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 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 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.*

Theorem 1.1 relies crucially on work of Zywina [Zyw13]. 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 may be taken as in Definition 3.4: it is effectively computable, if m is given.

The primary motivation for this theorem is the following algorithmic application (relying on Algorithm 5.1).

Date: June 6, 2019.

Theorem 1.2. *Let A be an abelian variety over a number field and suppose that the Mumford–Tate conjecture for A holds. Then the center of the geometric endomorphism algebra of A is effectively computable.*

Remark 1.3. 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. However, the upper bound is not guaranteed to be sharp—the truth of the Mumford-Tate conjecture is an essential ingredient in the proof of Proposition 5.3.

Theorem 1.2 strengthens a result of Costa–Mascot–Sijsling–Voight [CMSV19, Proposition 7.4.7] by removing a hypothesis [CMSV19, Hypothesis 7.4.6] that is directly implied by Theorem 1.1. Having a practical algorithm to determine a sharp upper bound on $\dim_{\mathbb{Z}} \mathrm{End}(A^{\mathrm{al}})$ enables us to rigorously certify that a numerical calculation of the endomorphism ring of a Jacobian is correct. This gives an efficient algorithm to compute $\mathrm{End}(A^{\mathrm{al}})$ whenever the abelian variety A/F is explicitly given as a Jacobian or, more generally, as an isogeny factor of one (hence in principle all abelian varieties). It is explained in [CMSV19] how to reduce to the case where A is isotypic.

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 the algorithm in Theorem 1.2 does not compute the field F_A^{conn} directly. In particular, we prove Theorem 1.2 without establishing if the exceptional primes $\mathfrak{p}$ at the end of Theorem 1.1 can be computed effectively.

Finally, we also show 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 1.4. *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, 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 1.4, the intersection $N(\mathfrak{q}) \cap N(\mathfrak{p})$ is well-defined up to isomorphism since both fields are normal extensions of $\mathbb{Q}$.

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 [Zyw13] and Costa–Mascot–Sijsling–Voight [CMSV19] and prove Theorem 1.1. Then in section 4 we prove Theorem 1.4. We conclude in section 5 with the algorithmic application, proving Theorem 1.2.

Acknowledgements. The authors would like to thank Andrea Maffei for an enlightening discussion about the Steiner section for reductive groups, 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

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

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 contains $L \supseteq K$.

Example 2.2. If $f(T) \in K[T]$ is 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 $\sigma\colon L \hookrightarrow K(a)$ and $\sigma(h)(T)$ 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 $h(T)$.

Remark 2.4. If we start with $L \subseteq K(a)$ an embedded subfield, then for every $\sigma \in \mathrm{Aut}_K(K(a))$, by (a) we have $g(T) = \mathrm{Nm}_{L|K} h(T)$ for $h(T)$ the minimal polynomial of $\sigma(a)$ over L—but not every $h(T)$ necessarily arises this way (unless $K(a)$ is Galois over K).

Proof. 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 $\{\sigma_i\}_i = \operatorname{Hom}_K(L, N)$. 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

$$\begin{aligned}[K(a) : K] &= \deg g(T) = \deg h(T)[L : K] = \deg h'(T)[L' : K] \\ &= [L'(a) : L'][L' : K] = [L'(a) : K];\end{aligned} \tag{2.5}$$

since $L'(a) \supseteq K(a)$, by (2.5) we have $L'(a) = K(a)$ so $L' \subseteq K(a)$, and we may take $\sigma = \sigma_i$ in (ii).

We now prove (ii) ⇒ (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

$$[K(a) : K] = \deg g(T) = \deg \sigma(h(T))[\sigma(L) : K] = \deg h(T)[L : K]. \tag{2.6}$$

To conclude, we show (iii) ⇒ (i). Let $b \in N$ be a root of $h(T)$. We are given $h(T) \mid g(T)$ and $h(b) = 0$, so $g(b) = 0$; since $g(T) \in K[T]$ is irreducible we conclude $g(T)$ is the minimal polynomial of b over K. Let $n(T) := \operatorname{Nm}_{L|K} h(T) \in K[T]$. 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 2.7. 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) $g(T) = \operatorname{Nm}_{L|K} h(T)$, where $L \subseteq M$ is generated over K by the coefficients of $h(T)$.

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 do not need to employ these more advanced techniques.

Example 2.9. 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 $h_2(T) := \operatorname{Nm}_{L_1|L_2} h_1(T)$ is also normic for $g(T)$ over M.

We apply the previous bit of Galois theory as follows.

Proposition 2.10. *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 $M \supseteq K$ 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 $h_1(T) = (\sigma h_1)(T) \mid (\sigma h_2)(T)$, contradiction. So $H_1 \subseteq H_2$ and by the Galois correspondence $L_2 \subseteq L_1$. □

Remark 2.11. Proposition 2.10(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 2.12. In Proposition 2.10(b), the converse does not need to hold. For example, suppose that $M := K(a) \supseteq K$ is Galois. 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 [Zyw13] concerning splitting of reductions of abelian varieties (as further elaborated upon by Costa–Mascot–Sijsling–Voight [CMSV19]).

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}). 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 (i.e., a nonzero prime ideal of its ring of integers), write $\mathbb{F}_{\mathfrak{p}}$ for its residue field, and let $\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}$ be the algebraic closure of $\mathbb{F}_{\mathfrak{p}}$ and $\mathrm{Frob}_{\mathfrak{p}}$ 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 $V_\ell A := T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, a $\mathbb{Q}_\ell$-vector space of dimension $2g$; 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 good $\mathfrak{p}$ 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 $\mathrm{Frob}_{\mathfrak{p}}$ (independent of ℓ).

Let $\mathbf{GL}(V_\ell(A))$ be the $\mathbb{Q}_\ell$-algebraic group of ($\mathbb{Q}_\ell$-linear) automorphisms of $V_\ell(A)$, so that $\rho_{A,\ell}(\mathrm{Gal}_F) \leq \mathrm{GL}(V_\ell(A)) = \mathbf{GL}(V_\ell(A))(\mathbb{Q}_\ell)$. 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 $\mathbf{G}^0_{A,\ell}$ be the identity component of $\mathbf{G}_{A,\ell}$.

Let F_A^{conn} be the fixed field in F^{al} of $\rho^{-1}_{A,\ell}(\mathbf{G}^0_{A,\ell}(\mathbb{Q}_\ell))$. 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 $\mu\colon \mathbf{G}_{m,\mathbb{C}} \to \mathbf{GL}(V_{\mathbb{C}})$ 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 that is independent of the choice of embedding of F into $\mathbb{C}$.

Let $\mathbf{T} \subset \mathbf{G}_A$ be a maximal torus, and let $W(\mathbf{G}_A, \mathbf{T})$ denote the absolute Weyl group of $\mathbf{G}_A$ with respect to $\mathbf{T}$ [Zyw13, §3.2]. We write $\operatorname{rk} \mathbf{G}_A$ for the rank of $\mathbf{G}_A$ (i.e., equal to the dimension of $\mathbf{T}$).

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 $\mathbf{G}^0_{A,\ell}$.*

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) $\mathrm{End}(A^{\mathrm{al}}_{\mathfrak{p}})$ is defined over $\mathbb{F}_{\mathfrak{p}}$;
- (iv) We have an isogeny $A_{\mathfrak{p}} \sim Y^m_{\mathfrak{p}}$ 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 $\Phi_{\mathfrak{p}} \leq (\mathbb{Q}^{\mathrm{alg}})^\times$ of rank equal to $\operatorname{rk} \mathbf{G}_A$.

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 $\operatorname{rk} \mathbf{G}_A$ is also given, then S'_{MT} is effectively computable.*

Proof. Condition (i′) can be checked by ensuring the model is smooth. We can clearly check (ii). Given $c_{\mathfrak{p}}(T)$, which can be computed by counting points modulo $\mathfrak{p}$, we can check conditions (iii), (iv), and (v) as follows. For (iii), we may apply the (proven) Tate conjecture [CMSV19, Lemma 7.2.7]. From (iii), it follows that $c_{\mathfrak{p}}(T)$ is not divisible by $1 - pT^2$, where $p = \#\mathbb{F}_{\mathfrak{p}}$. Thus, under the assumption of (ii) and (iii), condition (iv) is equivalent to $c_{\mathfrak{p}}(T)$ being an mth power of an irreducible $\mathbb{Q}$ polynomial, and if so (v) follows by Honda–Tate theory (as explained by Zywina [Zyw13, Lemma 2.1]).

To conclude, we claim that condition (vi) can be checked effectively if $\operatorname{rk} \mathbf{G}_A$ 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. Using standard algorithms, we can compute generators for the group $\mathbb{Z}_{N,(p)}^{\times}$, a free abelian group of finite rank modulo its torsion subgroup of roots of unity. Then, using linear algebra over $\mathbb{Z}$ (in the exponents), we can see if the subgroup generated by the (reciprocal) roots is free of the correct rank. □

Remark 3.6. If m is not given, we can still guess its value, as follows.

To obtain an upper bound for m, we consider primes $\mathfrak{p}$ that satisfy conditions (i′)–(iii) of Definition 3.4, so that $c_{\mathfrak{p}}(T)$ is the $m_{\mathfrak{p}}$th power of an irreducible polynomial in $\mathbb{Q}[T]$; then $m \leq m_{\mathfrak{p}}$. This upper bound is sharp for a set of primes $\mathfrak{p}$ of positive density if the Mumford–Tate conjecture for A holds [Zyw13, Theorem 1.2]. In the application to the computation of endomorphism rings of Jacobians, a sharp lower bound for m comes from the numerical computation of the endomorphism ring, and so m can also be determined effectively in this case.

Similar techniques can be applied to guess the value of $\operatorname{rk} \mathbf{G}_A$.

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

Proposition 3.7. *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 [Zyw13]: 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 $F = F_A^{\mathrm{conn}}$ [Zyw13, Proposition 2.4(ii)]. □

Proposition 3.8. *Let $\mathfrak{q} \in S$ and let $M := \mathbb{Q}[T]/(g_{\mathfrak{q}}(T))$, and suppose that the Mumford–Tate conjecture holds for A. Then there exists 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 in N.*

Proof. First, part (a). Let $N \supseteq \mathbb{Q}$ be a finite normal extension containing F_A^{conn}, M, and $F_{\mathbf{G}_A}$. By a result of Zywina (see [Zyw13, Lemma 6.1(ii)] and the proof of [Zyw13, Lemma 6.7]), the absolute Weil group $W(\mathbf{G}_A, \mathbf{T})$ with respect to $\mathbf{T}$ acts on the roots of $g_{\mathfrak{p}}(T)$ (equivalently, the roots of $c_{\mathfrak{p}}(T)$) with $[L:\mathbb{Q}]$ orbits for any $\mathfrak{p} \in S_{MT}$. Moreover, for all $\mathfrak{p} \in S_{MT}$ outside of a zero-density set depending on N, we have that the action of Gal_N on the roots of $g_{\mathfrak{p}}(T)$ matches the action of $W(\mathbf{G}_A, \mathbf{T})$ [Zyw13, Proposition 6.6]. Combining these two statements with Proposition 3.7(d) gives the result.

Next, part (b). Let $\mathfrak{p}$ be a prime not among the set of exceptions in the previous paragraph. 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 degree $\deg g_{\mathfrak{p}}(T)/[L:\mathbb{Q}]$. Let $h'_{\mathfrak{p}}(T)$ be such an irreducible factor 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

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

Then condition (iii) in Proposition 2.3 is satisfied, so $h'_{\mathfrak{p}}(T)$ is normic and $g_{\mathfrak{p}}(T) = \mathrm{Nm}_{L'|K}\, h'_{\mathfrak{p}}(T)$, that is to say, $h'_{\mathfrak{p}}(T)$ is normic for $g_{\mathfrak{p}}(T)$. 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 3.7(a), there exists an embedding $L \hookrightarrow M \subseteq N$. Then by Proposition 3.7(c), there exists a normic factor $h_{\mathfrak{p}}(T) \in L[T] \subseteq N[T]$ for $g_{\mathfrak{p}}(T)$. Therefore condition (iii) in Proposition 2.3 is satisfied, and $\deg h_{\mathfrak{p}}(T) = \deg g_{\mathfrak{p}}(T)/[L:\mathbb{Q}]$, 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 $h_{\mathfrak{p}}(T)$ generated L (as a subfield of N), and therefore each L' is 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 3.7(b). Properties (iii) and (iv) together imply that $Y_{\mathfrak{p}}$ is geometrically simple; then properties (i), (iii), (iv), and (v) of S and Proposition 3.7(a) 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 3.8, 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 $h_{\mathfrak{p},K}(T) \in K[T]$ for $g_{\mathfrak{p}}(T)$ over M whose coefficients generate

K. On the other hand, by Proposition 3.8(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 2.10(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 1.4. 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 [Zyw13, §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 1.4.

Proof of Theorem 1.4. 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 3.7. 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 [Zyw13, Proposition 6.6] (with $L = F_{\mathbf{G}_A}$), there is a set Σ_1 of primes of density zero such that for every $\mathfrak{q} \in S_{MT} \smallsetminus \Sigma_1$, we have $\mathrm{Gal}(F_{\mathbf{G}_A}(\mathcal{W}_\mathfrak{q}) \mid F_{\mathbf{G}_A}) \simeq W(\mathbf{G}_A, \mathbf{T})$. 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 [Zyw13, 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 $\mathrm{Gal}(N(\mathfrak{q})(\mathcal{W}_\mathfrak{p}) \mid N(\mathfrak{q})) \simeq W(\mathbf{G}_A, \mathbf{T})$ and $\mathrm{Gal}(F_{\mathbf{G}_A}(\mathcal{W}_\mathfrak{p}) \mid F_{\mathbf{G}_A}) \simeq W(\mathbf{G}_A, \mathbf{T})$. 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. $\square$

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.

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 $\mathrm{Nm}\,\mathfrak{p} \leq C$.

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 $S'_C := S' \cap \{\mathfrak{p} : \mathrm{Nm}\,\mathfrak{p} \leq C\}$. 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. For each irreducible factor $h_{\mathfrak{p},i}(T) \mid g_\mathfrak{p}(T)$, compute the subfield $L_{\mathfrak{p},i} \subseteq M$ generated over $\mathbb{Q}$ by its coefficients, and keep those fields $\{L_{\mathfrak{p},i}\}_i$ for which the factor $h_{\mathfrak{p},i}(T)$ is normic, checked using condition (iii) of Proposition 2.3. If no irreducible factor is normic, remove $\mathfrak{p}$ from the set S'_C and continue with the next prime.
   d. Reduce $\{L_{\mathfrak{p},i}\}_i$ to a subset of representatives up to isomorphism of number fields.
   e. 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 $\{L_{\mathfrak{p},i}\}_i$.

Proof of correctness. By Proposition 3.7(b), for each good $\mathfrak{p}$ there is an embedding $\sigma\colon L \hookrightarrow \mathbb{Q}(a_\mathfrak{p}) := \mathbb{Q}[T]/(g_\mathfrak{p}(T))$. 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 $h_{\mathfrak{p},i}(T) \mid g(T)$ such that $L_{\mathfrak{p},i} = L'$. Therefore the algorithm gives correct output for any prime $\mathfrak{p}$ selected in Step 4. $\square$

Remark 5.2. In step 2c 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 2.11.

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 unique field $L_{C,i}$, such that $[L_{C,i} : \mathbb{Q}] = d_C$ and $L \simeq L_{C,i}$.*

Proof. By Proposition 3.8, there exists an extension $N \supseteq M := M(\mathfrak{q}) = \mathbb{Q}[T]/(g_{\mathfrak{q}}(T))$, 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 depending on N; for each such irreducible factor of $g_{\mathfrak{p}}(T)$, the number field generated by its coefficients is conjugate to L in N. In other words, each $L_{C,i}$ is indeed isomorphic to L.

For C large enough, in the algorithm we will find $\mathfrak{p} \in S'_C$ which is not in the density zero set of exceptions so that the conclusion of Theorem 1.1 holds: namely, if M' is a number field that embeds in $M(\mathfrak{p})$ and in $M(\mathfrak{q})$, then M' embeds in L. We claim that such a prime $\mathfrak{p}$ does not get discarded in Step 3 and yields $d_{\mathfrak{p}} = [L : \mathbb{Q}]$, $r_{\mathfrak{p}} = 1$ and $\{L_{\mathfrak{p},i}\}_i = \{L\}$. Indeed, choose an irreducible factor $h'_{\mathfrak{p}}(T)$ of $g_{\mathfrak{p}}(T)$ in $N[T]$ with field of coefficients L: such an irreducible factor exists, because all the coefficient fields are conjugated to L in N and all irreducible factors of $g_{\mathfrak{p}}(T)$ are conjugated to each other. Then $h'_{\mathfrak{p}}(T)$ belongs to $L[T] \subseteq M[T]$, so it is an irreducible normic factor of $g_{\mathfrak{p}}(T)$ in $M[T]$. This proves that $\mathfrak{p}$ does not get discarded during Step 3.

Moreover, since we still have $L \hookrightarrow M(\mathfrak{p})$, by Proposition 2.3 there is a normic factor $h_{\mathfrak{p},i}(T) \in M[T]$ with field of coefficients $L_{\mathfrak{p},i} \simeq L$. For any other normic factor $h_{\mathfrak{p},j}(T)$ with field of coefficients $L_{\mathfrak{p},j}$, there exists an irreducible factor of $h_{\mathfrak{p},j}(T)$ in $N[T]$ whose field of coefficients is isomorphic to L. But then by Proposition 2.10(b) we conclude that $L_{\mathfrak{p},j}$ is contained in a subfield of N isomorphic to L, so in particular $[L_{\mathfrak{p},j} : \mathbb{Q}] \leq [L : \mathbb{Q}] = [L_{\mathfrak{p},i} : \mathbb{Q}]$ with equality if and only if $L_{\mathfrak{p},j} \simeq L$ if and only if $\deg h_{\mathfrak{p},j}(T) = d_{\mathfrak{p}}$.

For any other prime $\mathfrak{p}'$ such that $d_{\mathfrak{p}'} = d_{\mathfrak{p}} = [L : \mathbb{Q}]$ and $r_{\mathfrak{p}'} = 1$ (as in Step 4), we have $L \hookrightarrow L_{\mathfrak{p}',1}$ so by degrees, $L \simeq L_{\mathfrak{p}',1}$ and the desired conclusion holds. □

Proof of Theorem 1.2. By Costa–Mascot–Sijsling–Voight [CMSV19, Proposition 7.4.7], the result holds assuming a hypothesis that can be replaced by Algorithm 5.1. □

Example 5.4. 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 5.5. Consider the Jacobian $J := \operatorname{Jac}(X)$, where X is the genus 4 curve canonically embedded in $\mathbb{P}^3(x, y, z)$ defined by the equations

$$\begin{aligned} -yz - 12z^2 + xw - 32w^2 = 0 \\ y^3 + 108x^2z + 36y^2z + 8208xz^2 - 6480yz^2 + 74304z^3 + 96y^2w \\ +2304yzw - 248832z^2w + 2928yw^2 - 75456zw^2 + 27584w^3 = 0. \end{aligned} \tag{5.6}$$

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 Remark 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

$$g_{19}(T) = 1 - 2T + 19T^2, \quad M(19) \simeq \mathbb{Q}(\sqrt{-2}); \tag{5.7}$$
$$g_{37}(T) = 1 + 7T + 37T^2, \quad M(37) \simeq \mathbb{Q}(\sqrt{-11}).$$

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 $j^2 - 7317j + 283593393 = 0$. Furthermore, by looking at $c_p(T)$ for $5 \leq p \leq 181$, we believe that J corresponds to the abelian variety attached to the modular form with LMFDB label 81.2.c.b of level 81, and thus J only has bad reduction at 3.

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.

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

[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.

[Ser13] Jean-Pierre Serre. *Oeuvres/Collected papers. IV. 1985–1998.* Springer Collected Works in Mathematics. Springer, Heidelberg, 2013. Reprint of the 2000 edition [MR1730973].

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

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

[Zyw13] David Zywina. The Splitting of Reductions of an Abelian Variety. *International Mathematics Research Notices*, 2014(18):5042–5083, 06 2013.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

E-mail address: `edgarc@mit.edu`

URL: https://edgarcosta.org

Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo 5, 56127, Pisa, Italy

E-mail address: `davide.lombardo@unipi.it`

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

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: `jvoight@gmail.com`

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