fité, Andrew V. Sutherland, [Arithmetic invariants from Sato-Tate moments](#), *C. R. Math. Acad. Sci. Paris* **357** (2019), 823–826.
- [CMSV19] E. Costa, N. Mascot, J. Sijsling, and J. Voight, [Rigorous computation of the endomorphism ring of a Jacobian](#), *Math. Comp.* **88** (2019), 1303–1339.
- [DM82] P. Deligne and J.S. Milne, *Tannakian Categories*, Lecture Notes in Math. 900, Springer, New York, 1982, 100–228.
- [Dod84] B. Dodson, [The structure of Galois groups of CM-fields](#), *Trans. Amer. Math. Soc.* **283** (1984), 1–32.
- [Fei03] W. Feit, [Some integral representations of complex reflection groups](#), *J. Algebra* **260** (2003), 138–153.
- [FG18] F. Fité and X. Guitart, [Fields of definition of elliptic \$k\$ -curves and the realizability of all genus 2 Sato-Tate groups over a number field](#), *Trans. Amer. Math. Soc.* **370** (2018), 4623–4659.
- [FKRS12] F. Fité, K.S. Kedlaya, V. Rotger, and A.V. Sutherland, [Sato-Tate distributions and Galois endomorphism modules in genus 2](#), *Compos. Math.* **148** (2012), 1390–1442.
- [FKS16] F. Fité, K.S. Kedlaya, and A.V. Sutherland, [Sato-Tate groups of some weight 3 motives](#), in *Frobenius distributions: Lang-Trotter and Sato-Tate conjectures*, Contemp. Math., 663, Amer. Math. Soc., Providence, 2016, 57–101.
- [FKS] F. Fité, K.S. Kedlaya, A.V. Sutherland, [Sato-Tate groups of abelian threefolds](#), preprint.
- [FS14] F. Fité and A.V. Sutherland, [Sato-Tate distributions of twists of \$y^2 = x^5 - x\$ and \$y^2 = x^6 + 1\$](#) , *Algebra Number Theory* **8** (2014), 543–585.
- [GK17] R. Guralnick and K.S. Kedlaya, [Endomorphism fields of abelian varieties](#), *Res. Number Theory* **3**:22 (2017).
- [HLP00] E.W. Howe, F. Leprévost, and B. Poonen, [Large torsion subgroups of split Jacobians of curves of genus two or three](#), *Forum Math.* **12** (2000), 315–364.
- [Kan11] E. Kani, [Products of CM elliptic curves](#), *Collect. Math.* **62** (2011), 297–339.

- [KS08] K.S. Kedlaya and A.V. Sutherland, [Computing L-series of hyperelliptic curves](#), in *Algorithmic Number theory: 8th International Symposium, ANTS-VIII (Banff, Canada, May 2008)*, Lect. Notes Comp. Sci. 5011, Springer, Berlin, 2008, 312–326.
- [KS09] K.S. Kedlaya and A.V. Sutherland, [Hyperelliptic curves, L-polynomials, and random matrices](#), in *Arithmetic, Geometry, Cryptography, and Coding Theory: International Conference, November 5–9, 2007, CIRM, Marseilles, France*, Contemp. Math. 487, Amer. Math. Soc., Providence, 2009, 119–162.
- [Kil16] P. Kılıçer, [The CM class number one problem for curves](#), thesis, Université de Bordeaux, 2016, <https://openaccess.leidenuniv.nl/handle/1887/41145>.
- [KM01] J. Klüners and G. Malle, [A database for field extensions of the rationals](#), *LMS J. Comput. Math.* **4** (2001), 182–196; <http://galoisdb.math.upb.de>.
- [LMFDB] The LMFDB Collaboration, [The L-functions and Modular Forms Database](#), <https://www.lmfdb.org>, 2018 (accessed Oct 2019).
- [Ma11] S. Ma, [Decompositions of an Abelian surface and quadratic forms](#), *Ann. Inst. Fourier* **61** (2011), 717–743.
- [MM10] I. Marin and J. Michel, [Automorphisms of complex reflection groups](#), *Rep. Theory* **14** (2010), 747–788.
- [MBD61] G.A. Miller, H.F. Blichfeldt, and L.E. Dickson, *Theory and Applications of Finite Groups*, Dover, New York, 1961.
- [Mum69] D. Mumford, [A note on Shimura’s paper “Discontinuous subgroups and abelian varieties”](#), *Math. Annalen* **181** (1969) 345–351.
- [Oo87] F. Oort, [Endomorphism algebras of abelian varieties](#), in *Algebraic geometry and commutative algebra*, 469–502 (1988).
- [ST54] G.C. Shephard and J.A. Todd, [Finite unitary reflection groups](#), *Canad. J. Math.* **6** (1954), 274–304.
- [Shi71] G. Shimura, [On the zeta-function of an abelian variety with complex multiplication](#), *Ann. of Math.* **94** (1971), 504–533.
- [SM74] T. Shioda and N. Mitani, [Singular abelian surfaces and binary quadratic forms](#), in *Classification of algebraic varieties and compact complex manifolds*, Lecture Notes in Math. 412, Springer, 1974, 259–287.
- [Sut16] A.V. Sutherland, [Sato–Tate distributions](#), in *Analytic Methods in Arithmetic Geometry: Arizona Winter School, March 12–16, 2016, The University of Arizona, Tucson, AZ*, Contemp. Math. 740, Amer. Math.Soc., Providence 2019, 197–248..
- [Sut18a] A.V. Sutherland, [Fast Jacobian arithmetic for hyperelliptic curves of genus 3](#), in *Thirteenth Algorithmic Number Theory Symposium (ANTS XIII)*, Open Book Series **2** (2019), 425–442.
- [Sut18b] A.V. Sutherland, [A database of nonhyperelliptic genus 3 curves over \$\mathbb{Q}\$](#) , in *Thirteenth Algorithmic Number Theory Symposium (ANTS XIII)*, Open Book Series **2** (2019), 443–459.
- [Upt09] M. Upton, [Galois representations attached to Picard curves](#), *J. Algebra* **322** (2009), 1038–1059.
- [Vas04] A. Vasiu, [Surjectivity criteria for \$p\$ -adic representations, part II](#), *Manuscripta Math.* **114** (2004), 399–422.
- [Za00] Y.G. Zarhin, [Hyperelliptic curves without complex multiplication](#), *Math. Res. Lett.* **7** (2000), 123–132.

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 77 MASSACHUSETTS AVE., CAMBRIDGE, MA 02139, USA
Email address: ffite@mit.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SAN DIEGO, 9500 GILMAN DRIVE #0112, LA JOLLA, CA 92093, USA
Email address: kedlaya@ucsd.edu

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 77 MASSACHUSETTS AVE., CAMBRIDGE, MA 02139, USA
Email address: drew@math.mit.edu