IDENTIFYING CENTRAL ENDOMORPHISMS OF AN ABELIAN VARIETY VIA FROBENIUS ENDOMORPHISMS

EDGAR COSTA*, DAVIDE LOMBARDO, AND JOHN VOIGHT

Abstract. Assuming the Mumford–Tate conjecture, we show that the center of the endomorphism ring of an abelian variety defined over a number field can be recovered from an appropriate intersection of the fields obtained from its Frobenius endomorphisms. We then apply this result to exhibit a practical algorithm to compute this center.

1. Introduction

Let F be a number field with algebraic closure F^{al}. Let A be an abelian variety over F and let $A^{\mathrm{al}} := A \times_F F^{\mathrm{al}}$ be its base change to F^{al}. For a prime $\mathfrak{p}$ of F (i.e., a nonzero prime ideal of its ring of integers), we write $\mathbb{F}_{\mathfrak{p}}$ for its residue field, and when A has good reduction at $\mathfrak{p}$ we let $A_{\mathfrak{p}}$ denote the reduction of A modulo $\mathfrak{p}$.

In this article, we seek to recover the center of the geometric endomorphism algebra of A from the action of the Frobenius endomorphisms on its reductions $A_{\mathfrak{p}}$. Our main result is the following theorem.

Theorem 1.1. *Let A be an abelian variety over a number field F such that A^{al} is isogenous to a power of a simple abelian variety. Let $B := \mathrm{End}(A^{\mathrm{al}}) \otimes \mathbb{Q}$ be the geometric endomorphism algebra of A, let $L := Z(B)$ be its center, and let $m \in \mathbb{Z}_{\geq 1}$ be such that $m^2 = \dim_L B$. Suppose that the Mumford–Tate conjecture (Conjecture 3.2) for A holds. Then the following statements hold.*

(a) *There exists a set S of primes of F of positive density such that for each $\mathfrak{p} \in S$:*
   (i) *A has good reduction at $\mathfrak{p}$, and the reduction $A_{\mathfrak{p}}$ is isogenous (over $\mathbb{F}_p$) to the mth power of a geometrically simple abelian variety over $\mathbb{F}_{\mathfrak{p}}$; and*
   (ii) *The $\mathbb{Q}$-algebra $M(\mathfrak{p}) := Z(\mathrm{End}(A_{\mathfrak{p}}) \otimes \mathbb{Q})$ is a field, generated by the $\mathfrak{p}$-Frobenius endomorphism, and there is an embedding $L = Z(B) \hookrightarrow M(\mathfrak{p})$ of number fields.*

(b) *For any $\mathfrak{q} \in S$, and for all $\mathfrak{p} \in S$ outside of a set of density 0 (depending on $\mathfrak{q}$), if M' is a number field that embeds in $M(\mathfrak{q})$ and in $M(\mathfrak{p})$, then M' embeds in L.*

(Edgar Costa) Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA, ORCiD: 0000-0003-1367-7785

(Davide Lombardo) Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo 5, 56127, Pisa, Italy, ORCiD: 0000-0002-1069-3379

(John Voight) Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA, ORCiD: 0000-0001-7494-8732

E-mail addresses: edgarc@mit.edu, davide.lombardo@unipi.it, jvoight@gmail.com.

Date: May 6, 2021.

*Corresponding author.

Theorem 1.1 relies crucially on work of Zywina [Zyw14]. By an explicit argument, the result was proven for A an abelian surface by Lombardo [Lom19, Theorem 6.10]. This theorem may be thought of as a kind of local-global principle for the center of the endomorphism algebra: roughly speaking, the center of the geometric endomorphism algebra of A is the largest number field that embeds in the center of the geometric endomorphism algebra in a relevant set of reductions over finite fields.

The set S in Theorem 1.1 may be taken as in Definition 3.4. If m and a model for A are given, then there is an effectively computable subset $S' \subseteq S$ with $S \smallsetminus S'$ finite (see Lemma 3.5). The value of m is effectively computable given a model for A (see Lemma 3.6), and in fact it is easy in practice to guess m (see Remark 3.7).

The primary motivation for this theorem is an algorithmic application. A result of Costa–Mascot–Sijsling–Voight [CMSV19, Proposition 7.4.7] gives a conditional way to rigorously certify that a numerical calculation [CMSV19, §2.2] of the endomorphism ring of a Jacobian is correct. This result is conditioned on a hypothesis [CMSV19, Hypothesis 7.4.6] that is directly implied by Theorem 1.1(b). In this way, Theorem 1.1 allows us to determine a sharp upper bound on $\operatorname{rk}\operatorname{End}(A^{\mathrm{al}})$, conditional on the Mumford–Tate conjecture holding for A, and thereby compute $\operatorname{End}(A^{\mathrm{al}})$ in practice whenever the abelian variety A is explicitly given as a Jacobian of a curve over F or, more generally, as an isogeny factor of one (hence in principle all abelian varieties, see e.g. Milne [Mil08, § III-10]).

Going a bit further in this direction, we present here an alternative method to compute the center of the geometric endomorphism algebra of A in Algorithm 5.1, again conditional on the Mumford–Tate conjecture, using the notion of normic polynomials (see Section 2). This algorithm has the advantage of avoiding potentially impractical field intersections suggested by Theorem 1.1(b).

One expects to have correctly identified the center L as in the conclusion of Theorem 1.1 after testing $O([F_A^{\mathrm{conn}} : F]^2)$ pairs of primes $\mathfrak{p}, \mathfrak{q}$, where F_A^{conn} is the smallest extension of F for which all the ℓ-adic monodromy groups associated to A are connected—but Algorithm 5.1 does not compute the field F_A^{conn} directly. In particular, we prove the correctness of Algorithm 5.1 without establishing if the density zero set of primes in Theorem 1.1(b) can be computed effectively. Finally, even without assuming the Mumford–Tate conjecture for A, Algorithm 5.1 still yields an *upper bound* on the center of the geometric endomorphism algebra of A—we just have no guarantee that this upper bound is sharp.

We conclude with a result refining Theorem 1.1 to obtain another arithmetically interesting field attached to A, namely the splitting field of the Mumford–Tate group (see Section 3 for a precise definition). Keeping notation as in Theorem 1.1, for $\mathfrak{p} \in S$ let $N(\mathfrak{p})$ be a normal closure of the extension $M(\mathfrak{p}) \supseteq \mathbb{Q}$ generated by the $\mathfrak{p}$-Frobenius endomorphism.

Theorem 1.2. *Let A be an abelian variety over a number field F such that A^{al} is isogenous to a power of a simple abelian variety, and suppose that the Mumford–Tate conjecture for A holds. Let $F_{\mathbf{G}_A}$ be the splitting field of the Mumford–Tate group $\mathbf{G}_A$ of A. Then the following statements hold.*

(a) *There exists a subset $S_{MT} \subseteq S$, of the same density as S, such that for each $\mathfrak{p} \in S_{MT}$, conditions* (i)–(ii) *of Theorem* 1.1(a) *hold and moreover:*
(iii) *There is an embedding $F_{\mathbf{G}_A} \hookrightarrow N(\mathfrak{p})$.*

(b) *For any $\mathfrak{q} \in S_{MT}$, and for all $\mathfrak{p} \in S_{MT}$ outside of a set of density 0 (depending on $\mathfrak{q}$), we have $N(\mathfrak{q}) \cap N(\mathfrak{p}) \simeq F_{\mathbf{G}_A}$.*

In Theorem 1.2, the intersection $N(\mathfrak{q}) \cap N(\mathfrak{p})$ is well-defined up to isomorphism since both fields are normal extensions of $\mathbb{Q}$, and so this intersection can be computed without resorting to normic polynomials.

For further work in this direction, see also the recent paper of Zywina [Zyw20], giving an algorithmic approach to the computation of the Mumford–Tate group itself up to inner twist using the data of Frobenius polynomials.

Organization. This article is organized as follows. In section 2 we set up some basic Galois theory. Then in section 3 we review what is needed from work of Zywina [Zyw14] and Costa–Mascot–Sijsling–Voight [CMSV19] and prove Theorem 1.1. Then in section 4 we prove Theorem 1.2. We conclude in section 5 with an algorithmic application (Algorithm 5.1).

Acknowledgements. The authors would like to thank Andrea Maffei for an enlightening discussion about the Steiner section for reductive groups, the anonymous referees for their critical feedback, Claus Fieker, Mark van Hoeij, Tommy Hofmann, and Jeroen Sijsling for pointers, and David Zywina for helpful guiding discussions. Costa was supported by a Simons Collaboration Grant (550033). Voight was supported by an NSF CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029).

2. Galois theory

In this section, we relate field embeddings to normic factors of a minimal polynomial using some basic Galois theory: see also Klüners [Klü99], van Heoij–Klüners–Novocin [vHKN13, Definition 5], and Szutkoski–van Hoeij [SvH17, Theorem 4]. Throughout this section, let K be a field with separable closure K^{sep}. For a field homomorphism $v\colon K \hookrightarrow L$ and a polynomial $f(T) = \sum_i a_i T^i \in K[T]$, we define

$$(vf)(T) := \textstyle\sum_i v(a_i) T^i \in L[T]$$

to be the polynomial obtained by applying v to the coefficients of f.

Definition 2.1. Let $L \supseteq K$ be a separable field extension of finite degree. For a polynomial $f(T) \in L[T]$, define the norm from L to K of $f(T)$ to be

$$\mathrm{Nm}_{L|K}(f(T)) := \prod_{v : L \hookrightarrow K^{\mathrm{sep}}} (vf)(T),$$

where the product runs over the $[L : K]$ distinct K-embeddings $L \hookrightarrow K^{\mathrm{sep}}$.

Since $\mathrm{Gal}(K^{\mathrm{sep}} \,|\, K)$ permutes the embeddings $L \hookrightarrow K^{\mathrm{sep}}$, by Galois theory we have $\mathrm{Nm}_{L|K}(f(T)) \in K[T]$. Accordingly, we may also define the norm as the product over the embeddings $L \hookrightarrow N$ for any Galois extension $N \supseteq K$ that has at least one such embedding.

Example 2.2. If $f(T) \in K[T]$ is monic, irreducible, and separable, and $L = K(a)$ is the field obtained by adjoining a root a of $f(T)$, then $\mathrm{Nm}_{L|K}(T - a) = f(T)$.

Proposition 2.3. *Let $g(T) \in K[T]$ be monic, irreducible, and separable, and let $a \in K^{\mathrm{sep}}$ be a root of $g(T)$. Let $L \supseteq K$ be a finite separable extension and let $h(T) \in L[T]$ be monic. Then the following conditions are equivalent:*

(i) $g(T) = \mathrm{Nm}_{L|K}\, h(T)$;
(ii) *There exists a K-embedding $\sigma\colon L \hookrightarrow K(a)$ such that $(\sigma h)(T)$ is the minimal polynomial of a over $\sigma(L)$; and*

(iii) $h(T)$ *is an irreducible factor of* $g(T)$ *in* $L[T]$ *and* $\deg g(T) = [L : K] \deg h(T)$.

Moreover, if $h(T)$ *satisfies these equivalent conditions, then* L *is generated over* K *by the coefficients of* $h(T)$.

Proof. Throughout, let N be a splitting field of $g(T)$ over K.

We start with (i) $\Rightarrow$ (ii). Suppose that $g(T) = \mathrm{Nm}_{L|K} h(T)$ with $h(T) \in L[T]$. We first claim that $h(T)$ is irreducible in $L[T]$: if $d(T) \mid h(T)$ with $d(T) \in L[T]$ monic of positive degree, then $\mathrm{Nm}_{L|K} d(T) \mid \mathrm{Nm}_{L|K} h(T) = g(T)$ with $\mathrm{Nm}_{L|K} d(T) \in K[T]$; but $g(T)$ is irreducible in $K[T]$, so equality holds; and then by comparison of degrees we conclude that $d(T) = h(T)$. Next, let $\{\sigma_i\}_i = \mathrm{Hom}_K(L, N)$. Since $g(a) = 0$ and $g(T) = \prod_i (\sigma_i h)(T)$, there exists i such that $(T - a) \mid (\sigma_i h)(T)$. Since $h(T)$ is irreducible in L, we conclude $h'(T) := (\sigma_i h)(T)$ is irreducible in $L' := \sigma_i(L)$ and so $h'(T)$ is the minimal polynomial of a over L'. Thus

$$\begin{aligned}[K(a) : K] &= \deg g(T) = \deg h(T)[L : K] = \deg h'(T)[L' : K] \\ &= [L'(a) : L'][L' : K] = [L'(a) : K];\end{aligned} \tag{2.4}$$

since $L'(a) \supseteq K(a)$, by (2.4) we have $L'(a) = K(a)$ so $L' \subseteq K(a)$, and we may take $\sigma = \sigma_i$ in (ii).

We now prove (ii) $\Rightarrow$ (iii). Since $g(T)$ is the minimal polynomial of a over K and $(\sigma h)(T)$ is the minimal polynomial of a over $\sigma(L)$ we have $(\sigma h)(T) \mid g(T)$ in $\sigma(L)[T]$ so $h(T) \mid g(T)$ since σ is a K-embedding. Moreover,

$$[K(a) : K] = \deg g(T) = \deg(\sigma h)(T)[\sigma(L) : K] = \deg h(T)[L : K]. \tag{2.5}$$

To conclude, we show (iii) $\Rightarrow$ (i). We are given $h(T) \mid g(T)$, so every root of $h(T)$ is a root of $g(T)$. The field N contains all roots of $g(T)$ hence all roots of $h(T)$. Let $b \in N$ be a root of $h(T)$, hence also of $g(T)$; since $g(T) \in K[T]$ is irreducible we conclude $g(T)$ is the minimal polynomial of b over K. Let $n(T) := \mathrm{Nm}_{L|K} h(T) \in K[T]$. Then $n(b) = 0$, so $g(T) \mid n(T)$. But $\deg n(T) = [L : K] \deg h(T) = \deg g(T)$, so $g(T) = n(T)$ since both are monic.

For the final statement, we may suppose (ii) holds and identify L with its image in $K(a)$ under σ. Let $L' \subseteq L$ be the subfield of L generated by the coefficients of $h(T)$; then $[K(a) : L'] = [K(a) : L] = \deg h(T)$ since $h(T)$ is irreducible, so $L' = L$. □

Definition 2.6. Let $M \supseteq K$ be a finite separable extension, and let $g(T) \in K[T]$ be monic. We say a polynomial $h(T) \in M[T]$ is normic for $g(T) \in K[T]$ over M if all of the following conditions hold:

(i) $h(T)$ is monic;
(ii) $h(T) \mid g(T)$; and
(iii) $g(T) = \mathrm{Nm}_{L|K} h(T)$, where $L \subseteq M$ is generated over K by the coefficients of $h(T)$.

Example 2.7. If $h_1(T)$ is normic for $g(T)$ over M, with $L_1 \subseteq M$ the subfield generated by the coefficients of $h_1(T)$, and $K \subseteq L_2 \subseteq L_1$, then $h_2(T) := \mathrm{Nm}_{L_1|L_2} h_1(T)$ is also normic for $g(T)$ over M.

Remark 2.8. If $h(T)$ is normic for $g(T)$ over $M = K(a)$ and further $(T - a) \mid h(T)$, then van Heoij–Klüners–Novocin call $h(T)$ the subfield polynomial of L [vHKN13, Definition 5]; they state a version of Proposition 2.3 in their setting [vHKN13, Remark 6]. More recently, Szutkoski–van Hoeij [SvH17, Theorem 4] have developed further equivalent conditions for

subfield polynomials. We will soon find ourselves in a situation that would be a very simple case of these algorithms, so we will not need to employ these more advanced techniques.

We apply the previous bit of Galois theory as follows.

Proposition 2.9. *Let $g(T) \in K[T]$ be monic, irreducible, and separable. Let $M \supseteq K$ be a finite separable extension. Then the following statements hold.*

(a) *The set of normic polynomials for $g(T)$ over M is a nonempty, partially ordered set under divisibility.*
(b) *Let $h_1(T) \mid h_2(T)$ be normic polynomials for $g(T)$ over M, and let $L_1, L_2 \subseteq M$ be the subfields generated over K by the coefficients of $h_1(T), h_2(T)$, respectively. Then $L_2 \subseteq L_1$.*

Proof. For part (a), the set is nonempty by taking $h(T) = g(T)$ (and $L = K$), and divisibility clearly gives a partial ordering.

Now part (b). Let N be a splitting field for $g(T)$ over K, let $G := \mathrm{Gal}(N \mid K)$ and $H_i := \mathrm{Gal}(N \mid L_i)$ for $i = 1, 2$. Let $\sigma \in H_1 \backslash H_2$. Since $h_2(T)$ is normic for $g(T)$ and $g(T)$ is separable, $(\sigma h_2)(T)$ is coprime to $h_2(T)$. But since $\sigma \in H_1$, we have

$$h_1(T) = (\sigma h_1)(T) \mid (\sigma h_2)(T),$$

a contradiction. So $H_1 \subseteq H_2$ and by the Galois correspondence $L_2 \subseteq L_1$. □

Remark 2.10. Proposition 2.9(a) does not assure the existence of an irreducible normic factor over M. For example, let $g(T) \in \mathbb{Q}[T]$ have degree 4 and Galois group $\mathrm{Gal}(g(T)) = S_4$. Let N be the splitting field of $g(T)$ over $\mathbb{Q}$ and let M be the subfield of N of degree 6 fixed by the subgroup $H = \langle (1\,2), (3\,4) \rangle < S_4$. The polynomial $g(T)$ factors over $M[T]$ as a product of two irreducible degree-2 polynomials. By Proposition 2.3(iii), we conclude that neither factor can be normic, as M does not have an intermediate field of degree 2. Indeed, the field generated by the coefficients of either factor is M itself.

Remark 2.11. In Proposition 2.9(b), the converse need not hold. For example, suppose that $M := K(a) \supseteq K$ is Galois, where $a \in K^{\mathrm{sep}}$ is a root of $g(T)$. Then $g(T)$ splits in M and any linear factor generates M.

3. Splitting of reductions of abelian varieties

In this section, we set up some notation and describe some results from Zywina [Zyw14] concerning splitting of reductions of abelian varieties. See also Costa–Mascot–Sijsling–Voight [CMSV19] for a summary in an algorithmic context.

We begin with a bit of notation. Let F be a number field with algebraic closure F^{al} and let $\mathrm{Gal}_F := \mathrm{Gal}(F^{\mathrm{al}} \mid F)$. Let A be an abelian variety over F of dimension g and let $A^{\mathrm{al}} := A \times_F F^{\mathrm{al}}$ denote the base change of A to F^{al}. Suppose that A^{al} is isogenous to a power of a simple abelian variety (over F^{al}—ultimately, in algorithmic applications we will reduce to this case [CMSV19, Remark 7.4.10]). We write $\mathrm{End}(A)$ for the ring of endomorphisms of A defined over F and $\mathrm{End}(A)_{\mathbb{Q}} := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$; if $K \supseteq F$ is an extension, we will write $\mathrm{End}(A_K)$ for the ring of endomorphisms defined over K. Let $B := \mathrm{End}(A^{\mathrm{al}})_{\mathbb{Q}}$ be the geometric endomorphism algebra of A, and let $L := Z(B)$ be the center of B. Then L is a number field and B is a central simple algebra over L. Let $m^2 := \dim_L B$ with $m \in \mathbb{Z}_{\geq 1}$, so that $\dim_{\mathbb{Q}} B = m^2[L : \mathbb{Q}]$.

For a prime $\mathfrak{p}$ of F, write $\mathbb{F}_\mathfrak{p}$ for its residue field and $q := \#\mathbb{F}_\mathfrak{p}$, let $\mathbb{F}_\mathfrak{p}^{\mathrm{al}}$ be the algebraic closure of $\mathbb{F}_\mathfrak{p}$, and let $\mathrm{Frob}_\mathfrak{p}$ be the Frobenius automorphism of $\mathbb{F}_\mathfrak{p}^{\mathrm{al}}$ fixing $\mathbb{F}_\mathfrak{p}$. For $\mathfrak{p}$ a prime of good reduction for A, write $A_\mathfrak{p}$ for the reduction of A over the residue field $\mathbb{F}_\mathfrak{p}$ and $A_\mathfrak{p}^{\mathrm{al}}$ for the base change of $A_\mathfrak{p}$ to $\mathbb{F}_\mathfrak{p}^{\mathrm{al}}$.

Let ℓ be a prime number. Let $T_\ell A$ be the ℓ-adic Tate module of A, a free $\mathbb{Z}_\ell$-module of rank $2g$. Let $V_\ell A := T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$; then there is a continuous homomorphism

$$\rho_{A,\ell} \colon \mathrm{Gal}_F \to \mathrm{GL}(V_\ell(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

For a prime $\mathfrak{p}$ of good reduction of A that is coprime to ℓ, let

$$c_\mathfrak{p}(T) := \det(1 - \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})T) \in 1 + T\mathbb{Z}[T] \tag{3.1}$$

be the inverse characteristic polynomial of the Frobenius $\mathrm{Frob}_\mathfrak{p}$. Then $c_\mathfrak{p}(T)$ is independent of ℓ. Indeed, $c_\mathfrak{p}(T)$ is the factor of the zeta function of $A_\mathfrak{p}$ whose reciprocal roots have complex absolute value $\sqrt{q}$. Thereby, $c_\mathfrak{p}(T)$ can be recovered from the point counts $\#A(\mathbb{F}_{q^r})$ for $r = 1, \dots, \max(2g, 18)$ [Ked06, §8]; when $A \sim \mathrm{Jac}(C)$ is isogenous to the Jacobian of a curve C, one can also recover $c_\mathfrak{p}(T)$ from $\#C(\mathbb{F}_{q^r})$ for $r = 1, \dots, g$.

Let $\mathbf{GL}(V_\ell(A))$ be the $\mathbb{Q}_\ell$-algebraic group of ($\mathbb{Q}_\ell$-linear) automorphisms of $V_\ell(A)$. The absolute Galois group Gal_F acts by linear automorphisms on $V_\ell(A)$, hence we have $\rho_{A,\ell}(\mathrm{Gal}_F) \leq \mathrm{GL}(V_\ell(A)) = \mathbf{GL}(V_\ell(A))(\mathbb{Q}_\ell)$. Let $\mathbf{G}_{A,\ell}$ be the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_F)$ in $\mathbf{GL}(V_\ell(A))$. Then $\mathbf{G}_{A,\ell} \leq \mathbf{GL}(V_\ell(A))$ is an algebraic subgroup called the ℓ-adic monodromy group of A. Let $\mathbf{G}_{A,\ell}^0$ be the identity component of $\mathbf{G}_{A,\ell}$. Let F_A^{conn} be the fixed field in F^{al} of $\rho_{A,\ell}^{-1}(\mathbf{G}_{A,\ell}^0(\mathbb{Q}_\ell))$. Then F_A^{conn} is a finite Galois extension of F, independent of ℓ by a result of Serre [Ser13, p. 17]. The field F_A^{conn} is the smallest extension of F for which the ℓ-adic monodromy groups are connected for all primes ℓ.

Choose an embedding $F \hookrightarrow \mathbb{C}$. Let $V := H_1(A(\mathbb{C}), \mathbb{Q})$; then $V_\mathbb{C} := V \otimes \mathbb{C}$ has a Hodge decomposition of type $\{(-1,0),(0,-1)\}$. Let $\mu : \mathbf{G}_{m,\mathbb{C}} \to \mathbf{GL}(V_\mathbb{C})$ be the cocharacter such that $\mu(z)$ acts as multiplication by z on $V^{-1,0}$ and as the identity of $V^{0,-1}$ for all $z \in \mathbb{C}^\times = \mathbf{G}_{m,\mathbb{C}}(\mathbb{C})$. The Mumford–Tate group of $A_\mathbb{C}$, denoted $\mathbf{G}_A$, is the smallest algebraic subgroup of $\mathbf{GL}(V)$ defined over $\mathbb{Q}$ such that $\mathbf{G}_A(\mathbb{C})$ contains $\mu(\mathbb{C}^\times)$; then $\mathbf{G}_A$ is a reductive group over $\mathbb{Q}$ that is independent of the choice of embedding of F into $\mathbb{C}$.

Conjecture 3.2 (Mumford–Tate)**.** *The comparison isomorphism $V \otimes \mathbb{Q}_\ell \xrightarrow{\sim} V_\ell(A)$ identifies $\mathbf{G}_A \times_\mathbb{Q} \mathbb{Q}_\ell$ with $\mathbf{G}_{A,\ell}^0$.*

Let $\mathbf{T} \subset \mathbf{G}_A$ be a maximal torus and $X(\mathbf{T})$ be its character group. We write $\operatorname{rk} \mathbf{G}_A$ for the rank of $\mathbf{G}_A$ (i.e., the dimension of $\mathbf{T}$). The absolute Weyl group of $\mathbf{G}_A$ with respect to $\mathbf{T}$ is the (finite) group

$$W(\mathbf{G}_A, \mathbf{T}) := N_{\mathbf{G}_A}(\mathbf{T})(\mathbb{C})/\mathbf{T}(\mathbb{C}),$$

where $N_{\mathbf{G}_A}(\mathbf{T})$ is the normalizer of $\mathbf{T}$ in $\mathbf{G}_A$. For an element $g \in N_{\mathbf{G}_A}(\mathbf{T})(\mathbb{C})$, the map $\mathbf{T}_\mathbb{C} \to \mathbf{T}_\mathbb{C}$ given by $t \mapsto gtg^{-1}$ is an isomorphism of groups that depends only on the image of g in $W(\mathbf{G}_A, \mathbf{T})$; this induces a faithful action of $W(\mathbf{G}_A, \mathbf{T})$ on $\mathbf{T}_\mathbb{C}$, so that we can identify $W(\mathbf{G}_A, \mathbf{T})$ with a subgroup of $\mathrm{Aut}(\mathbf{T}_\mathbb{C})$ and hence also of $\mathrm{Aut}(X(\mathbf{T}))$.

Any element $t \in \mathbf{T}(\mathbb{C}) \leq \mathbf{G}_A(\mathbb{C})$ acts on $V_\mathbb{C}$, and $\det(T - t) = \prod_{\alpha \in \Omega}(T - \alpha(t))^{m_\alpha}$, where $\Omega \subset X(\mathbf{T})$ is the set of weights of $\mathbf{T}$ appearing in the representation $\mathbf{G}_A \to \mathrm{GL}(V_\mathbb{C})$ and the m_α are the corresponding multiplicities. As $W(\mathbf{G}_A, \mathbf{T})$ acts on $X(\mathbf{T})$ stabilizing Ω, in

particular we obtain an action of $W(\mathbf{G}_A, \mathbf{T})$ on Ω, hence on the roots of the characteristic polynomial of t.

We also recall the definition of the splitting field of $\mathbf{G}_A$.

Definition 3.3. The splitting field of $\mathbf{G}_A$, denoted $F_{\mathbf{G}_A}$, is the intersection of all fields $K \subseteq \mathbb{Q}^{\mathrm{al}}$ such that $\mathbf{G}_A \times_{\mathbb{Q}} K$ is split as a reductive group.

The field $F_{\mathbf{G}_A}$ is a finite Galois extension of $\mathbb{Q}$. With this notation in hand, we now introduce our set of primes.

Definition 3.4. Let S be the set of primes $\mathfrak{p}$ of F with the following properties:

(i) The prime $\mathfrak{p}$ is a prime of good reduction for A;
(ii) $\mathrm{Nm}(\mathfrak{p})$ is prime, i.e., the residue field $\#\mathbb{F}_{\mathfrak{p}}$ has prime cardinality;
(iii) $\mathrm{End}(A_{\mathfrak{p}}^{\mathrm{al}})$ is defined over $\mathbb{F}_{\mathfrak{p}}$;
(iv) We have an isogeny $A_{\mathfrak{p}} \sim Y_{\mathfrak{p}}^m$ over $\mathbb{F}_{\mathfrak{p}}$, with $Y_{\mathfrak{p}}$ simple; and
(v) The algebra $\mathrm{End}(Y_{\mathfrak{p}})_{\mathbb{Q}}$ is a field, generated by the Frobenius endomorphism.

Let S_{MT} be the set of primes $\mathfrak{p}$ satisfying (i)–(v) and

(vi) The roots of $c_{\mathfrak{p}}(T)$ (defined in (3.1)) generate a free subgroup $\Phi_{\mathfrak{p}} \leq (\mathbb{Q}^{\mathrm{al}})^\times$ of rank equal to $\mathrm{rk}\,\mathbf{G}_A$.

We have $S_{MT} \subseteq S$. Given a model for A (provided by equations in projective space), we consider the property:

(i′) The prime $\mathfrak{p}$ is a prime of good reduction for the model of A.

Let S' be the set of primes satisfying (i′) and (ii)–(v) in Definition 3.4. The sets S and S' differ in only finitely many primes. We define S'_{MT} similarly, satisfying (i′) and (ii)–(vi).

Lemma 3.5. *Given m and a model for A, the set S' is effectively computable. If $\mathrm{rk}\,\mathbf{G}_A$ is also given, then S'_{MT} is effectively computable.*

Proof. Condition (i′) can be checked by ensuring the model is smooth. We can check (ii) using standard algorithms, and we let $p := \#\mathbb{F}_{\mathfrak{p}}$. For such $\mathfrak{p}$, we compute $c_{\mathfrak{p}}(T)$ using a model of A by counting $\#A(\mathbb{F}_{\mathfrak{p}^r})$ as above. (A finite list of primes containing those of bad reduction and the ability to compute $c_{\mathfrak{p}}(T)$ for each good prime $\mathfrak{p}$ are all we need from a model.) We can check conditions (iii), (iv), and (v) as follows.

For properties (iii)–(iv), we refer to Costa–Mascot–Sijsling–Voight [CMSV19, Lemma 7.2.7] and Zywina [Zyw14, Lemma 2.1] for details; we indicate only the key points here. To verify (iii) we use the (proven) Tate conjecture: letting $c_{\mathfrak{p}}^{\otimes 2}(T)$ be the characteristic polynomial of $\rho_{A,\ell}^{\otimes 2}(\mathrm{Frob}_{\mathfrak{p}})$, we verify that the only reciprocal roots of $c_{\mathfrak{p}}^{\otimes 2}$ of the form $p\zeta$ with ζ a root of unity in fact have $\zeta = 1$. For (iv), we recall from Honda–Tate theory that an abelian variety over a prime finite field whose characteristic polynomial of Frobenius has no real roots is simple if and only if this polynomial is irreducible if and only if its endomorphism algebra is a field, generated by the Frobenius endomorphism. With (iii) established, it follows that $c_{\mathfrak{p}}(T)$ has no real roots: indeed, otherwise it would be divisible by $1 - pT^2$, but then $-p = (-\sqrt{p})(\sqrt{p})$ would be a root of $c_{\mathfrak{p}}^{\otimes 2}(T)$. We then verify (iv) and (v) by checking that $c_{\mathfrak{p}}(T) \in \mathbb{Q}[T]$ is the mth power of an irreducible polynomial (in $\mathbb{Q}[T]$) — this is where we use m.

To conclude, we claim that condition (vi) can be checked effectively if $\mathrm{rk}\,\mathbf{G}_A$ is known. Let N be a splitting field for $c_{\mathfrak{p}}$; then the reciprocal roots of $c_{\mathfrak{p}}$ are algebraic integers that are

p-units in N, i.e., their valuation at any prime that does not lie above p is 0. The unit group $\mathbb{Z}_N[1/p]^\times$ is a finitely generated abelian group. Moreover, there is an effectively computable isomorphism from the set of elements of N that belong to $\mathbb{Z}_N[1/p]^\times$ to an abstract finitely generated abelian group defined by a minimal set of generators and relations (see e.g. Cohen [Coh00, §7.4]). We then apply this isomorphism to the reciprocal roots of $c_{\mathfrak{p}}(T)$, and by linear algebra over $\mathbb{Z}$ (Smith normal form) we compute a minimal presentation for the subgroup they generate and thereby check if this subgroup is free of the correct rank. □

Lemma 3.6. *Suppose that the Mumford-Tate conjecture holds for A. Then given a model for A, the rank $\operatorname{rk} \mathbf{G}_A$ of the Mumford–Tate group and m are effectively computable.*

Proof. The algorithm runs using a day-and-night strategy.

By day, we pick up from Lemma 3.5. In showing that S'_{MT} is effectively computable, we showed that $\operatorname{rk} \Phi_{\mathfrak{p}}$ is effectively computable for $\mathfrak{p} \in S'_{MT}$; then necessarily $\operatorname{rk} \Phi_{\mathfrak{p}} \leq \operatorname{rk} \mathbf{G}_A$. On the assumption of the Mumford–Tate conjecture for A, this lower bound is sharp for a set of primes $\mathfrak{p}$ of positive density [Zyw14, Proposition 2.4]. In a similar way, we may obtain an upper bound for m: we have $m \leq m_{\mathfrak{p}}$ for $\mathfrak{p} \in S'$ if $c_{\mathfrak{p}}(T)$ is an $m_{\mathfrak{p}}$th power of an irreducible element of $\mathbb{Q}[T]$. On Mumford–Tate, this upper bound is sharp for a set of primes $\mathfrak{p}$ of positive density [Zyw14, Theorem 1.2]. (Again, we only need access to the polynomials $c_{\mathfrak{p}}(T)$ for these bounds, not the model.)

By night, we complement these bounds by a (hopelessly slow) search for nontrivial algebraic cycles in powers of A. Since every algebraic cycle is an eigenvector for the action of the Mumford–Tate group on homology (see for example Deligne [DMOS82, Article I, Proposition 3.4] or van Geemen [vG00, Theorem 3.5]), this gives an (eventually sharp) upper bound on the rank of $\mathbf{G}_A$. Similarly, one can also search for endomorphisms of A again represented as algebraic cycles, which eventually gives a sharp lower bound for m. The algorithm halts when the lower and upper bounds for $\operatorname{rk} \mathbf{G}_A$ and m meet, which will happen eventually (under the hypothesis of the Mumford–Tate conjecture). □

Remark 3.7. The upper bound for m in Lemma 3.6 only needs the characteristic polynomial $c_{\mathfrak{p}}(T)$ of Frobenius for primes $\mathfrak{p} \in S'$; this upper bound is unconditional. The upper bound is tight if the Mumford–Tate conjecture holds for A, and then in practice one can quickly guess m.

We now record two important properties about primes in S, S_{MT}.

Proposition 3.8. *The following statements hold.*

(a) *For all $\mathfrak{p} \in S$, there exists a unique monic irreducible $g_{\mathfrak{p}}(T) \in \mathbb{Q}[T]$ such that*

$$c_{\mathfrak{p}}(T) = g_{\mathfrak{p}}(T)^m.$$

(b) *Let $\mathfrak{p} \in S$ and let $M := \mathbb{Q}[T]/(g_{\mathfrak{p}}(T))$. Then there exists an embedding $L \hookrightarrow M$.*

(c) *For all primes $\mathfrak{p} \in S$, there exists an irreducible $h_{\mathfrak{p}}(T) \in L[T]$ such that*

$$g_{\mathfrak{p}}(T) = \operatorname{Nm}_{L|\mathbb{Q}} h_{\mathfrak{p}}(T)$$

and such that the coefficients of $h_{\mathfrak{p}}(T)$ generate L (over $\mathbb{Q}$).

(d) *Suppose that the Mumford–Tate conjecture for A holds. Then the sets S, S_{MT} have positive density, equal to $[F_A^{\mathrm{conn}} : F]^{-1}$.*

Proof. Part (a) was proven in Lemma 3.5 (following from property (iv)). Part (b), that the center embeds in each Frobenius field, follows from the (proven) Tate conjecture [CMSV19, Corollary 7.4.4]. For part (c), using part (b) we have an embedding $L \hookrightarrow \mathbb{Q}[T]/(g_{\mathfrak{p}}(T))$, so $g_{\mathfrak{p}}(T)$ is normic over L by Proposition 2.3 applied to the monic reciprocal polynomial $T^d g_{\mathfrak{p}}(1/T) \in \mathbb{Q}[T]$, where $d = \deg g_{\mathfrak{p}}(T)$.

Finally, part (d) is a slight refinement of fundamental work of Zywina [Zyw14]: the proof of [CMSV19, Proposition 7.3.25] gives the result for S, and the statement for S_{MT} then follows using the fact that the set of primes satisfying (vi) has full density when $F = F_A^{\mathrm{conn}}$ [Zyw14, Proposition 2.4(ii)]. □

Proposition 3.9. *Let $\mathfrak{q} \in S$ and let $M := \mathbb{Q}[T]/(g_{\mathfrak{q}}(T))$. Suppose that the Mumford–Tate conjecture holds for A. Then there exists an embedding $L \hookrightarrow M$, and an extension $N \supseteq M$, normal over $\mathbb{Q}$, such that for all $\mathfrak{p} \in S$ outside of a set of density zero (depending on $\mathfrak{q}$), the following hold:*

(a) *The polynomial $g_{\mathfrak{p}}(T)$ factors over $N[T]$ into exactly $[L : \mathbb{Q}]$ irreducible factors conjugate under $\mathrm{Gal}(N \mid \mathbb{Q})$.*
(b) *Any such irreducible factor is normic for $g_{\mathfrak{p}}(T)$ over N, and the subfield of N generated by its coefficients is conjugate to L (over $\mathbb{Q}$).*

Proof. We prove part (a) relying on work of Zywina [Zyw14] and comparing the action of Galois groups and the Weyl group. Let $N \supseteq \mathbb{Q}$ be a finite normal extension containing the fields F_A^{conn}, M, and $F_{\mathbf{G}_A}$.

Let $\mathfrak{p} \in S$. By Proposition 3.8(d), the sets S and S_{MT} have the same density, so avoiding a set of density zero we may suppose $\mathfrak{p} \in S_{MT}$. Further avoiding a zero-density set depending on N, the orbits of the natural action of Gal_N on the roots of $g_{\mathfrak{p}}(T)$ are the same as the orbits the action of the absolute Weyl group $W(\mathbf{G}_A, \mathbf{T})$ [Zyw14, Proposition 6.6]. (In fact, there is a natural homomorphism $\mathrm{Gal}_N \to \mathrm{Aut}(X(\mathbf{T}))$ depending on $\mathfrak{p}$ whose image lies in $W(\mathbf{G}_A, \mathbf{T})$ and which is an isomorphism for all primes of N above a prime $\mathfrak{p} \in S$ outside a set of density zero.)

We claim that there are $[L : \mathbb{Q}]$ such orbits by making a second comparison to the action on the weights. The group $W(\mathbf{G}_A, \mathbf{T})$ also acts on the set Ω of weights of $\mathbf{T}$. By Zywina [Zyw14, Lemma 6.1(ii)], this action has $[L : \mathbb{Q}]$ orbits. Using property (vi) of S_{MT}, there is an element $t_{\mathfrak{p}} \in \mathbf{T}(\mathbb{C})$ whose characteristic polynomial agrees with $c_{\mathfrak{p}}(T)$: see Noot [Noo09, Theorem 1.8] or Zywina [Zyw14, §4.2]. On the assumption the Mumford–Tate conjecture for A, the set Ω is in natural bijection with the roots of $g_{\mathfrak{p}}(T)$ (equivalently, of $c_{\mathfrak{p}}(T)$) by [Zyw14, Lemma 6.2] applied to $t = t_{\mathfrak{p}}$. The claim follows.

From the claim, the polynomial $g_{\mathfrak{p}}(T) \in \mathbb{Q}[T]$ factors into $[L : \mathbb{Q}]$ irreducible factors in $N[T]$. Since $g_{\mathfrak{p}}(T) \in \mathbb{Q}[T]$ is irreducible, the irreducible factors of $g_{\mathfrak{p}}(T)$ in $N[T]$ are conjugate under $\mathrm{Gal}(N \mid \mathbb{Q})$, so these factors are distinct and of common degree $\deg g_{\mathfrak{p}}(T)/[L : \mathbb{Q}]$, proving (a).

Next, part (b). Let $\mathfrak{p}$ be a prime not among the set of exceptions in the previous paragraph. Let $h'_{\mathfrak{p}}(T) \in N[T]$ be such an irreducible factor of $g_{\mathfrak{p}}(T)$ and L' the number field generated by its coefficients. As $\mathrm{Gal}(N \mid \mathbb{Q})$ acts transitively on the $[L : \mathbb{Q}]$ irreducible factors of $g_{\mathfrak{p}}(T)$ with stabilizer $\mathrm{Gal}(N \mid L')$, by the orbit-stabilizer lemma we have

$$[L : \mathbb{Q}] = \frac{\#\,\mathrm{Gal}(N \mid \mathbb{Q})}{\#\,\mathrm{Gal}(N \mid L')} = [L' : \mathbb{Q}].$$

Therefore condition (iii) in Proposition 2.3 is satisfied, so $h'_{\mathfrak{p}}(T)$ is normic for $g_{\mathfrak{p}}(T)$, which is to say, $g_{\mathfrak{p}}(T) = \mathrm{Nm}_{L'|K} h'_{\mathfrak{p}}(T)$. Thus, the minimal degree of a normic factor for $g_{\mathfrak{p}}(T)$ over N is $\deg g_{\mathfrak{p}}(T)/[L:\mathbb{Q}]$.

On the other hand, by Proposition 3.8(b), there exists an embedding $L \hookrightarrow M \subseteq N$. Then by Proposition 3.8(c), there exists a normic factor $h_{\mathfrak{p}}(T) \in L[T] \subseteq N[T]$ for $g_{\mathfrak{p}}(T)$. With Proposition 2.3(iii) again satisfied, we conclude $\deg h_{\mathfrak{p}}(T) = \deg g_{\mathfrak{p}}(T)/[L:\mathbb{Q}]$, so $h_{\mathfrak{p}}(T) \in L[T] \subseteq N[T]$ achieves the minimal degree of a normic factor of $g_{\mathfrak{p}}(T)$ over N. It follows that $h_{\mathfrak{p}}(T)$ is one of the irreducible factors of $g_{\mathfrak{p}}(T)$ in $N[T]$, hence is conjugate to $h'_{\mathfrak{p}}(T)$ in N. The coefficients of $h_{\mathfrak{p}}(T)$ generate L (as a subfield of N), and so each L' is isomorphic and therefore Galois conjugate to L in N. □

We now prove our first theorem.

Proof of Theorem 1.1. Let S be the set defined in Definition 3.4. The set S has positive density by Proposition 3.8(d). Properties (iii) and (iv) together imply that $Y_{\mathfrak{p}}$ is geometrically simple; then properties (i), (iii), (iv), and (v) of S and Proposition 3.8(b) give properties (i) and (ii) in the theorem.

We turn to the final statement of the theorem. Let $\mathfrak{q} \in S$ be fixed, let $M := M(\mathfrak{q})$, let $N \supseteq M$ be as in Proposition 3.9, and let $\mathfrak{p}$ be a prime not in the exceptional set in this proposition. Let $K \subseteq M$ be a number field that embeds in $M(\mathfrak{p}) := \mathbb{Q}[T]/(g_{\mathfrak{p}}(T))$; we show K embeds in the center L. Let $\sigma\colon K \hookrightarrow M(\mathfrak{p})$ be an embedding and let $a \in M(\mathfrak{p})$ be a root of $g_{\mathfrak{p}}(T)$. Then, by Proposition 2.3, the minimal polynomial of a over $\sigma(K)$ pulls back under σ to a normic polynomial $h_{\mathfrak{p},K}(T) \in K[T]$ for $g_{\mathfrak{p}}(T)$ over M whose coefficients generate K. On the other hand, by Proposition 3.9(b), there exists a normic factor of $g_{\mathfrak{p}}(T)$ over N that is *irreducible* in $N[T]$ and whose coefficients generate L, so after conjugating there exists $L' \subseteq N$ conjugate to L and $h_{\mathfrak{p},L'}(T) \in L'[T]$ normic for $g_{\mathfrak{p}}(T)$ over N such that $h_{\mathfrak{p},L'}(T) \mid h_{\mathfrak{p},K}(T)$. Then by Proposition 2.9(b), since the coefficients of $h_{\mathfrak{p},L'}(T)$ generate L' we conclude that $K \subseteq L' \simeq L$. □

4. The splitting field of the Mumford–Tate group

In this section we prove Theorem 1.2. We start with the following lemma on algebraic groups, which is similar in spirit to results of Jouve–Kowalski–Zywina [JKZ13, Lemma 2.3].

Lemma 4.1. *Let $\mathbf{G} \leq \mathrm{GL}_{n,k}$ be a (linear) reductive group over a perfect field k, let $\mathbf{T} \leq \mathbf{G}$ be a maximal torus, and let $t \in \mathbf{T}(k^{\mathrm{al}})$ be any element. Let $\mathcal{W}_t$ be the set of eigenvalues of t and let $L := k(\mathcal{W}_t)$. Let Φ_t be the subgroup of $(k^{\mathrm{al}})^\times$ generated by $\mathcal{W}_t$.*

Suppose that Φ_t is a free abelian group of rank equal to the dimension of $\mathbf{T}$. Then L is a splitting field for $\mathbf{T}$.

Proof. Let $\mathbf{D}$ be the k-subgroup of $\mathbf{G}$ generated by t. As t is contained in a torus, it is a semisimple element, and this implies that $\mathbf{D}$ is a group of multiplicative type (the identity component $\mathbf{D}^0_{k^{\mathrm{al}}}$ of $\mathbf{D}_{k^{\mathrm{al}}}$ is a torus). By Borel [Bor91, §8.4], we have that L is a splitting field of $\mathbf{D}$, so it suffices to show that $\mathbf{D} = \mathbf{T}$. Clearly $\mathbf{D}^0 \leq \mathbf{D} \leq \mathbf{T}$, so it is enough to prove that $\mathbf{D}^0$ is a torus of the same dimension as $\mathbf{T}$. The group Φ_t can be identified with the image of the group homomorphism

$$\begin{aligned} \gamma_{\mathbf{D}}\colon X(\mathbf{D}) &\to (k^{\mathrm{al}})^\times \\ \chi &\mapsto \chi(t), \end{aligned}$$

where $X(\mathbf{D})$ is the character group of $\mathbf{D}$. Notice that $X(\mathbf{D})$ is an abelian group of finite type, but not necessarily free. We obtain

$$\dim \mathbf{T} = \operatorname{rk} \Phi_t = \operatorname{rk} \gamma_{\mathbf{D}}(X(\mathbf{D})) \leq \operatorname{rk} X(\mathbf{D}) = \dim \mathbf{D}^0,$$

which concludes the proof. □

Lemma 4.2. *Let $\mathfrak{p} \in S_{MT}$ and let $\mathcal{W}_{\mathfrak{p}} \subseteq (\mathbb{Q}^{\mathrm{al}})^{\times}$ be the set of roots of $g_{\mathfrak{p}}(T)$. Then the Mumford–Tate group $\mathbf{G}_A$ is split over the field $\mathbb{Q}(\mathcal{W}_{\mathfrak{p}})$.*

Proof. Let $\mathbf{T}$ be a maximal torus of $\mathbf{G}_A$. As explained by Zywina [Zyw14, §6.2], there exists $t_{\mathfrak{p}} \in \mathbf{T}(\mathbb{Q}^{\mathrm{al}})$ such that $c_{\mathfrak{p}}(T) = \det(T - t_{\mathfrak{p}})$, so the eigenvalues of $t_{\mathfrak{p}}$ are precisely the roots of $c_{\mathfrak{p}}(T)$ (equivalently, of $g_{\mathfrak{p}}(T)$). By definition of S_{MT}, the group $\Phi_{\mathfrak{p}} < (\mathbb{Q}^{\mathrm{al}})^{\times}$ generated by $\mathcal{W}_{\mathfrak{p}}$ is free of rank equal to the rank of $\mathbf{G}_A$, so we can apply Lemma 4.1. □

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Let S_{MT} be the set of Definition 3.4. Since $S_{MT} \subseteq S$, we have already shown property (i) in Theorem 1.1(a), and S_{MT}, S have the same density by Proposition 3.8. For $\mathfrak{p} \in S_{MT}$, let $\mathcal{W}_{\mathfrak{p}}$ the set of roots of $c_{\mathfrak{p}}(T)$ in $(\mathbb{Q}^{\mathrm{al}})^{\times}$, so $N(\mathfrak{p}) = \mathbb{Q}(\mathcal{W}_{\mathfrak{p}})$. By Lemma 4.2, for every $\mathfrak{p} \in S_{MT}$, the Mumford–Tate group $\mathbf{G}_A$ is split over $\mathbb{Q}(\mathcal{W}_{\mathfrak{q}})$, which proves (a).

Suppose now that $F = F_A^{\mathrm{conn}}$. Applying a result of Zywina [Zyw14, Proposition 6.6] (with $L = F_{\mathbf{G}_A}$), there is a set Σ_1 of primes of density zero such that for every $\mathfrak{p} \in S_{MT} \smallsetminus \Sigma_1$, we have $\mathrm{Gal}(F_{\mathbf{G}_A}(\mathcal{W}_{\mathfrak{p}}) \,|\, F_{\mathbf{G}_A}) \simeq W(\mathbf{G}_A, \mathbf{T})$. Let $\mathfrak{q} \in S_{MT}$. Since $F_{\mathbf{G}_A} \subseteq \mathbb{Q}(\mathcal{W}_{\mathfrak{q}})$, by Lemma 4.2, we have $F_{\mathbf{G}_A}(\mathcal{W}_{\mathfrak{q}}) = \mathbb{Q}(\mathcal{W}_{\mathfrak{q}}) = N(\mathfrak{q})$. Applying the result of Zywina [Zyw14, Proposition 6.6] again (now with $L = N(\mathfrak{q})$), there is a set $\Sigma_{2,\mathfrak{q}}$ (depending on $\mathfrak{q}$) of primes of density zero such that for every $\mathfrak{p} \in S_{MT} \smallsetminus (\Sigma_1 \cup \Sigma_{2,\mathfrak{q}})$ we have $\mathrm{Gal}(N(\mathfrak{q})(\mathcal{W}_{\mathfrak{p}}) \,|\, N(\mathfrak{q})) \simeq W(\mathbf{G}_A, \mathbf{T})$ and $\mathrm{Gal}(F_{\mathbf{G}_A}(\mathcal{W}_{\mathfrak{p}}) \,|\, F_{\mathbf{G}_A}) \simeq W(\mathbf{G}_A, \mathbf{T})$. This means precisely that the two fields $F_{\mathbf{G}_A}(\mathcal{W}_{\mathfrak{p}}) = N(\mathfrak{p})$ and $N(\mathfrak{q})$ are linearly disjoint over $F_{\mathbf{G}_A}$, hence $N(\mathfrak{q}) \cap N(\mathfrak{p}) = F_{\mathbf{G}_A}$. This proves (b) in the case $F = F_A^{\mathrm{conn}}$.

The general case follows by extension to F_A^{conn}, taking the set of primes of F that lie below the set of primes of F_A^{conn} constructed in the previous paragraph. □

5. Algorithm

In this section, we exhibit how Theorem 1.1 can be used effectively to compute the center L of a geometric endomorphism algebra. We keep notation as introduced in section 3.

Algorithm 5.1.
Input:

- $m \in \mathbb{Z}_{\geq 1}$ such that $m^2 = \dim_L B$,
- $C \in \mathbb{Z}_{\geq 1}$, and
- $c_{\mathfrak{p}}(T) \in 1 + T\mathbb{Z}[T]$ as in (3.1) for all good primes $\mathfrak{p}$ with $\operatorname{Nm} \mathfrak{p} \leq C$.

Output:

- a boolean; if this boolean is `true`, then further
- $d_C \in \mathbb{Z}_{\geq 1}$ such that $[L : \mathbb{Q}] \leq d_C$, and
- $\{L_{C,i}\}_i$, a set of number fields such that for some i there exists an embedding $L \hookrightarrow L_{C,i}$ of number fields.

Steps:

1. Using Lemma 3.5, compute the set of primes $S'_C := S' \cap \{\mathfrak{p} : \operatorname{Nm}\mathfrak{p} \leq C\}$. If $S'_C = \emptyset$, return false.
2. Choose $\mathfrak{q} \in S'_C$ and initialize $M := \mathbb{Q}[T]/(g_\mathfrak{q}(T))$ where $c_\mathfrak{q}(T) = g_\mathfrak{q}(T)^m$.
3. For each prime $\mathfrak{p} \in S'_C$ with $\mathfrak{p} \neq \mathfrak{q}$:
   a. Let $g_\mathfrak{p}(T) \in \mathbb{Q}[T]$ be such that $g_\mathfrak{p}(T)^m = c_\mathfrak{p}(T)$.
   b. Factor $g_\mathfrak{p}(T)$ into irreducibles in $M[T]$.
   c. Compute the set of normic factors $h_{\mathfrak{p},i}(T) \mid g_\mathfrak{p}(T)$ by checking condition (iii) of Proposition 2.3 for each divisor of $g_\mathfrak{p}(T)$ (using the factorization in Step 3b). If no factor is normic, remove $\mathfrak{p}$ from the set S'_C and continue with the next prime.
   d. For each normic divisor $h_{\mathfrak{p},i}(T)$, compute the subfield $L_{\mathfrak{p},i} \subseteq M$ generated over $\mathbb{Q}$ by its coefficients.
   e. Reduce $\{L_{\mathfrak{p},i}\}_i$ to a subset of representatives up to isomorphism of number fields.
   f. Let $d_\mathfrak{p} := \max_i [L_{\mathfrak{p},i} : \mathbb{Q}]$ and let $r_\mathfrak{p} := \#\{L_{\mathfrak{p},i} : [L_{\mathfrak{p},i} : \mathbb{Q}] = d_\mathfrak{p}\}$.
4. If now $S'_C = \emptyset$, return false.
5. Let $\mathfrak{p}$ minimize first $\min_\mathfrak{p} d_\mathfrak{p}$ then $\min_\mathfrak{p} r_\mathfrak{p}$. For any such minimal prime $\mathfrak{p}$, return true, $d_C := d_\mathfrak{p}$ and the set of subfields $\{L_{\mathfrak{p},i} : [L_{\mathfrak{p},i} : \mathbb{Q}] = d_\mathfrak{p}\}$.

Proof of correctness. By Proposition 3.8(b), for each good $\mathfrak{p}$ there is an embedding $\sigma\colon L \hookrightarrow \mathbb{Q}[T]/(g_\mathfrak{p}(T))$. By finiteness, there exists a maximal subextension $\mathbb{Q} \subseteq L \subseteq L' \subseteq M$ with an embedding $L' \hookrightarrow \mathbb{Q}[T]/(g_\mathfrak{p}(T))$, which we may take as extending σ. By (ii) $\Rightarrow$ (iii) of Proposition 2.3, there exists a normic factor $h_{\mathfrak{p},i}(T) \mid g_\mathfrak{p}(T)$ such that $L_{\mathfrak{p},i} = L'$. Therefore the algorithm gives correct output for any prime $\mathfrak{p}$ selected in Step 5. □

Remark 5.2. In step 3c we cannot limit ourselves to testing *irreducible* factors, because a polynomial $f(T) \in \mathbb{Q}[T]$ may in general have no irreducible normic factors in $M[T]$, see Remark 2.10.

Proposition 5.3. *Suppose that the Mumford–Tate conjecture for A holds. Then for large enough C, Algorithm 5.1 returns* true, *$d_C = [L : \mathbb{Q}]$, and a singleton $\{L_{C,i}\}$, such that $[L_{C,i} : \mathbb{Q}] = d_C$ and $L \simeq L_{C,i}$.*

Proof. By Proposition 3.9, there exists an embedding $L \hookrightarrow M$ and an extension $N \supseteq M$, with N normal over $\mathbb{Q}$, such that $g_\mathfrak{p}(T)$ factors over $N[T]$ with exactly $[L : \mathbb{Q}]$ irreducible factors for all $\mathfrak{p} \in S$ outside a set of density zero. Moreover, each such irreducible factor is normic, and the number field generated by its coefficients is conjugate to L (over $\mathbb{Q}$) by an element of $\operatorname{Gal}(N \mid \mathbb{Q})$. For C large enough, in the course of the algorithm we will eventually find $\mathfrak{p} \in S' \subseteq S$ which is not in this density zero set of exceptions.

We first claim that such a prime $\mathfrak{p}$ does not get discarded in Step 3. Indeed, let $h'_\mathfrak{p}(T)$ be any irreducible factor of $g_\mathfrak{p}(T)$ in $N[T]$. Then $h'_\mathfrak{p}(T)$ is normic. Moreover, its field of coefficients is isomorphic to L, so after Galois conjugation we may suppose it is equal to L. Then $h'_\mathfrak{p}(T) \in L[T] \subseteq M[T]$, so it is an irreducible factor of $g_\mathfrak{p}(T)$ in $M[T]$, and still normic, so $h'_\mathfrak{p}(T) = h_{\mathfrak{p},i}$ for some i, passing Step 3c.

Next, we claim that for such a prime $\mathfrak{p}$ we have $d_\mathfrak{p} = [L : \mathbb{Q}]$, $r_\mathfrak{p} = 1$, and $\{L_{\mathfrak{p},i}\}_i = \{L\}$ (up to isomorphism). Indeed, let $h_{\mathfrak{p},j}(T)$ be another normic factor of $g_\mathfrak{p}(T)$ from Step 3c with $i \neq j$ and field of coefficients $L_{\mathfrak{p},j}$. From the earlier factorization of $g_\mathfrak{p}(T)$ over N into normic irreducibles, there exists a normic factor of $h_{\mathfrak{p},j}(T)$ over $N[T]$ whose field of coefficients is Galois conjugate to L. By Proposition 2.9(b), we conclude that $L_{\mathfrak{p},j}$ is contained in this field

of coefficients, thus $[L_{\mathfrak{p},j} : \mathbb{Q}] \leq [L : \mathbb{Q}] = [L_{\mathfrak{p},i} : \mathbb{Q}]$ with equality if and only if $L_{\mathfrak{p},j} \simeq L$ if and only if $\deg h_{\mathfrak{p},j}(T) = d_{\mathfrak{p}}$.

To conclude, suppose that $\mathfrak{p}'$ is a prime such that $d_{\mathfrak{p}'} = d_{\mathfrak{p}} = [L : \mathbb{Q}]$ and $r_{\mathfrak{p}'} = 1$. Then $L \hookrightarrow L_{\mathfrak{p}',1}$ so by degrees $L \simeq L_{\mathfrak{p}',1}$ and the desired conclusion holds. □

Remark 5.4. In particular, the quantity $r_{\mathfrak{p}}$ in Algorithm 5.1 is only used when C is not yet large enough for Proposition 5.3 to apply, and is used only to possibly reduce the size of the output (without affecting its correctness).

Example 5.5. For a very simple example of the algorithm, consider the elliptic curve with LMFDB label 11.a2 a model for the modular curve $X_0(11)$. One can easily verify that $2, 3 \in S'$ and that $M(2) \simeq \mathbb{Q}(\sqrt{-1})$ and $M(3) \simeq \mathbb{Q}(\sqrt{-11})$. Thus by Theorem 1.1, $L = \mathbb{Q}$ and therefore $\operatorname{End} E^{\mathrm{al}} = \mathbb{Z}$.

Example 5.6. Let X be the curve defined in $\mathbb{P}^3$ by the equations

$$\begin{aligned} -yz - 12z^2 + xw - 32w^2 &= 0 \\ y^3 + 108x^2z + 36y^2z + 8208xz^2 - 6480yz^2 + 74304z^3 + 96y^2w & \\ +2304yzw - 248832z^2w + 2928yw^2 - 75456zw^2 + 27584w^3 &= 0. \end{aligned} \tag{5.7}$$

Then X is a canonically embedded curve of genus 4. This curve arises in the classification of elliptic curves over $\mathbb{Q}$ with constrained 3-adic Galois image (in upcoming work of Jeremy Rouse, Drew Sutherland, and David Zureick-Brown): it can be obtained as the image of a $\mathbb{Q}$-rational basis of modular forms attached to the newspace with LMFDB label 81.2.c.b of level 81. We use this example as a test case for our algorithm, ignoring its modular provenance. Let $J := \mathrm{Jac}(X)$ be the Jacobian of X.

With a Gröbner basis computation one can show that X has good reduction away from 2 and 3, and hence also J. By point counting on the reduction of X modulo p one can compute $c_p(T)$, for $p \neq 2, 3$ which is feasible for small primes. By employing Lemma 3.6, we guess $m = 4$ and under that assumption we have that the first two primes in S' are 19 and 37. Furthermore, we have

$$\begin{aligned} g_{19}(T) &= 1 - 2T + 19T^2, \quad M(19) \simeq \mathbb{Q}(\sqrt{-2}); \\ g_{37}(T) &= 1 + 7T + 37T^2, \quad M(37) \simeq \mathbb{Q}(\sqrt{-11}). \end{aligned} \tag{5.8}$$

We conclude that $L = \mathbb{Q}$. In fact, we can indeed verify [CMSV19] that J is of GL_2-type over $\mathbb{Q}$, and geometrically we have an isogeny $J^{\mathrm{al}} \sim E^4$ where E is an elliptic curve whose j-invariant satisfies $j^2 - 7317j + 283593393 = 0$.

References

[Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih. *Hodge cycles, motives, and Shimura varieties*, volume 900 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1982.

[JKZ13] Florent Jouve, Emmanuel Kowalski, and David Zywina. Splitting fields of characteristic polynomials of random elements in arithmetic groups. *Israel J. Math.*, 193(1):263–307, 2013.

[Ked06] Kiran S. Kedlaya. Quantum computation of zeta functions of curves. *Comput. Complexity*, 15(1):1–19, 2006.

[Klü99] Jürgen Klüners. On polynomial decompositions. *J. Symbolic Comput.*, 27(3):261–269, 1999.

[Lom19] Davide Lombardo. Computing the geometric endomorphism ring of a genus-2 Jacobian. *Math. Comp.*, 88(316):889–929, 2019.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[Noo09] Rutger Noot. Classe de conjugaison du Frobenius d'une variété abélienne sur un corps de nombres. *J. Lond. Math. Soc. (2)*, 79(1):53–71, 2009.

[Ser13] Jean-Pierre Serre. *Oeuvres/Collected papers. IV. 1985–1998*. Springer Collected Works in Mathematics. Springer, Heidelberg, 2013. Reprint of the 2000 edition.

[SvH17] Jonas Szutkoski and Mark van Hoeij. The complexity of computing all subfields of an algebraic number field. *preprint*, 2017. `arXiv:1606.01140`.

[vG00] Bert van Geemen. Kuga-Satake varieties and the Hodge conjecture. In *The arithmetic and geometry of algebraic cycles (Banff, AB, 1998)*, volume 548 of *NATO Sci. Ser. C Math. Phys. Sci.*, pages 51–82. Kluwer Acad. Publ., Dordrecht, 2000.

[vHKN13] Mark van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. *J. Symbolic Comput.*, 52:17–34, 2013.

[Zyw14] David Zywina. The Splitting of Reductions of an Abelian Variety. *International Mathematics Research Notices*, 2014(18):5042–5083, 2014.

[Zyw20] David Zywina. Determining monodromy groups of abelian varieties. *preprint*, 2020. `arXiv:2009.07441v1` .

URL: https://edgarcosta.org

URL: http://people.dm.unipi.it/lombardo/

URL: http://www.math.dartmouth.edu/~jvoight/