Conditional Algorithmic Mordell

Levent Alpöge & Brian Lawrence

The problem.

The problem is the following. Let $f \in \mathbb{Z}[x, y]$. It is known that the set of integral solutions of $f(x, y) = 0$ has a finitary description. The same goes for the set of rational such solutions. So: can one find such finitary descriptions automatically? — that is, is there an algorithm which, when run on such an f, eventually returns a finite description of its set of integral (or rational) points?

Thanks to the negative solution of Hilbert's tenth problem [Mb70, DPR61, Sun21] no such algorithm exists for the analogous problem of determining whether there is even a single integral solution to an equation $f(x_1, \ldots, x_n) = 0$ with $f \in \mathbb{Z}[x_1, \ldots, x_n]$ in $n \geq 11$ variables, and it is a conjecture of Baker, Matiyasevich, and Robinson [Sun92, Gas21] that the same should hold when $n \geq 3$, at least with "integral solution" replaced with "positive integral solution". Of course when $n = 1$ the problem is trivial. So the case of points on curves is, it seems, the only interesting one where one has a chance.

Contents.

1 Introduction. **3**

1.1 Outline of the paper. 5

1.2 Acknowledgements. 6

2 A characterization of Galois representations attached to abelian varieties. **7**

3 The main algorithms. **9**

3.1 $T_{\text{Shafarevich}}$. 9

3.2 T_{Mordell}. 11

4 Proofs of Theorems 1.2 and 1.3. **12**

5 Some remarks on computability **14**

5.1 Byte representations. 14

5.2 Abelian varieties and polarizations. 15

5.3 The brute-force search principle. 15

6 Fundamental algorithms for Galois representations. **17**

6.1 Search for number fields. 17

6.2 Faltings' Lemma. 17

6.3 Computability of the property of finite flatness. 18
6.4 Computability of the necessary conditions modulo ℓ^N. 18

7 Fundamental algorithms for abelian varieties over number fields. 20
7.1 Computability of torsion. 20
7.2 Computability of Frobenius traces. 20
7.3 Computability of the conductor. 20
7.4 Computability of the endomorphism ring. 22
7.5 Computability of the set of polarizations of given degree. 23
7.6 Computability of the isomorphism relation. 23
7.7 Computability of the isogeny class. 24
7.8 Computability of a k-th root. 25
7.9 Computability of the Néron model. 25
7.10 Computability of a nonisotrivial family over a given curve. . . . 27
7.11 Computability of an integral model. 28

8 Computability of the set of polarizations of given degree. 29
8.1 Introduction and setup. 29
8.2 Computation of some polarization. 30
8.3 Reduction to computing the set of symmetric endomorphisms of given degree modulo automorphisms. 31
8.4 Reduction to the effectivization of certain cases of Borel–Harish-Chandra. 33
8.5 Characterization of the relevant real orbits. 34
8.5.1 Type I. 34
8.5.2 Type II. 35
8.5.3 Type III. 36
8.5.4 Type IV. 37
8.6 Proof of Proposition 8.4. 38
8.7 Making algorithmic a result of Borel and Harish-Chandra. . . . 38

9 The homology of an abelian variety. 43

10 Algorithmic decomposition of $\mathbb{Q}_\ell$-algebras. 50

11 Algorithmic decomposition of semisimple algebras over number fields. 55

12 Mumford coordinates. 57
12.1 Introduction. 57
12.2 δ-markings. 58
12.3 Let us count the ways (to put Mumford coordinates on an abelian variety). 59
12.4 Representation theory of the group $\mathcal{G}(\delta)$. 61
12.5 Characterizing δ-markings. 62
12.6 Different Mumford coordinates on the same abelian variety. . . 64
12.7 Detecting an abelian variety in a family. 66

1 Introduction.

It is not currently known that the rank of an elliptic curve over $\mathbb{Q}$ is a computable quantity. In other words, it is not currently known that there is a finite-time algorithm, aka Turing machine that terminates on all inputs, that, on input an elliptic curve $E/\mathbb{Q}$, outputs $\operatorname{rank} E(\mathbb{Q})$. However, what is known is that there is a Turing machine that, on input $E/\mathbb{Q}$, outputs $\operatorname{rank} E(\mathbb{Q})$ *if it terminates*, and moreover a standard conjecture[1] implies that said Turing machine indeed terminates on all inputs.

The purpose of this paper is to do the same[2] for the age-old question of computing the rational points on hyperbolic curves. In other words, in this paper we will produce a Turing machine which, on input C/K a smooth projective hyperbolic curve over a number field K, outputs $C(K)$ upon termination, and such that standard conjectures imply that said Turing machine terminates on all inputs.

Let us now describe the algorithm.

Let K be a number field, S a finite set of primes of $\mathcal{O}_K$, and g a positive integer. The Shafarevich conjecture (a theorem of Faltings [Fal83, Satz 6]) asserts that there are only finitely many isomorphism classes of abelian varieties of dimension g over K having good reduction at all primes outside S. Faltings' proof is ineffective: it does not provide a way to show that a list of abelian varieties is complete.

Assuming standard conjectures, we show that there exists an algorithm, terminating in finite time, that takes K, S and g as inputs, and returns a list of all isomorphism classes of abelian varieties of dimension g over K having good reduction outside S.

More precisely, in Section 2 we formulate Conjecture 2.1 and prove that it follows from standard conjectures in arithmetic geometry.

Theorem 1.1. *The Hodge, Tate, and Fontaine-Mazur conjectures imply Conjecture 2.1.*

Then we show that said conjecture has the following ramifications.

Theorem 1.2. *There is a Turing machine $T_{\textit{Shafarevich}}$ with the following properties.*

- *On input (g, K, S, d), with $g, d \in \mathbb{Z}^+$, $K/\mathbb{Q}$ a number field, and S a finite set of places of K, if $T_{\textit{Shafarevich}}$ terminates, then it outputs the finitely many polarized g-dimensional abelian varieties A/K, with polarization of degree d, having good reduction outside S.*
- *Conjecture 2.1 implies that $T_{\textit{Shafarevich}}$ always terminates.*

[1] — namely the finiteness of the corresponding Tate-Shafarevich group $Ш(E/\mathbb{Q})$, or even "just" that $(n, \#|n \cdot Ш(E/\mathbb{Q})|) = 1$ for some $n \in \mathbb{Z}^+$ —

[2] However: **our algorithm is extraordinarily inefficient!** Our goal is only to produce *some* algorithm, whereas the algorithm conjecturally computing the rank of an elliptic curve $E/\mathbb{Q}$ is efficient enough that it is used in practice.

Theorem 1.3. *There is a Turing machine $T_{\textit{Mordell}}$ with the following properties.*

- *On input $(K, C/K)$, with $K/\mathbb{Q}$ a number field and C/K a smooth projective hyperbolic curve, if $T_{\textit{Mordell}}$ terminates, then it outputs $C(K)$.*
- *Conjecture 2.1 implies that $T_{\textit{Mordell}}$ always terminates.*

We expect that both algorithms are too slow for practical use.

The algorithms rely on the following. For the sake of exposition we will be slightly imprecise (e.g. semisimplifications will be omitted, etc.).

- Bounds of Masser–Wüstholz or Raynaud show that, given an abelian variety over K, one can effectively compute all other K-abelian varieties isogenous to it.
- Étale cohomology gives a correspondence between abelian varieties over K, with good reduction outside S, up to isogeny, and certain ℓ-adic representations of the absolute Galois group Gal_K, unramified outside S.
- Using a result of Faltings (a form of the Faltings–Serre method), an ℓ-adic Galois representation is determined by the Frobenius traces at an explicitly computable finite list of primes.
- Conditionally on the Fontaine–Mazur, Hodge, and Tate conjectures, one can give local conditions under which an ℓ-adic Galois representation must come from an abelian variety. (A more precise but less general result of this form was recently proven by Patrikis, Voloch, and Zarhin [PVZ16].)
- These conditions are the limits of conditions modulo ℓ^n for each $n \in \mathbb{Z}^+$. Moreover, given n, the mod-ℓ^n conditions can be checked algorithmically by explicit calculations involving finite flat group schemes.

Just for clarity we state the following immediate consequence of Theorem 1.3.

Corollary 1.4. *Assume the Hodge, Tate, and Fontaine-Mazur conjectures. Then there is a finite-time algorithm which computes the rational points on a given hyperbolic curve over a given number field.*

Let us also note in passing that Theorem 1.3 implies the following.

Theorem 1.5. *There is a Turing machine $T_{\textit{Hilbert}}$ with the following properties.*

- *On input $(\mathfrak{o}, f)$, with $\mathfrak{o} \subseteq \mathfrak{o}_K$ an order in a number field $K/\mathbb{Q}$ and $f \in \mathfrak{o}[x, y]$, if $T_{\textit{Hilbert}}$ terminates, then it outputs $\{(a, b) \in \mathfrak{o} \times \mathfrak{o} : f(a, b) = 0\}$.*
- *On input (K, f), with $K/\mathbb{Q}$ a number field and $f \in K[x, y]$, if $T_{\textit{Hilbert}}$ terminates, then it outputs a finite-length description[3] of $\{(a, b) \in K \times K : f(a, b) = 0\}$.*

[3] If the set is finite then the algorithm outputs it, else the geometric genus of $f = 0$ is at most 1. Thus (the other cases being evident) we need only comment on the case of a smooth curve of genus 1, where a finite-length "description" means (the set being infinite) a K-point along with a "$\mathbb{Z}$-basis" of the group of K-points of the curve's Jacobian.

- *Conjecture 2.1 and the "finiteness-of-$\text{Ш}(E/K)$" conjecture imply that T_{Hilbert} always terminates.*

By the "finiteness-of-$\text{Ш}(E/K)$" conjecture we mean the conjecture that all Tate-Shafarevich groups of elliptic curves over K are finite.

The deduction is immediate so we provide it immediately.

Proof. On input (R, f) with $R \subseteq K$ and $K/\mathbb{Q}$ a number field, write C_f/K (implicitly embedded in $\mathbb{P}^N_{/K}$) for the normalization of the scheme-theoretic closure of $f = 0$ in $\mathbb{P}^2_{/K}$ and g for its genus (which is of course explicitly computable, e.g. for fun via point counting over finite fields). If $g \geq 2$ apply Theorem 1.3. If $g = 1$ and $R =: \mathfrak{o}$ is an order in a number field, apply Baker's lower bound on linear forms in logarithms [Bak66] (see e.g. Baker-Coates [BC70]). If $g = 0$ apply the usual finite-time algorithm depending on the divisor at infinity of C_f (via an explicit form of Hasse-Minkowski or else Baker's effective solution of S-unit equations via his lower bounds on linear forms in logarithms [Bak66]). Else we are in the case $g = 1$ and $R = K$ — then C_f has no K-point if it is not everywhere locally soluble (an explicit finite check by e.g. the Hasse bound and Hensel lifting), else it is everywhere locally soluble and so, choosing an explicit $P \in C_f(\overline{\mathbb{Q}})$ and writing L/K for the Galois closure of its field of definition, one obtains that C_f induces a class $\alpha \in \mathrm{Sel}_{[L:K]}(E_f/K)$ with $E_f := \mathrm{Jac}\, C_f$. By hypothesis the usual compute-$\mathrm{Sel}_N(E_f/K)$-by-day / brute-force-search-to-lower-bound-$\mathrm{rank}\ E_f(K)$-by-night algorithm terminates with a "$\mathbb{Z}$-basis" of $E_f(K)$, whence in finite time we determine whether or not α lies in the image of $E_f(K)/[L : K] \to \mathrm{Sel}_{[L:K]}(E_f/K)$ — if not then C_f has no K-points, while if so a brute-force search will find a K-point $P \in C_f(K)$ aka a K-isomorphism $C_f \simeq E_f$, and we have already found a "$\mathbb{Z}$-basis" of $E_f(K)$. □

1.1 Outline of the paper.

In Section 2, we state the conjecture (Conjecture 2.1) on which our conditional results rely, and we prove that Conjecture 2.1 is a consequence of the Hodge, Tate, and Fontaine–Mazur conjectures.

We state the main algorithms in Sections 3.1 and 3.2; Section 4 contains a proof that the algorithms achieve what we claim.

In Section 5 we discuss how to work with various mathematical objects (number fields, abelian varieties, endomorphisms, etc.) at the level of (finite) byte representations, and the need to approximate objects that cannot be represented by finite bit strings (e.g. complex numbers, varieties and morphisms over $\mathbb{C}$, and ℓ-adic Galois representations). We also discuss brute-force search as a technique for finding various algebro-geometric objects.

The rest of the paper explains in some detail how to perform various calculations that are used in the main algorithms. We expect that a significant proportion of this material is known to the experts; for lack of a suitable reference, we wrote the material in some level of detail. Sections 6 and 7 present a large number of algorithms for fundamental calculations involving Galois representations and abelian varieties. In Section 8, we explain how to find all polarizations (up to isomorphism) of given degree on a given abelian variety. In Section 9 we show how to compute the singular homology of an abelian variety in terms of differentials and the complex-analytic uniformization; this is needed for various exact calculations involving homology, endomorphisms, and polarizations. Sections 10 and 11 contain algorithms for working with semisimple algebras, which we will apply to the endomorphism ring of an abelian variety. We conclude with Section 12, where we explain Mumford's parametrization of a certain moduli space of abelian varieties with level structure.

1.2 Acknowledgements.

We would like to thank Manjul Bhargava, Frank Calegari, Ignacio Darago, Matt Emerton, Hao Lee, David Benjamin Lim, Bjorn Poonen, Michael Stoll, Andrew Sutherland, Akshay Venkatesh, John Voight, and Felipe Voloch for helpful conversations.

LA thanks the Society of Fellows. BL would like to acknowledge support from a grant from the US National Science Foundation (2101985).

Work on this paper was performed at Schloss Schney, the Mathematical Sciences Research Institute, the University of Wisconsin–Madison, Sierra-at-Tahoe, and Kirkwood. We are grateful to these institutions for their hospitality.

2 A characterization of Galois representations attached to abelian varieties.

The purpose of this section is to state Conjecture 2.1 and to prove (Theorem 1.1) that Conjecture 2.1 is a consequence of the Hodge, Tate, and Fontaine–Mazur conjectures. Note that Theorem 1.1 is closely related to the main result of [PVZ16].

Conjecture 2.1. *Let $K/\mathbb{Q}$ be a number field. Let*

$$\rho\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$$

be a Galois representation such that

- *ρ is unramified outside S and primes above (ℓ),*
- *for every prime $\mathfrak{p} \nmid (\ell)$ of K not in S, $\mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p})) \in \mathbb{Z}$,*
- *and, at each place of K above ℓ, the representation ρ is de Rham, with Hodge–Tate weights 0 and 1, each appearing with multiplicity g.*

Then there exists a Galois extension L/K, a CM field E, a degree one prime $\lambda|(\ell)$ of E, and an abelian variety B/L admitting $\mathfrak{o}_E \hookrightarrow \mathrm{End}_L(B)$ with good reduction outside S and primes above ℓ such that $B \sim_L B^\sigma$ for all $\sigma \in \mathrm{Gal}(L/K)$ and moreover the $E_\lambda \cong \mathbb{Q}_\ell$-adic rational Tate module $V_\lambda(B) := T_\lambda(B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is isomorphic to ρ as a $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-representation:

$$V_\lambda(B) \cong \rho.$$

In particular letting $A := \mathrm{Res}^L_K(B)$ we conclude that $V_\ell(A) \cong \rho^{\oplus[E:\mathbb{Q}]\cdot[L:K]}$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-representations.

Standard examples of abelian surfaces with quaternionic multiplication demonstrate that we cannot hope to take the above $E = \mathbb{Q}$ in general (see e.g. Section 4 of [PVZ16]).

Now let us prove Theorem 1.1.

Proof of Theorem 1.1. By Fontaine-Mazur ([FM95, Conjecture 1]), there is a smooth projective variety X/K and $i, j \in \mathbb{Z}$ such that ρ is a subquotient of $H^i_{\text{ét.}}(X/\overline{\mathbb{Q}}, \mathbb{Q}_\ell)(j)$. By the Hodge and Tate conjectures [Moo19], $H^i_{\text{ét.}}(X/\overline{\mathbb{Q}}, \mathbb{Q}_\ell)(j)$ is a semisimple $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-representation, and so ρ is in fact a summand thereof. Write $\pi \in \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}(\overline{\mathbb{Q}}/K)]}(H^i_{\text{ét.}}(X/\overline{\mathbb{Q}}, \mathbb{Q}_\ell)(j))$ for the corresponding projector. Let $M := H^i(X)(j)$, a pure motive with $\mathbb{Q}$-coefficients over K — thus $\mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}(\overline{\mathbb{Q}}/K)]}(H^i_{\text{ét.}}(X/\overline{\mathbb{Q}}, \mathbb{Q}_\ell)(j)) \simeq \mathrm{End}_K(M) \otimes_\mathbb{Q} \mathbb{Q}_\ell$. Thus $\mathrm{End}_K(M)$ is a semisimple $\mathbb{Q}$-algebra, whence it splits over $\overline{\mathbb{Q}}$. In other words π is in the image of $\mathrm{End}_K(M) \otimes_\mathbb{Q} \overline{\mathbb{Q}} \hookrightarrow \mathrm{End}_K(M) \otimes_\mathbb{Q} \overline{\mathbb{Q}}_\ell \simeq \mathrm{End}_{\overline{\mathbb{Q}}_\ell[\mathrm{Gal}(\overline{\mathbb{Q}}/K)]}(H^i_{\text{ét.}}(X/\overline{\mathbb{Q}}, \mathbb{Q}_\ell)(j))$, where we have implicitly chosen a particular embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Thus, because semisimple algebras over $\mathbb{Q}$ all split over the maximal CM extension of $\mathbb{Q}$, by the Tate conjecture it follows that there is a finite set $\mathscr{C}$ of $(\dim X)$-dimensional correspondences $C \subseteq X \times X$ and

$\alpha_C \in \overline{\mathbb{Q}}$ lying in a CM field such that $\pi = \sum_{C \in \mathscr{C}} \alpha_C \cdot C_*$. Let $E := \mathbb{Q}(\{\alpha_C : C \in \mathscr{C}\})$, a (totally real or imaginary CM) number field because $\mathscr{C}$ is finite, equipped with a choice of embedding $E \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ (and thus a chosen $\lambda \mid (\ell)$) from our preferred $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ from before.

We conclude that π is in the image of $\mathrm{End}_K(M) \otimes_{\mathbb{Q}} E$, and so $\rho \otimes_{\mathbb{Q}} E$ is the λ-adic realization of an object in the category of pure motives with E-coefficients over K. On restricting coefficients from E to $\mathbb{Q}$ we conclude that $\mathrm{Res}^E_{\mathbb{Q}}(\rho \otimes_{\mathbb{Q}} E)$ is the ℓ-adic realization of an object $\widetilde{M}$ in the category of pure motives with $\mathbb{Q}$-coefficients over K. But because ρ has rational Frobenius traces it follows from Chebotarev that $\mathrm{Res}^E_{\mathbb{Q}}(\rho \otimes_{\mathbb{Q}} E) \cong \rho^{\oplus [E:\mathbb{Q}]}$.

So $\rho^{\oplus [E:\mathbb{Q}]}$ is the ℓ-adic realization of $\widetilde{M}$. Now choose embeddings $K \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Then the $\mathbb{Q}$-Hodge structure corresponding to (aka Betti realization of) $\widetilde{M}$ has weights $\{\underbrace{(1,0), \ldots, (1,0)}_{g \cdot [E:\mathbb{Q}]}, \underbrace{(0,1), \ldots, (0,1)}_{g \cdot [E:\mathbb{Q}]}\}$ by hypothesis on the weights of ρ. Moreover it is polarizable by our construction of $\widetilde{M}$ from the smooth projective X/K. It follows by Riemann that there is an isogeny class of abelian varieties over $\mathbb{C}$ with said $\mathbb{Q}$-Hodge structure, and it follows from the Hodge conjecture (applied to a product of one such abelian variety with a power of X) that said isogeny class is stable under the action of $\mathrm{Aut}(\mathbb{C}/\overline{\mathbb{Q}})$, whence it is an isogeny class of abelian varieties over $\overline{\mathbb{Q}}$.

Let $B/\overline{\mathbb{Q}}$ be one of the abelian varieties in said isogeny class, and $L/\mathbb{Q}$ a number field over which B is defined (with an implicitly chosen embedding $L \hookrightarrow \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$). Thus the $\mathbb{Q}$-Hodge structure of B matches the Betti realization of $\widetilde{M}$. By enlarging $L/\mathbb{Q}$ if necessary, without loss of generality we may assume that $L/\mathbb{Q}$ is Galois and that the Hodge class providing the isomorphism between the $\mathbb{Q}$-Hodge structure of B and that of $\widetilde{M}$ is invariant under $\mathrm{Aut}(\mathbb{C}/L)$ — note that it then follows that $E \hookrightarrow \mathrm{End}^0_L(B)$, and, by taking a Serre tensor product if necessary, without loss of generality that $\mathfrak{o}_E \hookrightarrow \mathrm{End}_L(B)$. By transporting said Hodge class along the comparison isomorphism between Betti and ℓ-adic cohomology we find that $V_\ell(B)$ is isomorphic to the ℓ-adic realization of $\widetilde{M}$ (aka $\rho^{\oplus [E:\mathbb{Q}]}$) as $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$-representations. Note that this immediately implies that $B \sim_L B^\sigma$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Let then $A := \mathrm{Res}^L_K(B)$. It follows that $V_\ell(A) \cong \rho^{\oplus [E:\mathbb{Q}] \cdot [L:K]}$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-representations, so we are done. □

3 The main algorithms.

In this section we present the two main algorithms: $T_{\text{Shafarevich}}$, which finds all abelian varieties of dimension g over a number field K, having good reduction outside S, and equipped with a polarization of degree d; and T_{Mordell}, which finds all rational points on a curve of genus at least 2 over a number field K. The algorithms make use of subroutines which are given in later sections.

3.1 $T_{\textbf{Shafarevich}}$.

Algorithm 3.1 ($T_{\text{Shafarevich}}$)**.** *On input (g, K, S, d),*

1. *Check that the input specifies $g, d \in \mathbb{Z}^+$, a number field $K/\mathbb{Q}$, and a finite set S of primes of K.*
2. *Initialize* 🎁 $:= \varnothing$.

   (This will be the output set of abelian varieties.)
3. *Choose a prime $\ell \in \mathbb{Z}^+$ not dividing $\prod_{\mathfrak{p} \in S} \operatorname{Nm} \mathfrak{p}$.*

   (We're going to work with ℓ-adic Galois representations.)
4. *Follow the proof of Lemma 6.3 on input (g, K, S, ℓ) to compute T as guaranteed in Lemma 6.3.*

   (T is a finite set of primes of K such that a semisimple rank-$2g$ Galois representation is determined by its Frobenius traces at primes in T.)
5. *Let $C := \left\{ (a_{\mathfrak{p}})_{\mathfrak{p} \in T} : a_{\mathfrak{p}} \in \mathbb{Z}, |a_{\mathfrak{p}}| \leq 2g \cdot \sqrt{\operatorname{Nm} \mathfrak{p}} \right\}$, and initialize Ç $= C$.*

   (This C is a list of all possible tuples of Frobenius traces, at primes in T, of a Galois representation coming from an abelian variety. Over the course of the algorithm we will remove elements from Ç; Ç is the set of elements of C that "have not been processed yet.")
6. *Initialize $k_{max} := 1, H := 1, N := 1$.*
7. *While Ç $\neq \varnothing$:*
   - *(a) Increment $k_{max} \mapsto k_{max} + 1, H \mapsto H + 1, N \mapsto N + 1$.*

     (This loop is going to be executed over increasing tuples (k_{max}, H, N) such that N is sufficiently large with respect to k_{max} (see step 7b). If the loop were allowed to run forever, k_{max}, H, N would go to infinity.)
   - *(b) For all $k \leq k_{max}$, follow the proof of Lemma 6.3 on input $(k \cdot g, K, S, \ell)$, and let $\widetilde{T}$ be the union of the outputs over all $k \leq k_{max}$. Increase N if necessary to ensure that all primes $\mathfrak{p} \in \widetilde{T}$ satisfy $\operatorname{Nm} \mathfrak{p} < \frac{\ell^{2N}}{16g^2}$.*

     (A rank-kg Galois representation is determined by its Frobenius traces at all primes in $\widetilde{T}$; here we take N large enough to ensure that if the representation comes from an abelian variety, those Frobenius traces are determined by their value modulo ℓ^N.)

(c) *Let* $\text{Ç}_N := \varnothing$.

(This will be a list of all possible tuples of Frobenius traces at primes in the extended set $\widetilde{T}$*. Each tuple in* $(a_\mathfrak{p})_{\mathfrak{p}\in T} \in \text{Ç}$ *will extend to at most one tuple* $(a_\mathfrak{p})_{\mathfrak{p}\in\widetilde{T}} \in \text{Ç}_N$*.)*

(d) *For each* $(a_\mathfrak{p})_{\mathfrak{p}\in T} \in \text{Ç}$*, do the following.*

  i. *Follow the proof of Theorem 6.5 on input* $(g, K, S, T, (a_\mathfrak{p})_{\mathfrak{p}\in T}, \ell, N)$*, to compute* $(\Phi, (a_\mathfrak{p})_{\mathfrak{p}\in\widetilde{T}})$ *as guaranteed in Theorem 6.5.*

  (In other words: the trace tuple $(a_\mathfrak{p})_{\mathfrak{p}\in T}$ *comes from at most one good Galois representation; we attempt to lift that Galois representation to a mod-*ℓ^N *representation with good Frobenius traces at all* $\mathfrak{p} \in \widetilde{T}$*.*

  If we succeed, $(a_\mathfrak{p})_{\mathfrak{p}\in\widetilde{T}}$ *is the (necessarily unique) tuple of Frobenius traces at all* $\mathfrak{p} \in \widetilde{T}$*, though there may be multiple mod-*ℓ^N *Galois representations* $\rho \in \Phi$ *having that same trace tuple.)*

  ii. *If* $\Phi = \varnothing$ *then remove* $(a_\mathfrak{p})_{\mathfrak{p}\in T}$ *from Ç.*

  (If the Galois representation does not lift mod ℓ^N*, or if the lift does not satisfy the Weil bound at all primes in* $\widetilde{T}$*, we remove the tuple* $(a_\mathfrak{p})_{\mathfrak{p}\in T}$ *from consideration.)*

  iii. *If* $\Phi \neq \varnothing$*, add* $(a_\mathfrak{p})_{\mathfrak{p}\in\widetilde{T}}$ *to* Ç_N*.*

  (If the Galois representation lifts, add the extended trace tuple to Ç_N*. At the end of Step 7d,* Ç_N *will contain one extended trace tuple for each trace tuple in Ç.)*

(e) *Perform a brute-force search, with parameter* H *(§5.3 and Principle 5.1), for abelian varieties* A/K *in Mumford form (Definition 12.7), of dimension* $\dim A \leq k \cdot g$ *with* $g \mid \dim A$*, which are of good reduction outside* S*. Let* Ъ_H *denote the resulting finite set of abelian varieties.*

Note that Lemma 12.8 gives an algorithmically verifiable condition to test whether A/K *is an abelian variety in Mumford form, while Theorem 7.4 allows one to test whether* A *is of good reduction outside* S*.*

(f) *For each* $A \in \text{Ъ}_H$*, do the following.*

  i. *Let* $(a_\mathfrak{p})_{\mathfrak{p}\in\widetilde{T}} \in \text{Ç}_N$ *be the unique element such that* $\operatorname{tr}(\rho_{A,\ell}(\operatorname{Frob}_\mathfrak{p})) \equiv \binom{\dim A}{g} \cdot a_\mathfrak{p} \pmod{\ell^N}$ *for all* $\mathfrak{p} \in \widetilde{T}$*. (Use Lemma 7.2 to compute Frobenius traces on* A*.)*

  ii. *Follow the proofs of Proposition 7.15 and Theorem 7.14 to determine whether or not there is a* B/K *with* $\dim B = g$ *such that* $A \sim_K B^{\times k}$*, and to compute one such* B/K *if one exists.*

  iii. *If there is such a* B/K*, follow the proof of Theorem 7.14 to compute all polarized abelian varieties* $(B', \mathcal{L})/K$ *such that* $B' \sim_K B$ *and* $\mathcal{L}$ *is a polarization of degree* d *on* B'*, and add all such* $(B', \mathcal{L})$ *to* 🎁*.*

  (In other words: using the Masser–Wüstholz isogeny estimates ([MW93], [Bos96]), determine all abelian varieties in the isogeny class of B*.)*

  iv. *Remove* $(a_\mathfrak{p})_{\mathfrak{p}\in T}$ *from Ç if it has not been removed already.*

(At this point we have found a single abelian variety A whose Galois representation "explains" the tuple $(a_{\mathfrak{p}})_{\mathfrak{p}\in T}$, and used A to determine all abelian varieties with these Frobenius traces; we now remove the tuple $(a_{\mathfrak{p}})_{\mathfrak{p}\in T}$ from consideration.)

8. *Output* 🎁.

3.2 $T_{\textbf{Mordell}}$.

Algorithm 3.2 (T_{Mordell})**.** *On input $(K, C/K)$,*

1. *Let* ڭ $:= \varnothing$.
2. *Follow the proof of Theorem 7.18 on input $(K, C/K)$ to compute a nonisotrivial family $A \to C$ of abelian varieties parametrized by C (with some projective embedding).*

   Let d be the degree of the polarization of the given projective embedding of A.
3. *Apply Theorem 7.19 to $(K, C, \mathcal{A} \to C)$ to compute a finite set S of primes of K, such that for every $x \in C(K)$, the fiber $\mathcal{A}_x$ has good reduction at all primes outside of S.*
4. *Let g be the relative dimension of the abelian scheme $\mathcal{A} \to C$, and apply Algorithm 3.1 on input (g, K, S) to determine (up to isomorphism) the set Σ of all abelian varieties A of dimension g over K having good reduction outside S.*
5. *For each abelian variety $A \in \Sigma$:*
   - (a) *Run the algorithm of Theorem 7.8 to determine all polarizations $\mathcal{L}$ of degree d on A.*
   - (b) *For each such $\mathcal{L}$:*
     - i. *Apply Theorem 12.15 to determine all $s \in C(\overline{\mathbb{Q}})$ such that $\mathcal{A}_s \cong A$ as polarized abelian varieties over $\overline{\mathbb{Q}}$.*
     - ii. *For each such s:*
       - (α) *Determine whether $s \in C(K)$. If so, add s to the set* ڭ.
6. *Return* ڭ.

4 Proofs of Theorems 1.2 and 1.3.

We now prove that the two algorithms just presented achieve what we claim.

Proof of Theorem 1.2. We claim that the Turing machine specified in Section 3.1 has the desired properties.

First, suppose it terminates on input (g, K, S). We claim that its output is then exactly the set of B/K with $\dim B = g$ which have good reduction outside S.

So let $\widetilde{B}/K$ be in the output, and let us show that it has good reduction outside S. Because, in the notation of Algorithm 3.1, $\widetilde{B}^{\times k} \sim_K A$ with $A \in$ Ъ$_N$ for some $N \in \mathbb{Z}^+$ and each A/K has good reduction outside S, it follows that $\widetilde{B}/K$ also has good reduction outside S.

Now let $\widetilde{B}/K$ with $\dim \widetilde{B} = g$ have good reduction outside S, and let us show that it is the output. Certainly, in the notation of Algorithm 3.1, $(\mathrm{tr}(\rho_{B,\ell}(\mathrm{Frob}_\mathfrak{p}))_{\mathfrak{p}\in T} \in$ Ç, and it is never removed in Step 7.(c).ii because $\rho_{\widetilde{B},\ell} \pmod{\ell^N} \in \Phi$ as defined in Step $7.(c).i$. So, because $T_{\text{Shafarevich}}$ terminates on input (g, K, S), it must be removed in Step $7.(f).iv$, which is to say that at the corresponding value of N there is an $A \in$ Ъ such that $\mathrm{tr}(\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})) = k \cdot \mathrm{tr}(\rho_{\widetilde{B},\ell}(\mathrm{Frob}_\mathfrak{p}))$ for all $\mathfrak{p} \in \widetilde{T}$, whence by Lemma 6.3 $A \sim_K \widetilde{B}^{\times k}$. Since $\widetilde{B}^{\times k} \sim_K B^{\times k}$ implies that $\widetilde{B} \sim_K B$, it follows that $\widetilde{B}/K$ is then added to the output in Step 7.(f).iv, so indeed it occurs in the output as desired.

So the output is correct provided $T_{\text{Shafarevich}}$ terminates.

Now let us show that Conjecture 2.1 implies that $T_{\text{Shafarevich}}$ always terminates.

What we must show is that each $(a_\mathfrak{p})_{\mathfrak{p}\in T} \in$ Ç as computed in Step 5 is eventually removed, or in other words that each $(a_\mathfrak{p})_{\mathfrak{p}\in T} \in$ Ç which is never removed in Step 7.(c).ii is eventually removed in Step 7.(f).iv.

So let $(a_\mathfrak{p})_{\mathfrak{p}\in T} \in$ Ç be such that it is never removed in Step 7.(c).ii. Thus for all $N \in \mathbb{Z}^+$ there is a $\rho_N : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^N)$ such that

- ρ_N is unramified outside S and the primes above (ℓ),
- for all $\mathfrak{p} \in T$, $\mathrm{tr}(\rho_N(\mathrm{Frob}_\mathfrak{p})) \equiv a_\mathfrak{p} \pmod{\ell^N}$,
- $\det \rho \equiv \chi_\ell^g \pmod{\ell^N}$,
- for all $\lambda \mid (\ell)$, the Galois module corresponding to ρ_N prolongs to a finite flat group scheme over $\mathfrak{o}_{K,\lambda}$,
- and, for all primes $\mathfrak{p} \subseteq \mathfrak{o}_K$ not in S and prime to (ℓ) with $\mathrm{Nm}\,\mathfrak{p} < \frac{\ell^{2N}}{16g^2}$, there is a unique $a_\mathfrak{p} \in \mathbb{Z}$ with $|a_\mathfrak{p}| \leq 2g \cdot \sqrt{\mathrm{Nm}\,\mathfrak{p}}$ and such that $\mathrm{tr}(\rho_N(\mathrm{Frob}_\mathfrak{p})) \equiv a_\mathfrak{p} \pmod{\ell^N}$.

By Kőnig's Lemma[4] it follows that we may assume without loss of generality that $\rho_{N+1} \pmod{\ell^N} = \rho_N$. Let then $\rho := \varprojlim \rho_N$. Thus $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ is such that

- ρ is unramified outside S and the primes above (ℓ),
- for all $\mathfrak{p} \in T$, $\mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p})) = a_\mathfrak{p}$,
- $\det \rho = \chi_\ell^g$,
- for all $\lambda \mid (\ell)$, the ℓ-divisible group corresponding to ρ prolongs to an ℓ-divisible group over $\mathfrak{o}_{K,\lambda}$,
- and, for all $\mathfrak{p}$ not in S and prime to (ℓ), $\mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p})) \in \mathbb{Z}$.

The first property amounts to the statement that ρ factors through a map $G_{K,S,\ell} \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. The fourth property amounts to the statement that the restriction of ρ to an inertia group above (ℓ) is crystalline with all Hodge-Tate weights in $\{0, 1\}$, from which, via $\det \rho = \chi_\ell^g$, we deduce the second hypothesis of Conjecture 2.1. The first hypothesis of Conjecture 2.1 is of course the fifth property.

Therefore by Conjecture 2.1 it follows that there is an abelian variety A/K with good reduction outside S such that $\rho_{A,\ell} \cong \rho^{\oplus \frac{\dim A}{g}}$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-representations. Therefore it must be the case that $(a_\mathfrak{p})_{\mathfrak{p} \in T}$ is eventually selected in Step 7.(f).i. But then it is removed in Step 7.(f).iv, as desired. □

Proof of Theorem 1.3. Given Theorem 1.2 the second part of Theorem 1.3 is evident. So let us prove the first part.

Thus suppose T_{Mordell} terminates on input $(K, C/K)$. Because Step 4.(b) only adds K-points of C to the output it follows that the output is a subset of $C(K)$. So let $P \in C(K)$, whence our claim is that P is in the output.

But because $\mathcal{C}/\mathfrak{o}_{K,S}$ is proper, $\mathcal{C}(\mathfrak{o}_{K,S}) = \mathcal{C}(K) = C(K)$, so that the fibre of $\mathcal{A} \to \mathcal{C}$ over $P \in C(K) = \mathcal{C}(\mathfrak{o}_{K,S})$ is an $\mathfrak{o}_{K,S}$-integral model of a g-dimensional abelian variety A_P/K with good reduction outside S. But said abelian variety must then occur in the output of $T_{\text{Shafarevich}}$ on input (g, K, S), whence the fibre of the family $(\mathcal{A} \to \mathcal{C}, \ldots)$ of Mumford data above $P \in C(K) = \mathcal{C}(\mathfrak{o}_{K,S})$ must occur in $\mathcal{E}$ when computed in the Step 4.(a) corresponding to A_P/K. Hence $P \in C(K)$ must be added to the output in the corresponding Step 4.(b), and we conclude. □

[4] (There are only finitely many representations $\mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^N)$ which are unramified outside S and the primes above (ℓ) by Hermite-Minkowski.)

5 Some remarks on computability

5.1 Byte representations.

In this paper we consider various types of arithmetic-geometric object that can be represented by a finite byte string. For example:

- an element of a number field K,
- a complex embedding of K,
- a projective variety over K,
- a morphism of projective varieties over K,

and so forth.

Any computer implementation will require some sort of standardized format for the byte string representing each such type of object that arises in the algorithm. Where it is clear that such a format can be chosen (in the cases above, for instance), we will not specify the format to be used.

On the other hand, certain types of objects, by nature, do *not* in general admit descriptions by finite byte strings. For example:

- a complex number
- a variety over $\mathbb{C}$
- an ℓ-adic Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$.

One cannot ask to compute such an object exactly, only to approximate it to some desired precision.

The case of Galois representations deserves special mention. An ℓ-adic Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ is an inverse limit of finite (mod-ℓ^N) representations

$$\mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^N).$$

Any such mod-ℓ^N representation factors through some finite quotient group $\mathrm{Gal}(L/K)$, with L/K some finite extension. It follows that a mod-ℓ^N Galois representation can be represented by a finite byte string as follows: First, specify the number field L and give names to the finitely many elements of the Galois group $\mathrm{Gal}(L/K)$; then specify the function

$$\mathrm{Gal}(L/K) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^N)$$

(which is now a function from one finite set to another). Our study of Galois representations is made possible by this "ℓ-adic approximation" of ℓ-adic representations by finitary objects.

5.2 Abelian varieties and polarizations.

Throughout the paper, an abelian variety over a number field K will be presented as a projective variety A over K, plus the usual structure morphisms (multiplication $A \times A \to A$, inverse $A \to A$ and identity $\operatorname{Spec} K \to A$). Any such object is automatically a polarized abelian variety as well – simply take the polarization to be the Neron–Severi class of $\mathcal{O}(1)$ in the given projective embedding.

For explicit computation with polarizations (e.g. as in Section 8), note that we can compute the Chern class of a polarization in terms of an integral basis for $H^1(A)$, by Lemma 9.11.

5.3 The brute-force search principle.

We will use the "brute-force search principle" repeatedly.

Principle 5.1. *Suppose we wish to find an O (some type of object) satisfying property P. Assume:*

- *Objects O are represented by finite byte strings.*
- *Given any finite byte string, one can determine algorithmically whether it represents an object O satisfying property P (assuming formatting conventions have been chosen as in §5.1).*
- *At least one object O with property P is known to exist.*

Then one can find an object O with property P, by the following silly algorithm: iterate over all finite byte strings (in increasing order of length, say). Test each string to determine whether it represents the object sought, and halt when a string passes the test.

In some situations we will say "run brute-force search with parameter H" (for some positive integer H) to mean "search over all byte strings of length at most H". This has the following features:

- For any fixed H, the brute-force search with parameter H will terminate in finite time (though it may or may not find the object sought).
- If the search is run with larger and larger values of H, eventually (for sufficiently large H) the search will find the object.

This is useful in "day-and-night searches", where we wish to interleave a brute-force search with some other type of calculation.

See, for example, Step 7 of Algorithm 3.1, where a search for abelian varieties "with parameter H" is interleaved with a search for Galois representations. (The search for Galois representations will give an upper bound on the number of abelian varieties that can arise.)

Some other places brute-force search is used:

- Lemma 6.3, to find a set of primes satisfying the conclusion of Chebotarev's density theorem.
- Lemma 7.1, to find the N-torsion points on an abelian variety.
- In computing the endomorphism ring of an abelian variety (Lemma 7.6), to find endomorphisms.
- Theorem 7.18, to find a nonisotrivial family of abelian varieties over a given curve as base.
- Lemma 12.13, to find a Mumford form for a given abelian scheme.

Remark 5.2. *In several of the above cases, there are more efficient algorithms than brute-force search. We do not attempt to describe them.*

Many of these algorithmic questions have been addressed in the literature; we hope this work will inspire further progress on explicit computational questions in arithmetic geometry.

6 Fundamental algorithms for Galois representations.

6.1 Search for number fields.

Lemma 6.1. *There is a finite-time algorithm which, on input (d, K, S) with $d \in \mathbb{Z}^+$, $K/\mathbb{Q}$ a number field, and S a finite set of places of K, outputs the set of extensions of K of degree at most d which are unramified at all primes outside S.*

Proof. The ramification hypothesis implies that the relative discriminant of L/K is bounded by a constant D that can be effectively computed.

Given the discriminant bound, one can find all such field extensions L/K by a targeted Hunter search [Coh00, §9.3] □

6.2 Faltings' Lemma.

Definition 6.2. *Let $d \in \mathbb{Z}^+$, and let ℓ be a prime. Let $K/\mathbb{Q}$ be a number field and S a finite set of places of K.*

Let T be a set of primes of K. We say that T determines trace functions *(with parameters (K, S, d, ℓ)) if it satisfies the following condition:*

> *Let R be either $\mathbb{Q}_\ell$, $\mathbb{Z}_\ell$, or $\mathbb{Z}/\ell^N$ for some N. If two Galois representations*
>
> $$\rho, \rho' \colon \operatorname{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_d(R))$$
>
> *satisfy* $\operatorname{tr}(\rho(\mathrm{Frob}_\mathfrak{p})) = \operatorname{tr}(\rho'(\mathrm{Frob}_\mathfrak{p}))$ *for all* $\mathfrak{p} \in T$, *then* $\operatorname{tr} \circ \rho = \operatorname{tr} \circ \rho'$ *on* $\operatorname{Gal}(\overline{\mathbb{Q}}/K)$.

Lemma 6.3 (Faltings, cf. e.g. [Alp20, Alp21])**.** *Let $d \in \mathbb{Z}^+$. Let $K/\mathbb{Q}$ be a number field and S a finite set of places of K. One can compute a finite set $T_{K,S,d,\ell}$ of primes of K that are prime to ℓ, which is disjoint from S, such that for all Galois extensions L/K of degree $[L : K] \leq \ell^{4d^2}$ that are unramified outside S and the primes dividing ℓ, the map $T_{K,S,d,\ell} \to \operatorname{Gal}(L/K)/conj.$ via $\mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p}$ is surjective.*

Such a T determines trace functions with parameters (K, S, d, ℓ).

Proof. The desired set of primes is guaranteed to exist by the Chebotarev density theorem, so they it be found by brute-force search (see Section 5.3).

(Alternatively, the usual explicit form of the Chebotarev density theorem [Cb23a, Cb23b] gives[5] an explicit $T_{K,S,d,\ell}$ satisfying the above — thus e.g. we may take $T_{K,S,d,\ell}$ satisfying the above and so that all $\mathfrak{p} \in T_{K,S,d,\ell}$ satisfy $\mathrm{Nm}\ \mathfrak{p} \ll_{K,S,d,N} 1$, where the implied constant is explicit.)

This $T_{K,S,d,\ell}$ has the required properties by [Fal83, proof of Satz 5]; we recall the argument here.

We may assume the coefficient ring R is either $\mathbb{Z}_\ell$ or $\mathbb{Z}/\ell^N$.

[5] Each such Galois extension L/K has explicitly bounded discriminant, and Frobenii of norm bounded in terms of said discriminant represent all conjugacy classes of $\operatorname{Gal}(L/K)$ — see e.g. Theorem 1.1 of Lagarias-Montgomery-Odlyzko's [LMO79] for one such bound.

It suffices to show that the R-span of $\mathrm{im}(\rho \oplus \rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_d(R)^{\times 2})$ inside $M_d(R)^{\times 2}$ is in fact spanned by $\bigcup_{\mathfrak{p} \in T_{K,S,d,N}} (\rho \oplus \rho')(\mathrm{Frob}_\mathfrak{p})$, where $\mathrm{Frob}_\mathfrak{p} \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is the Frobenius conjugacy class of $\mathfrak{p}$. To do this one uses Nakayama to reduce mod ℓ, after which it follows from the hypothesis on $T_{K,S,d,N}$. □

6.3 Computability of the property of finite flatness.

Lemma 6.4. *There is a finite-time algorithm that, on input $(d, K, \lambda, \ell, N, \rho)$ with $K/\mathbb{Q}$ a number field, $\lambda \subseteq \mathfrak{o}_K$ a prime of K, $\ell \in \mathbb{Z}^+$ a prime with $\lambda \mid (\ell)$, $N \in \mathbb{Z}^+$, and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_d(\mathbb{Z}/\ell^N)$ continuous, returns true if and only if the Galois module corresponding to ρ prolongs to a finite flat group scheme over $\mathfrak{o}_{K,\lambda}$.*

Proof. Write $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/K_\lambda) \simeq D_\lambda \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for a decomposition group at λ. The restriction $\rho|_{D_\lambda}$ describes a group scheme $\mathrm{Spec}\, A$ over the field K_λ, where A is a Hopf algebra. To say that $\rho|_{D_\lambda}$ comes from a finite flat group scheme means that there is a Hopf algebra $\mathcal{O}_A \subseteq A$ over $\mathfrak{o}_{K,\lambda}$ such that $\mathcal{O}_A \otimes_{\mathfrak{o}_{K,\lambda}} K_\lambda \to A$ is an isomorphism.

More precisely, A is a K_λ-vector space equipped with a multiplication map $A \otimes A \to A$ and a comultiplication $A \to A \otimes A$, subject to various axioms. By duality, the comultiplication map defines a multiplication map (i.e. a ring structure) on $A^\vee$, the K_λ-linear dual of A. We need to determine whether there exists an $\mathfrak{o}_{K,\lambda}$-lattice $\mathcal{O}_A \subseteq A$, such that $\mathcal{O}_A$ is stable under multiplication, and its dual is stable under comultiplication.

We can compute A concretely as follows. The representation ρ is a permutation representation of the Galois group on the finite set $(\mathbb{Z}/\ell^N)^{\oplus d}$; by Galois theory, it corresponds to the K-algebra $A = \mathrm{Hom}_{D_\lambda}((\mathbb{Z}/\ell^N)^{\oplus d}, \overline{\mathbb{Q}}_\ell)$. Writing $L := \overline{\mathbb{Q}}_\lambda^{\ker \rho|_{D_\lambda}}$, we have $A = \mathrm{Hom}_{\mathrm{Gal}(L/K_\lambda)}((\mathbb{Z}/\ell^N)^{\oplus d}, L)$; this allows us to compute A (with its multiplication law) explicitly, working only with finite-dimensional K_λ-vector spaces.

The natural identification $A^\vee \otimes_{K_\lambda} L = L[(\mathbb{Z}/\ell^N)^{\oplus d}]$ gives a multiplication law on $A^\vee \otimes_{K_\lambda} L$, which restricts to a multiplication law $A^\vee \times A^\vee \to A^\vee$.

Now let $\mathcal{O}_{\max}$ be the maximal order of A, and let $\mathcal{O}_{\min}$ be the dual of the maximal order of $A^\vee$. We can compute both maximal orders by Lemma 10.5.

We know that any Hopf algebra $\mathcal{O}_A \subseteq A$ must satisfy $\mathcal{O}_{\min} \subseteq \mathcal{O}_A \subseteq \mathcal{O}_{\max}$. Because the quotient $\mathcal{O}_{\max}/\mathcal{O}_{\min}$ is finite, we need only test the finitely many intermediate lattices $\mathcal{O}_A$ to determine whether any is stable under both multiplication and comultiplication. □

6.4 Computability of the necessary conditions modulo ℓ^N.

Theorem 6.5. *There is a finite-time algorithm that, on input $(K, S, g, \ell, T, (a_\mathfrak{p})_{\mathfrak{p} \in T}, \widetilde{T}, N)$, with*

- *$K/\mathbb{Q}$ a number field,*
- *S a finite set of places of K not dividing (ℓ),*

- *$g \in \mathbb{Z}^+$,*
- *$\ell \in \mathbb{Z}^+$ a prime,*
- *T a finite set, disjoint from S, of places of K not dividing (ℓ), which determines trace functions (Def. 6.2) with parameters $(K, S, 2g, \ell)$,*
- *$a_\mathfrak{p} \in \mathbb{Z}$ for all $\mathfrak{p} \in T$,*
- *$\widetilde{T}$ a finite set, disjoint from S, of places of K not dividing (ℓ), such that $T \subseteq \widetilde{T}$, such that $\mathrm{Nm}\ \mathfrak{p} < \frac{\ell^{2N}}{16g^2}$ for all $\mathfrak{p} \in \widetilde{T}$, and*
- *$N \in \mathbb{Z}^+$,*

returns $(\Phi, (a_\mathfrak{p})_{\mathfrak{p}\in\widetilde{T}})$, where

- *Φ is the (finite) set of all $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^N)$ such that*
  1. *ρ is unramified outside S and the primes above (ℓ),*
  2. *for all $\mathfrak{p} \in T$, $\mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p})) \equiv a_\mathfrak{p} \pmod{\ell^N}$,*
  3. *$\det \rho \equiv \chi_\ell^g \pmod{\ell^N}$,*
  4. *for all $\lambda \mid (\ell)$, the Galois module corresponding to ρ prolongs to a finite flat group scheme over $\mathfrak{o}_{K,\lambda}$, and*
  5. *for all $\mathfrak{p} \in \widetilde{T}$, the Frobenius trace $\mathrm{tr}(\rho(\mathrm{Frob}_\mathfrak{p}))$ is congruent (modulo ℓ^N) to some integer $a_{\mathfrak{p},\rho}$ with $|a_{\mathfrak{p},\rho}| \leq 2g \cdot \sqrt{\mathrm{Nm}\ \mathfrak{p}}$,*
- *and, for all primes $\mathfrak{p} \in \widetilde{T}$ and all $\rho \in \Phi$, we have $a_{\mathfrak{p},\rho} = a_\mathfrak{p}$.*

Remark 6.6. *This theorem statement has two parts. First, we can compute the set Φ of mod-ℓ^N Galois representations ρ satisfying conditions 1-5. Then, we claim that, for all such ρ, the Frobenius traces at primes in $\widetilde{T}$ agree (and can be computed).*

Proof. By Lemma 6.1 one can compute all (finitely many) $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^N)$ that are unramified outside S and the set of primes dividing ℓ.

Now it is simply a matter of testing which of these Galois representations satisfy conditions 2-5 above. For condition 5, we use Lemma 6.4; the other conditions are straightforward.

All these ρ will have the same Frobenius traces since T determines trace functions, and of course it is straightforward to compute those traces. □

7 Fundamental algorithms for abelian varieties over number fields.

7.1 Computability of torsion.

Lemma 7.1. *There is a finite-time algorithm that, on input $(K, A/K, N)$ with A/K an abelian variety over a number field $K/\mathbb{Q}$ and N a positive integer, returns the finite set $A[N]$.*

(Specifically, A is input to the algorithm in a projective embedding; the algorithm then outputs the finitely many points $A[N]$ in the same projective embedding, with coordinates presented as exact elements of some number field L extending K.)

Proof. Brute-force search (Principle 5.1).[6] Note that:

- One can test whether any point of the ambient projective space is an N-torsion point of A, and
- One knows that the total number of N-torsion points is $N^{2\dim A}$.

□

7.2 Computability of Frobenius traces.

Theorem 7.2. *There is an algorithm that takes as input a number field K, an abelian variety A over K, and a prime $\mathfrak{p}$ of K not dividing the conductor of A, and returns the trace of Frobenius acting on $H^1(A, \mathbb{Q}_\ell)$ (this trace is independent of ℓ provided ℓ is not divisible by $\mathfrak{p}$).*

Proof. Choose a prime $\widetilde{\ell} \gg_{\mathrm{Nm}\ \mathfrak{p}} 1$ coprime to the conductor of A and then use Lemma 7.1 to compute $A[\widetilde{\ell}]$ along with its action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. □

7.3 Computability of the conductor.

We will in fact show that Néron models are computable in Section 7.9, but the (implicit) algorithm will repeatedly invoke the book of Bosch-Lütkebohmert-Raynaud [BLR90] and thus will not be self-contained. Since we will only need to compute conductors for the main theorems of this paper, we will give a standalone algorithm to compute said conductors in this section.

Algorithm 7.3. *On input $(K, A/K)$,*

1. *Compute a finite set S of places of K such that A/K has good reduction outside S (e.g. via collecting all denominators etc. present in Mumford data for the given A/K).*
2. *For each $\mathfrak{p} \in S$,*

[6] Of course computing the kernel of multiplication of N is more sensible, but we have released ourselves to brute force throughout.

   (a) *Let $p \in \mathbb{Z}^+$ be the prime such that $\mathfrak{p} \mid (p)$.*
   (b) *Let $\ell \neq p$ be another prime.*
   (c) *Compute the Swan conductor $w_\mathfrak{p}$ of $A[\ell]$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\mathfrak{p})$-representation (using Lemma 7.1 to compute $A[\ell]$).*
   (d) *Let $N := 10^{10}$.*
      i. *Let $M := N$.*
      ii. *Compute the set α_N of all smooth integral models $\mathcal{A}/\mathfrak{o}_K$ of A/K involving coefficients in $\mathfrak{o}_K$ of height at most N.*
      iii. *For each $\mathcal{A} \in \alpha_N$,*
         (α) *Compute the exponent $e_\mathcal{A}$ of the ℓ-part of the component group of its special fibre $\overline{\mathcal{A}} := \mathcal{A} \pmod{\mathfrak{p}}$.*
         (β) *Increment $M \mapsto \max(M, e_\mathcal{A} + 1)$.*
      iv. *Let $e_\mathfrak{p}^\uparrow(M) := \infty$.*
      v. *For each $\mathcal{A} \in \alpha_N$,*
         (α) *If not all $P \in A[\ell^{M+1}]^{I_\mathfrak{p}}$ prolong over $\mathfrak{o}_{K,\mathfrak{p}}^{\mathrm{ur.}}$ then continue this loop to the next element of α_N.*
         (β) *Compute $e_\mathfrak{p}(\mathcal{A}) := w_\mathfrak{p} + 2g - \dim_{\mathbb{F}_\ell} \ell^M \cdot \overline{\mathcal{A}}\left(\overline{\mathbb{F}}_\ell\right)[\ell^{M+1}]$.*
         (γ) *Replace $e_\mathfrak{p}^\uparrow(M) \mapsto \min(e_\mathfrak{p}^\uparrow(M), e_\mathfrak{p}(\mathcal{A}))$.*
      vi. *If $e_\mathfrak{p}^\uparrow(M) = w_\mathfrak{p} + 2g - \dim_{\mathbb{F}_\ell} \ell^M \cdot \left(A[\ell^{M+1}]^{I_\mathfrak{p}}\right)$ then let $e_\mathfrak{p} := e_\mathfrak{p}^\uparrow(M)$ and break this loop.*
      vii. *Otherwise increment $N \mapsto M + 1$.*

3. *Return $\mathfrak{n} := \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{e_\mathfrak{p}}$.*

Theorem 7.4. *Algorithm 7.3 is a finite-time algorithm that, on input $(K, A/K)$ with A/K an abelian variety over a number field $K/\mathbb{Q}$, returns its conductor $\mathfrak{n} \subseteq \mathfrak{o}_K$.*

Remark 7.5. *In particular, by factoring the conductor, one can determine algorithmically the set of primes of bad reduction of A.*

Proof. We claim that the algorithm specified in Algorithm 7.3 terminates with the desired output on all inputs.

Let A/K be an abelian variety over a number field $K/\mathbb{Q}$. Let $\mathfrak{p} \subseteq \mathfrak{o}_K$ be a prime of $\mathfrak{o}_K$. Let $p \in \mathbb{Z}^+$ be the prime such that $\mathfrak{p} \mid (p)$. Let $\ell \neq p$ be another prime. Let $N \in \mathbb{Z}^+$. Let $\mathcal{A}/\mathfrak{o}_K$ be a smooth integral model of A/K of height at most N. Let $M \in \mathbb{Z}^+$ be such that the component group of $\overline{\mathcal{A}} := \mathcal{A} \pmod{\mathfrak{p}}$ is ℓ^M-torsion. Let $w_\mathfrak{p}$ be the Swan conductor of $A[\ell]$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\mathfrak{p})$-representation. Let $e_\mathfrak{p}(\mathcal{A}) := w_\mathfrak{p} + 2g - \dim_{\mathbb{F}_\ell} \ell^M \cdot \overline{\mathcal{A}}(\overline{\mathbb{F}}_p)[\ell^{M+1}]$. Let $G \subseteq A(K_\mathfrak{p}^{\mathrm{ur.}})[\ell^{M+1}]$ be the subgroup of points which prolong over $\mathfrak{o}_{K,\mathfrak{p}}^{\mathrm{ur.}}$.

We claim that $e_\mathfrak{p}(\mathcal{A}) \geq w_\mathfrak{p} + 2g - \dim_{\mathbb{F}_\ell} \ell^M \cdot G$. Indeed this amounts to the claim that $\dim_{\mathbb{F}_\ell} \ell^M \cdot G \leq \dim_{\mathbb{F}_\ell} \ell^M \cdot \overline{\mathcal{A}}\left(\overline{\mathbb{F}}_p\right)[\ell^{M+1}]$, which follows from the injection $G \hookrightarrow \overline{\mathcal{A}}(\overline{\mathbb{F}}_p)[\ell^{M+1}]$ arising from prolongation and then reduction modulo $\mathfrak{p}$, since G prolongs to a finite flat — indeed étale — subgroup scheme of $\mathcal{A}$ over $\mathfrak{o}_{K,\mathfrak{p}}^{\mathrm{ur.}}$.

Note also that if $\mathcal{A}/\mathfrak{o}_K$ is the Néron model of A/K then $G = A(K_{\mathfrak{p}}^{\mathrm{ur.}})[\ell^{M+1}] = A(\overline{\mathbb{Q}}_p)[\ell^{M+1}]^{I_{\mathfrak{p}}}$ and moreover by smoothness and étaleness (i.e. Hensel) $G = \mathcal{A}(\mathfrak{o}_{K,\mathfrak{p}}^{\mathrm{ur.}})[\ell^{M+1}] \to \overline{\mathcal{A}}(\overline{\mathbb{F}}_p)[\ell^{M+1}]$ is an isomorphism, whence it follows that $e_p(\mathcal{A}) = w_{\mathfrak{p}} + 2g - \dim_{\mathbb{F}_\ell} \ell^M \cdot G$.

So the bound is sharp with equality at least for the Néron model, whence once N becomes sufficiently large Step $2.(d).vi$ breaks the loop, which is to say that Algorithm 7.3 terminates on all inputs.

It remains to show that the corresponding $e_{\mathfrak{p}}^{\uparrow}(M)$ is the correct conductor exponent at $\mathfrak{p}$, which is to say that $\dim_{\mathbb{F}_\ell} \ell^M \cdot (A[\ell^{M+1}]^{I_{\mathfrak{p}}}) = t + 2b$, where $t = \dim T$ and $b = \dim B$ in the Chevalley decomposition $0 \to T \times U \to \overline{\mathcal{A}}^{\circ} \to B \to 0$, with $\overline{\mathcal{A}}^{\circ}/(\mathfrak{o}_K/\mathfrak{p})$ the connected component of the identity of the mod-$\mathfrak{p}$ special fibre of the Néron model $\mathcal{A}/\mathfrak{o}_K$ of A/K, $B/(\mathfrak{o}_K/\mathfrak{p})$ an abelian variety, $T/(\mathfrak{o}_K/\mathfrak{p})$ a torus, and $U/(\mathfrak{o}_K/\mathfrak{p})$ a unipotent group. However as noted above by smoothness and étaleness we have that $A(\overline{\mathbb{Q}}_p)[\ell^{M+1}]^{I_{\mathfrak{p}}} = A(K_{\mathfrak{p}}^{\mathrm{ur.}})[\ell^{M+1}] \to \overline{\mathcal{A}}(\overline{\mathbb{F}}_p)[\ell^{M+1}]$ is an isomorphism, and the latter satisfies $\dim_{\mathbb{F}_\ell} \ell^M \cdot \overline{\mathcal{A}}(\overline{\mathbb{F}}_p)[\ell^{M+1}] = t + 2b$ because $\ell^M \cdot \overline{\mathcal{A}}(\overline{\mathbb{F}}_p) \subseteq \overline{\mathcal{A}}^{\circ}(\overline{\mathbb{F}}_p)$, completing the proof. □

7.4 Computability of the endomorphism ring.

Algorithm 7.6. *On input $(K, A/K)$,*

1. *Choose a prime $\ell \in \mathbb{Z}^+$.*
2. *Let $N := 1$.*
3. *Until this loop is broken (by the termination condition in (c) below),*
    (a) *Perform a brute-force search with parameter N (Principle 5.1) for K-subvarieties of $A \times A$ of height at most N which are the graphs of endomorphisms of A, and, for each such, compute its action on singular homology $H_1(A, \mathbb{Z})$ (using Lemma 9.10). Let $S_N \subseteq \operatorname{End} H_1(A, \mathbb{Z})$ be a basis for the algebra generated by all such endomorphisms.*

    (b) *Compute a $\Sigma_N \subseteq \operatorname{End}_K(A)$ such that Σ_N is $\mathbb{Z}$-linearly independent and* $\operatorname{span}_{\mathbb{Z}} \Sigma_N$ *is the saturation of* $\operatorname{span}_{\mathbb{Z}} S_N$ *inside* $\operatorname{End}_K(A)$*. To do this:*
        i. *Compute a basis $\Sigma_{N,\mathrm{sing.}}$ for the saturation of* $\operatorname{span}_{\mathbb{Z}} S_N$ *inside* $\operatorname{End} H_1(A, \mathbb{Z})$.
        ii. *For each $f_{\mathrm{sing.}} \in \Sigma_{N,\mathrm{sing.}}$, find, by brute-force search, an endomorphism f of A such that $H_1(f) = f_{\mathrm{sing.}}$.*

    (c) *Using Lemma 7.1, compute the ℓ^N-torsion $A[\ell^N]$, and determine whether* $\operatorname{rank}_{\mathbb{Z}} \operatorname{span}_{\mathbb{Z}} \Sigma_N = \dim_{\mathbb{F}_\ell} \ell^{N-1} \cdot \operatorname{End}_{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}(A[\ell^N])$*. If so, return Σ_N. Else increment $N \mapsto N + 1$ and return to the beginning of this loop.*

Theorem 7.7. *Algorithm 7.6 is a finite-time algorithm that, on input $(K, A/K)$ an abelian variety over a number field $K/\mathbb{Q}$, outputs (a $\mathbb{Z}$-basis of) $\operatorname{End}_K(A)$.*

Proof. For all $N \in \mathbb{Z}^+$, $\operatorname{rank}_{\mathbb{Z}} \operatorname{span}_{\mathbb{Z}} \Sigma_N \leq \operatorname{rank}_{\mathbb{Z}} \operatorname{End}_K(A)$ and $\operatorname{rank}_{\mathbb{Z}_\ell} \operatorname{End}_{\operatorname{Gal}(\overline{\mathbb{Q}}/K)}(T_\ell(A)) \leq \dim_{\mathbb{F}_\ell} \ell^{N-1} \cdot \operatorname{End}_{\operatorname{Gal}(\overline{\mathbb{Q}}/K)}(A[\ell^N])$ — the first is evident and the second follows because the canonical map $\operatorname{End}_{\operatorname{Gal}(\overline{\mathbb{Q}}/K)}(T_\ell(A))/\ell \to \ell^{N-1} \cdot \operatorname{End}_{\operatorname{Gal}(\overline{\mathbb{Q}}/K)}(A[\ell^N])$ is an injection because $(\ell^{N-1} \cdot \varphi)(A[\ell^N]) = \varphi(A[\ell])$ and so if the left-hand side vanishes then $\varphi \in \operatorname{End}_{\operatorname{Gal}(\overline{\mathbb{Q}}/K)}(T_\ell(A))$ is divisible by ℓ. Moreover for N sufficiently large both inequalities are sharp — evident in the first case and a consequence of e.g. Kőnig's Lemma in the second case.

But now because $\operatorname{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \operatorname{End}_{\operatorname{Gal}(\overline{\mathbb{Q}}/K)}(T_\ell(A))$ is an isomorphism it follows that, for all N, $\operatorname{rank}_{\mathbb{Z}} \operatorname{span}_{\mathbb{Z}} \Sigma_N \leq \dim_{\mathbb{F}_\ell} \ell^{N-1} \cdot \operatorname{End}_{\operatorname{Gal}(\overline{\mathbb{Q}}/K)}(A[\ell^N])$, with equality if and only if both equal $\operatorname{rank}_{\mathbb{Z}} \operatorname{End}_K(A)$ (whence $\operatorname{span}_{\mathbb{Z}} \Sigma_N = \operatorname{End}_K(A)$), and we have seen that equality holds when N is sufficiently large, so that the algorithm always terminates with correct input, as desired. □

7.5 Computability of the set of polarizations of given degree.

Theorem 7.8. *There is a finite-time algorithm that, on input $(K, A/K, (d_1, \ldots, d_{\dim A}))$ with A/K an abelian variety over a number field $K/\mathbb{Q}$ and $d_i \in \mathbb{Z}^+$, outputs a set of representatives of the (finitely many) $\operatorname{Aut}_K(A)$-orbits of K-polarizations of A/K of multidegree $(d_1, \ldots, d_{\dim A})$.*

The proof of Theorem 7.8 is given in Section 8.

7.6 Computability of the isomorphism relation.

Lemma 7.9. *There is a finite-time algorithm that, on input $(K, (A, \mathcal{L}))$ with K a number field and $(A, \mathcal{L})$ a polarized abelian variety over K, returns the (finite) set of all K-automorphisms of A that preserve the Néron–Severi class of $\mathcal{L}$.*

Proof. Compute (Theorem 7.7) the endomorphism ring of A, along with its action (Lemma 9.10) on $H_1(A, \mathbb{Z})$.

Further compute (Lemma 9.11) the Chern class of $\mathcal{L}$ as an alternating pairing $\varphi(v, w)$ on $H_1(A, \mathbb{Z})$, and the complex structure $v \mapsto I \cdot v$ (Lemma 9.9) on $H_1(A, \mathbb{Z}) \otimes \mathbb{R}$, in approximate coordinates.

Compute approximate coordinates for the positive-definite pairing $(v, w) \mapsto \varphi(v, Iw)$ on $H_1(A, \mathbb{Z}) \otimes \mathbb{R}$. Any automorphism of $(A, \mathcal{L})$ must preserve this pairing; this gives us an explicit bound on the size of the coefficients of any such automorphism. Test all endomorphisms in $\operatorname{End}_K(A)$ up to this bound to determine which fix the Chern class of $\mathcal{L}$. □

Theorem 7.10. *There is a finite-time algorithm that, on input $(K, (A, \mathcal{L}_1), (B, \mathcal{L}_2))$ with $(A, \mathcal{L}_1)$ and $(B, \mathcal{L}_2)$ two polarized abelian varieties over a number field K, returns true if and only if $(A, \mathcal{L}_1) \cong_K (B, \mathcal{L}_2)$.*

If so, the algorithm also returns an explicit K-isomorphism.

Proof. Find some Mumford embedding of B over an extension L of K (Lemma 12.13), polarized by $8\mathcal{L}_2$.

Compute (Lemma 12.14) all embeddings in Mumford form of $(A_L, 8\mathcal{L}_1)$. Check to see whether any of these embeddings agrees with the Mumford embedding of B found above. If no, return false.

If yes, let $f\colon A_L \to B_L$ be the isomorphism given by the equality between the Mumford embeddings of A_L and B_L. Replace L with its Galois closure over K. Compute (Theorem 7.7) the endomorphism ring E of A over L. Then $\mathrm{Hom}_L(A, B)$ is a finitely-generated free abelian group, isomorphic to E by $e \mapsto f \circ e$.

Compute the action of the finite Galois group $\mathrm{Gal}(L/K)$ on the finitely generated abelian group $\mathrm{Hom}_L(A, B)$. Determine the fixed set $\mathrm{Hom}_K(A, B) = \mathrm{Hom}_L(A, B)^{\mathrm{Gal}(L/K)}$.

Apply Lemma 7.9 to find all automorphisms of A that respect the polarization $\mathcal{L}_1$. For every such automorphism e, determine whether $f \circ e \in \mathrm{Hom}_L(A, B)$ is stable under the action of $\mathrm{Gal}(L/K)$. If it is (for any e), return $f \circ e$; otherwise, return false. □

Theorem 7.11. *There is a finite-time algorithm that, on input (K, A, B) with $A, B/K$ two abelian varieties over a number field K, returns true if and only if $A \cong_K B$.*

If so, the algorithm also returns an explicit K-isomorphism.

Proof. Apply Theorems 7.8 (using e.g. the multidegree of the implicitly given polarization of A) and 7.10. □

7.7 Computability of the isogeny class.

Theorem 7.12. *There is a finite-time algorithm that, on input $(K, A/K)$ an abelian variety over a number field K, returns an N such that, if B is any abelian variety K-isogenous to A, then there is a K-isogeny $A \to B$ of degree at most N.*

Proof. This follows from [MW93] and [Bos96].[7] □

Theorem 7.14. *There is a finite-time algorithm that, on input $(d, K, A/K)$ with $d \in \mathbb{Z}^+$ and A/K an abelian variety over a number field $K/\mathbb{Q}$, returns $\{(B, \mathcal{L})/K : B \sim_K A, \deg(\mathcal{L}) = d\}/\cong_K$.*

Proof. Compute $\mathrm{End}_K(A)$. Compute (Theorem 7.12) an $N \in \mathbb{Z}^+$ such that $B \sim_K A$ implies there is a K-isogeny $\varphi : A \to B$ of degree $\deg \varphi \leq N$. Compute all subgroups $G \subseteq A[N']$ (with $N' \leq N$) which are $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-stable, i.e.

[7] For example:

Theorem 7.13 (Theorem 1.4 of Gaudron-Rémond's [GR14]). *Let $A, A'/K$ be K-isogenous abelian varieties over a number field K. Write $g := \dim A$. Then: there is a K-isogeny $\varphi : A \to A'$ of degree*

$$\deg \varphi \leq \left((14g)^{64g^2} \cdot [K : \mathbb{Q}] \cdot \max(h(A), \log [K : \mathbb{Q}], 1)^2\right)^{2^{10}g^3} =: \kappa(A),$$

where $h(A)$ is the Faltings height of A using Faltings' original normalization.

Consequently,

$$|h(A') - h(A)| \leq \frac{1}{2} \log \kappa(A).$$

$\mathrm{Gal}(\overline{\mathbb{Q}}/K) \cdot G = G$. For each such G, determine (Theorem 7.8) all polarizations $\mathcal{L}$ of degree d on A/G. Return the set (i.e. remove duplicates via Theorem 7.11) of all such pairs $(A, \mathcal{L})$. □

7.8 Computability of a k-th root.

Proposition 7.15. *There is a finite-time algorithm that, on input $(K, A/K, k)$ with A/K an abelian variety over a number field $K/\mathbb{Q}$ and $k \in \mathbb{Z}^+$, returns true if and only if there is an abelian variety B/K such that $A \cong_K B^{\times k}$.*

If so, the algorithm also returns such a B/K along with an explicit K-isomorphism.

Here there are a number of clear ways to proceed, e.g. by reading the answer off from the K-endomorphism ring, via brute force search, or e.g. the following.

Proof. Compute (Theorem 7.7) $\mathrm{End}_K(A)$. Compute (Proposition 11.1) a decomposition

$$\mathrm{End}_K^0(A) \cong \bigoplus_{i=1}^{s} M_{n_i}(E_i),$$

with each E_i a division algebra. Return false if at least one of the n_i's is not divisible by k.

Else (via this isomorphism and suitable elements of the form $\left(\kappa \cdot \delta_{i,a} \cdot \left(\delta_{(j,k),(b,c)}\right)_{j,k=1}^{n_i}\right)_{i=1}^{s}$ with $\kappa \in \mathbb{Z}^+$ sufficiently divisible) compute an abelian subvariety B/K with $B \subseteq A$ such that $A \sim_K B^{\times k}$.

Finally compute all $C \sim_K B$ (Theorem 7.14) and check if any have $A \cong_K C^{\times k}$ (Theorems 7.8 and 7.11). □

7.9 Computability of the Néron model.

This result is not used in the rest of the paper; we include it for our own amusement.

Theorem 7.16. *There is a finite-time algorithm that, on input (K, A) with $K/\mathbb{Q}$ a number field and A/K an abelian variety, outputs its Néron model $\mathcal{A}/\mathfrak{o}_K$.*

Let us show the local version of this statement first.

Theorem 7.17. *There is a finite-time algorithm that, on input (ℓ, K, λ, A) with $K_\lambda/\mathbb{Q}_\ell$ a finite extension and A/K_λ an abelian variety, outputs its Néron model $\mathcal{A}/\mathfrak{o}_{K,\lambda}$.*

Note that here we leave implicit the evident finitary statement in terms of ℓ-adic approximations.

Proof of Theorem 7.17. Implicitly we are given a "desired precision" $N \in \mathbb{Z}^+$ and, to the extent that we can, we will leave implicit the fact that we are working at finite precision (i.e. all varieties are over $\mathfrak{o}_K/\lambda^{\widetilde{N}}$ and the computations are repeated incrementing $\widetilde{N} \mapsto \widetilde{N} + 1$ until the desired precision is reached).

Let $\omega \neq 0$ be a left-invariant differential on A/K_λ.

A/K_λ is equipped with a polarization, so let $\mathcal{B}/\mathfrak{o}_{K,\lambda}$ be the scheme-theoretic closure of A in the corresponding projective space over $\mathfrak{o}_{K,\lambda}$. Compute $\mathcal{B} \pmod{\lambda^N}$. Compute (via Hensel) an $n \in \mathbb{Z}^+$ such that a point $P \in (\mathcal{B} \bmod \lambda)(\overline{\mathbb{F}}_\ell)$ lifts to $(\mathcal{B} \bmod \lambda^n)(\mathfrak{o}_K^{\mathrm{s.H.}}/\lambda^n)$ if and only if it lifts to $\mathcal{B}(\mathfrak{o}_K^{\mathrm{s.H.}})$. Without loss of generality (by replacing $N \mapsto \max(N, n)$) $N \geq n$, and indeed (by incrementing $N \mapsto N+1$ and restarting the algorithm if necessary, or else via e.g. Hensel) N is so large that all the below steps have errors contained in λ^N.

We will apply the "smoothening process" detailed in Chapter 3 (and specifically on page 72) of Bosch-Lütkebohmert-Raynaud's [BLR90] to $\mathcal{B}/\mathfrak{o}_{K,\lambda}$ to obtain a weak Néron model $\widetilde{\mathcal{B}}/\mathfrak{o}_{K,\lambda}$, exactly as in the first paragraph of their page 74.

Write $\mathcal{B}_0 := \mathcal{B}$.

For each $i \in \mathbb{Z}^+$, we will inductively define $\mathcal{B}_i$ as follows.

Let $E^{(i,0)} := \varnothing$.

For each $j \in \mathbb{Z}^+$, we will inductively define $E^{(i,j)}$, $F^{(i,j)}$, $Y^{(i,j)}_{/(\mathfrak{o}_K/\lambda)}$, and $U^{(i,j)}_{/(\mathfrak{o}_K/\lambda)}$ as follows.

Let $F^{(i,j)} \subseteq (\mathcal{B} \bmod \lambda^N)(\mathfrak{o}_K^{\mathrm{s.H.}}/\lambda^N)$ be the subset of points not in $E^{(i,j-1)}$ which reduce into the singular locus of $(\mathcal{B} \bmod \lambda)/\overline{\mathbb{F}}_\ell$ and let $Y^{(i,j)}_{/(\mathfrak{o}_K/\lambda)} \subseteq \mathcal{B} \bmod \lambda$ be the scheme-theoretic closure of the reduction of $F^{(i,j)}$. (This latter closed subscheme is computable, again by Hensel.)

Let $U^{(i,j)}_{/(\mathfrak{o}_K/\lambda)} \subseteq Y^{(i,j)}_{/(\mathfrak{o}_K/\lambda)}$ be the largest open subscheme which is smooth over $\mathfrak{o}_K/\lambda$ and over which $\Omega^1_{\mathcal{B}/\mathfrak{o}_K} \mid_{Y^{(i,j)}_{/(\mathfrak{o}_K/\lambda)}}$ is locally free. (This dense open subscheme is computable.)

Let $E^{(i,j)} \subseteq F^{(i,j)}$ be the points reducing into $U^{(i,j)}_{/(\mathfrak{o}_K/\lambda)}$.

Because the dimensions of the $Y^{(i,j)}_{/(\mathfrak{o}_K/\lambda)}$ are strictly decreasing it follows that for j explicitly sufficiently large $Y^{(i,j)}_{/(\mathfrak{o}_K/\lambda)} = \varnothing$. Let $t_i \in \mathbb{Z}^+$ be minimal with this property.

If $t_i = 0$ then break the loop over i and let $\widetilde{\mathcal{B}} := \mathcal{B}_i$.

Otherwise, let $\mathcal{B}_i$ be the blowup of $\mathcal{B}_{i-1}$ at $Y^{(i,t_i-1)}_{/(\mathfrak{o}_K/\lambda)}$ and continue the loop.

The proof of Theorem 2 of Section 3.4 of Bosch-Lütkebohmert-Raynaud's [BLR90] implies that this procedure terminates and moreover (and indeed this is how it is used in the proof of Corollary 4 of Section 3.1 of the same) that the resulting $\widetilde{\mathcal{B}}$ is a weak Néron model of A/K_λ.

Write $\widetilde{\mathcal{B}}_i$ for the preimages in $\widetilde{\mathcal{B}}$ of the irreducible components of $(\widetilde{\mathcal{B}} \bmod \lambda)/(\mathfrak{o}_K/\lambda)$.

For each i, let n_i be the valuation of ω at the generic point of the special fibre of $\widetilde{\mathcal{B}}_i$.

Let $n_* := \min_i n_i$ and let $S := \{i : n_i = n_*\}$. Then by Lemma 1 and Proposition 2 of Section 4.3 of Bosch-Lütkebohmert-Raynaud's [BLR90] it follows that an ω-minimal (their nomenclature) $\mathfrak{o}_{K,\lambda}$-model of A/K_λ is equivalent (in the sense of page 105 of Bosch-Lütkebohmert-Raynaud's [BLR90]) to one of the $\widetilde{\mathcal{B}}_i$ with $i \in S$.

Now we may simply follow the proof of Proposition 4 of Section 4.3 of Bosch-Lütkebohmert-Raynaud's [BLR90] to construct an $\mathfrak{o}_{K,\lambda}$-model $\widetilde{\widetilde{\mathcal{B}}}/\mathfrak{o}_{K,\lambda}$: shrink (via a finite computation on the special fibre) the special fibres of each of the $\widetilde{\mathcal{B}}_i$ for $i \in S$ to obtain $\widetilde{\mathcal{B}}'_i$, say, so that the diagonal of $A \times_{K_\lambda} A$ is Zariski closed inside $\widetilde{\mathcal{B}}'_i \times_{\mathfrak{o}_{K,\lambda}} \widetilde{\mathcal{B}}'_j$ when $i \neq j$ and $i, j \in S$, and then glue the $\widetilde{\mathcal{B}}'_i$ for $i \in S$ along their generic fibres. The proof of Proposition 5 of Section 4.3 of Bosch-Lütkebohmert-Raynaud's [BLR90] then constructs an explicit $\mathfrak{o}_{K,\lambda}$-birational group law on the resulting model $\widetilde{\widetilde{\mathcal{B}}}$.

Finally it is a matter of executing a brute-force search for $\mathfrak{o}_{K,\lambda}$-group scheme structure (i.e. for the multiplication and inversion maps) on $\widetilde{\widetilde{\mathcal{B}}}$ — Theorem 6 of Section 4.3 of Bosch-Lütkebohmert-Raynaud's [BLR90] amounts to the statement that this search terminates in finite time.

The resulting group scheme over $\mathfrak{o}_{K,\lambda}$ is the Néron model of A/K_λ by Corollary 4 of Section 4.4 of Bosch-Lütkebohmert-Raynaud's [BLR90], as desired. □

Proof of Theorem 7.16. Write $\mathcal{A}/\mathfrak{o}_K$ for the Néron model of A/K.

First note the following finite-time test of whether or not a smooth model $\mathcal{B}/\mathfrak{o}_K$ is the Néron model of A: compute (in the evident way) a finite set $T \supseteq S$ of primes of K containing all ramified primes of $K/\mathbb{Q}$ such that $\mathcal{B}$ has good reduction outside T. For each prime $\lambda \in T$, compute (via Hensel) an $n \in \mathbb{Z}^+$ such that if the canonical map induced by the Néron mapping property is an $(\mathfrak{o}_K/\lambda^n)$-isomorphism between $\mathcal{B} \pmod{\lambda^n}$ and the mod-λ^n reduction of the Néron model of A/K_λ, then said map is an $\mathfrak{o}_{K,\lambda}$-isomorphism. Then check (via Theorem 7.17) in finite time whether this is the case. If this test passes for each $\lambda \in T$, then return $\mathcal{B}/\mathfrak{o}_K$.

This test is indeed only passed by $\mathcal{A}/\mathfrak{o}_K$ — specifically, the Néron mapping property produces a map $\mathcal{B} \to \mathcal{A}$ which is an isomorphism at all primes λ: at all $\lambda \in T$ by construction, and at all $\lambda \notin T$ because of functoriality and the fact that abelian schemes are uniquely Néron models of their generic fibres (alternatively consider p-divisible groups).

Now we simply brute-force search through smooth models $\mathcal{B}/\mathfrak{o}_K$ of A/K by enumerating integral models of abelian varieties, testing smoothness (a calculation of e.g. a Gröbner basis), and then testing K-isomorphism of generic fibres (via Theorem 7.11). □

7.10 Computability of a nonisotrivial family over a given curve.

Theorem 7.18. *There is a finite-time algorithm that, on input $(K, C/K)$ with C/K a smooth projective hyperbolic curve over a number field $K/\mathbb{Q}$, outputs a nonisotrivial family $A \to C$ of abelian varieties, defined over K.*

Note that valid outputs exist for all inputs, thanks to e.g. the Kodaira-Parshin family (see for example [LV20, §7]).

Proof. Brute-force search (see Section 5.3). □

7.11 Computability of an integral model.

Theorem 7.19. *There is a finite-time algorithm that, on input $(K, C, A \to C)$, with $K/\mathbb{Q}$ a number field, C a smooth projective hyperbolic curve over K, and $A \to C$ a nonisotrivial family of abelian varieties over C, outputs a finite set S of places of K, such that for every $x \in C(K)$, the fiber A_x has good reduction at all places of K outside S.*

Proof. Take any integral model $\mathcal{A} \to \mathcal{C}$ of $A \to C$ over $\mathcal{O}_K$. (We can produce such a model by simply writing down defining equations for A and C in projective coordinates, and clearing denominators.)

The locus in $\operatorname{Spec} \mathcal{O}_K$ over which $\mathcal{A} \to \mathcal{C}$ is a smooth morphism of smooth schemes is an effectively computable open set U; compute it, and take S to be the set of points (i.e. primes) of $\mathcal{O}_K$ not contained in this U.

Then every K-point $x \in C(K)$ extends to an $\mathcal{O}_{K,S}$-point $x \in \mathcal{C}(\mathcal{O}_{K,S})$, and the fiber $\mathcal{A}_x$ is a smooth abelian scheme over $\mathcal{O}_{K,S}$. □

8 Computability of the set of polarizations of given degree.

In this and the following section we prove Theorem 7.8: we show how to compute all polarizations, up to automorphism, of given degree, on a given abelian variety.

That there are only finitely many such polarizations is a theorem of Narisimhan and Nori [NN81]; we need to prove that the finite list can be effectively computed.

Narasimhan and Nori reduce the statement about principal polarizations to a theorem of Borel and Harish-Chandra [BHC62a, Theorem 6.9] about orbits of arithmetic groups on lattices. The reduction relies on [NN81, Lemma 3.1], showing that a certain algebraic group acting on a certain variety *over* $\mathbb{C}$ has only finitely many orbits. We will explicitly enumerate these orbits.

Many of the results of [BHC62a] are made algorithmic in a paper of Grunewald and Segal [GS80]. While [BHC62a, Theorem 6.9] is not treated in [GS80], it is quickly reduced to previous lemmas that are.

There is one piece of the argument of [BHC62a] that we were unable to make effective in general: in order to determine all the integral orbits of G on W, we need to determine which real orbits of W contain a rational point, and identify a specific rational point in each. In the special case relevant to abelian varieties we do so by an explicit calculation (Lemma 8.4).

8.1 Introduction and setup.

Let us recall from [NN81] the connection between polarizations and the endomorphism algebra.

Let A be an abelian variety, and fix an ample line bundle $\mathcal{L}_0$ on A. This gives rise to a Rosati involution $\theta = \theta_{\mathcal{L}_0}$, defined by

$$\theta(f) = \varphi_{\mathcal{L}_0}^{-1} \circ \hat{f} \circ \varphi_{\mathcal{L}_0}.$$

For any other line bundle $\mathcal{L}$, the composition $\varphi_{\mathcal{L}_0}^{-1} \circ \varphi_{\mathcal{L}}$ is an endomorphism of A that is stable under θ; the map

$$\rho(\mathcal{L}) = \varphi_{\mathcal{L}_0}^{-1} \circ \varphi_{\mathcal{L}}$$

defines an injection

$$\mathrm{NS}(A) \to (\mathrm{End}(A) \otimes \mathbb{Q})^{\theta},$$

whose image is the lattice

$$\{\varphi_{\mathcal{L}_0}^{-1} \circ f | f \in \mathrm{Hom}(A, A')\} \cap (\mathrm{End}(A) \otimes \mathbb{Q})^{\theta}$$

in the θ-fixed subspace of $(\mathrm{End}(A) \otimes \mathbb{Q})$ ([MR08, §20, Thm. 2 and §23, Thm. 3]).

Let $E := \mathrm{End}(A)$; write $E_{\mathbb{Q}} = \mathrm{End}(A) \otimes \mathbb{Q}$, and let $E_{\mathbb{Q}}^{\theta}$ be the subspace fixed by θ.

We are interested in principal polarizations $\mathcal{L}$ on A, up to isomorphism of the pair $(A, \mathcal{L})$. We consider two polarizations $\mathcal{L}_1$ and $\mathcal{L}_2$ equivalent if there exists an automorphism f of A such that $f^*\mathcal{L}_1$ agrees with $\mathcal{L}_2$ up to an element of Pic^0. On the level of the endomorphism algebra, we have

$$\rho(f^*\mathcal{L}) = \theta(f)\rho(\mathcal{L})f,$$

giving an action of $E_{\mathbb{Q}}$ on $E_{\mathbb{Q}}^{\theta}$.

We want to compute a set of representatives for the (finitely many) orbits of the integral group E on the integral lattice $NS(A) \subseteq E_{\mathbb{Q}}^{\theta}$. The fact that these orbits are finite in number is [BHC62a, Theorem 6.9]. Using results of [GS80], it is straightforward to compute these representatives, provided one is given a rational "basepoint" in each real orbit; we do this in Section 8.7 and Lemma 8.9.

On the other hand, we do not know of any procedure in the generality of [BHC62a, Theorem 6.9] to determine which real orbits contain rational points! In our particular setting, we explicitly compute the real orbits (Proposition 8.4), and we see that every real orbit contains a rational point – which means that we can find the required basepoints by brute-force search.

8.2 Computation of some polarization.

First a definition.

Definition 8.1. *Let $A, B/K$ be abelian varieties over K and $\varphi : A \to B$ a K-isogeny. Then: $\varphi^\vee : B \to A$ is the K-homomorphism such that $\varphi^\vee \circ \varphi = \deg \varphi$ as elements of $\mathrm{End}_K(A)$. (It follows then that $\varphi \circ \varphi^\vee = \deg \varphi$ as elements of $\mathrm{End}_K(B)$.)*

Proposition 8.2. *There is a finite-time algorithm that, on input $(K, A/K)$ with A/K an abelian variety over a number field $K/\mathbb{Q}$, outputs*

$$(s, (e_i)_{i=1}^s, (n_i)_{i=1}^s, (E_i)_{i=1}^s, (\lambda_i)_{i=1}^s)$$

where

$$\mathrm{End}_K^0(A) \cong \bigoplus_{i=1}^{s} M_{n_i}(E_i)$$

with $s \in \mathbb{Z}^+$, each E_i a division algebra and each $e_i \in E$ the elementary idempotent projecting onto the i-th summand, and each $\lambda_i : A_i \to A_i^*$ a K-polarization, where

$$A_i := \mathrm{diag}(\underbrace{1, 0, \ldots, 0}_{n_i}) \cdot e_i \cdot A.$$

Proof of Proposition 8.2. Compute, via Theorem 7.7, $\mathrm{End}_K^0(A)$. Compute, via Proposition 11.1,

$$(s, (e_i)_{i=1}^s, (n_i)_{i=1}^s, (E_i)_{i=1}^s)$$

where

$$\mathrm{End}_K^0(A) \cong \bigoplus_{i=1}^{s} M_{n_i}(E_i)$$

with each E_i a division algebra and each $e_i \in E$ the elementary idempotent projecting onto the i-th summand. (Note that then $e_i \cdot A \sim_K e_j \cdot A$ implies $i = j$.) Thus via

$$\mathrm{diag}(\underbrace{1, 0, \ldots, 0}_{n_i}) \in M_{n_i}(E_i),$$

i.e. via letting $A_i := \mathrm{diag}(\underbrace{1, 0, \ldots, 0}_{n_i}) \cdot e_i \cdot A$, we obtain a K-isogeny decomposition

$$A \sim_K \prod_{i=1}^{s} A_i^{\times n_i}$$

with each A_i/K K-simple (indeed with $\mathrm{End}_K^0(A_i) \simeq E_i$) and $A_i \sim_K A_j$ only if $i = j$. Finally compute via brute force a K-polarization $\lambda_i : A_i \to A_i^*$ on each A_i/K. □

8.3 Reduction to computing the set of symmetric endomorphisms of given degree modulo automorphisms.

Proposition 8.3. *There is a finite-time algorithm that, on input*

$$(K, \widetilde{A}/K, \widetilde{\lambda}, n, d),$$

with $\widetilde{A}/K$ a K-simple abelian variety over a number field $K/\mathbb{Q}$, $\widetilde{\lambda} : \widetilde{A} \to \widetilde{A}^*$ a K-polarization of A/K, and $n, d \in \mathbb{Z}^+$, outputs a finite set

$$\Phi \subseteq \mathrm{End}_K(\widetilde{A}^{\times n})$$

such that $\mathrm{Aut}_K(\widetilde{A}^{\times n}) \cdot \Phi$ is the set of K-endomorphisms of A/K of degree d which are symmetric with respect to the Rosati involution of $\mathrm{End}_K^0(\widetilde{A}^{\times n})$ induced by $\widetilde{\lambda}^{\times n} : \widetilde{A}^{\times n} \to (\widetilde{A}^{\times n})^*$.

Note that the Rosati involution induced by a K-polarization $\lambda : B \to B^*$ of an abelian variety B/K is

$$\varphi \mapsto \tau_\lambda(\varphi) := \frac{1}{\deg \lambda} \cdot (\lambda^\vee \circ \varphi^* \circ \lambda),$$

with φ^* the dual K-endomorphism of B^* induced by φ and $\lambda^\vee : B^* \to B$ the K-homomorphism such that $\lambda^\vee \circ \lambda = \deg \lambda$, i.e. such that $\ker \lambda^\vee \simeq B[\deg \lambda]/(\ker \lambda)$ under the K-isomorphism $B^* \simeq B/(\ker \lambda)$ furnished by λ.

Let us now show that Proposition 8.3 implies Theorem 7.8.

Proof of Theorem 7.8 assuming Proposition 8.3. First we reduce to the situation where A has the form $A = \widetilde{A}^{\times n}$, with $\widetilde{A}$ a simple abelian variety. Use Lemma 7.7 to compute the endomorphism ring $E = \mathrm{End}_K(A)$, and use Proposition 3 to decompose E as a direct sum of matrix algebras

$$E \cong \bigoplus_{i=1}^{s} M_{n_i}(E_i).$$

Compute B_i, the kernel of $1 - e_i$, where $e_i \in E$ is an idempotent projecting onto the i-th factor.

Let d_0 be the degree of the natural map

$$\bigoplus_{i=1}^{s} B_i \to A.$$

Then every polarization on of degree d pulls back to a polarization of degree dd_0^2 on $\bigoplus_{i=1}^{s} B_i$; conversely, a polarization on $\bigoplus_{i=1}^{s} B_i$ descends to A if its Chern class in

$$H^2(A) \otimes \mathbb{Q} \cong \bigoplus_{i=1}^{s} H^2(B_i) \otimes \mathbb{Q}$$

is integral. (Recall that we can compute Chern classes effectively in terms of an integral basis, Lemma 9.11.)

So it suffices to find all polarizations of given degree on $\bigoplus_{i=1}^{s} B_i$. Any such polarization is a direct sum of polarizations on the individual factors B_i, so it is enough to find all polarizations of given degree on a single factor B_i.

We now rename B_i as A, and assume throughout that $A := \widetilde{A}^{\times n}$ is a power of a K-simple abelian variety.

Write $R := \mathrm{End}_K(\widetilde{A})$, $A = \widetilde{A}^{\times n}$, and $\lambda := \widetilde{\lambda}^{\times n}$. We find all K-polarizations of A/K of given degree d — up to the action of $M_n(R)^\times \simeq \mathrm{Aut}_K(A)$ via

$$\gamma \cdot \lambda' := \gamma \circ \lambda' \circ \gamma^*$$

— as follows. Given a K-endomorphism $\varphi : A \to A$ of degree $d^{\dim A - 1} \cdot \deg \lambda$ with kernel containing that of λ and which is symmetric under the Rosati involution induced by λ, we let $\lambda' : A \to A^*$ be the K-homomorphism such that $\varphi = (\lambda')^\vee \circ \lambda$ (via the fact that φ factors through $A/(\ker \lambda) \simeq A^*$), and then it is routine to determine in finite time whether or not this λ' is indeed a K-polarization of A/K.

Thus we need only show that each such K-polarization (regarded as a symmetric K-homomorphism $\lambda' : A \to A^*$) arises in this manner. But given such a $\lambda' : A \to A^*$, the K-endomorphism

$$(\lambda')^\vee \circ \lambda : A \to A$$

is of degree $d^{\dim A - 1} \cdot \deg \lambda$, has kernel containing that of λ, and is symmetric under the Rosati involution induced by λ. □

8.4 Reduction to the effectivization of certain cases of Borel–Harish-Chandra.

Proposition 8.4. *(Determination of the integral orbits in a real orbit)*

There is a finite-time algorithm that, on input $(K, A/K, \lambda, n, k, (\varphi_i)_{i=1}^k)$, with A/K a K-simple abelian variety over a number field $K/\mathbb{Q}$, $\widetilde{\lambda} : A \to A^*$ a K-polarization, $n \in \mathbb{Z}^+$, $k \in \mathbb{Z}^+$ the $\mathbb{Z}$-rank of $R := \mathrm{End}_K(A)$, and $(\varphi_i)_{i=1}^k$ a $\mathbb{Z}$-basis of R, outputs a finite set Ξ such that, writing:

- $\lambda := \widetilde{\lambda}^{\times n} : A^{\times n} \to (A^{\times n})^*$,
- $i : M_n(R) \hookrightarrow M_{k \cdot n}(\mathbb{Z})$ *for the map induced by the $\mathbb{Z}$-basis $(\varphi_i)_{i=1}^k$,*
- *G the algebraic group over $\mathbb{Q}$ defined by $G(S) := M_n(R \otimes_{\mathbb{Z}} S)^\times$,*
- $G_{\mathbb{Z}} := G(\mathbb{Q}) \cap i^{-1}\left(\mathrm{GL}_{n \cdot \mathrm{rank}_{\mathbb{Z}} R}(\mathbb{Z})\right) = M_n(R)^\times$,
- *V the trivial vector bundle over $\operatorname{Spec} \mathbb{Q}$ defined by $V(S) := \mathrm{End}_K^0(A) \otimes_{\mathbb{Q}} S \simeq M_n(R \otimes_{\mathbb{Z}} S)$ (whence $G \hookrightarrow \mathrm{Aut}_{\mathbb{Q}}(V)$ is an algebraic representation over $\mathbb{Q}$),*
- *$V_{\mathbb{Z}} := \mathrm{End}_K(R)$ (thus $V_{\mathbb{Z}}$ is a lattice inside V which is $G_{\mathbb{Z}}$-stable),*
- *$\tau_\lambda : V \to V$ the Rosati involution induced by λ,*
- *$V^{\mathrm{sym.}} := \ker(\tau_\lambda - \mathrm{id})$, with G-action given by $\gamma \cdot \varphi := \gamma \circ \varphi \circ \tau_\lambda(\gamma)$ (whence $V^{\mathrm{sym.}}$ is an algebraic G-representation defined over $\mathbb{Q}$),*
- *$V_{\mathbb{Z}}^{\mathrm{sym.}} := V^{\mathrm{sym.}} \cap V_{\mathbb{Z}}$ (thus $V_{\mathbb{Z}}^{\mathrm{sym.}}$ is a lattice inside V which is $G_{\mathbb{Z}}$-stable),*
- *$\det : G \to \mathbb{G}_m$ the evident map (defined using i), regarded as furnishing $\mathbb{Q}$ with the structure of an algebraic G-representation defined over $\mathbb{Q}$,*
- *$W := V^{\mathrm{sym.}} \oplus \det \oplus \det^{-1}$ as G-representations defined over $\mathbb{Q}$,*
- *and $W_{\mathbb{Z}} := V_{\mathbb{Z}}^{\mathrm{sym.}} \oplus \mathbb{Z} \oplus \mathbb{Z}$ (thus $W_{\mathbb{Z}}$ is a lattice inside W which is $G_{\mathbb{Z}}$-stable),*

it follows that $G_{\mathbb{Z}} \cdot \Xi = \{(\star, \pm 1, \pm 1) \in W_{\mathbb{Z}}\} = G(\mathbb{R}) \cdot \{(\star, \pm 1, \pm 1) \in W(\mathbb{R})\} \cap W_{\mathbb{Z}}$.

Let us now show that Proposition 8.4 implies Proposition 8.3 and thus Theorem 7.8.

Proof of Proposition 8.4 assuming Proposition 8.3. Compute such a Ξ via Proposition 8.4. For each $(\varphi, \pm 1, \pm 1) \in \Xi$ we may check if there is a $\gamma \in G_{\mathbb{Z}}$ such that

$$\ker\left(\gamma \circ \varphi \circ \tau_\lambda(\gamma)\right) \supseteq \ker \lambda$$

by computing a finite set of generators of $G_{\mathbb{Z}}$ [GS80, Theorem B], then a finite set of representatives in $G_{\mathbb{Z}}$ of $G_{\mathbb{Z}} \pmod{\deg \varphi}$, and finally checking whether there is a $\gamma \in G_{\mathbb{Z}}$ among said representatives such that

$$\ker\left(\gamma \circ \varphi \circ \tau_\lambda(\gamma)\right) \supseteq \ker \lambda,$$

since both are subsets of $A[\deg\varphi]$. If there is no such $\gamma \in G_{\mathbb{Z}}$ we may remove said representative, and if there is such a $\gamma \in G_{\mathbb{Z}}$ (thus already computed in terms of the generators provided by [GS80, Theorem B]) then without loss of generality $\gamma = \mathrm{id}$, and, writing the relevant representative as $\varphi \in \mathrm{End}_K(A)$ and, letting $\lambda' : A \to A^*$ be such that $\varphi = (\lambda')^\vee \circ \lambda$ (which is without loss of generality a K-polarization since this is easily checked in finite time), since

$$\gamma \circ \varphi \circ \tau_\lambda(\gamma) = (\gamma \circ \lambda' \circ \gamma^*) \circ \lambda$$

it follows that there is exactly one orbit of K-polarizations under $\mathrm{Aut}_K(A)$ corresponding to the $G_{\mathbb{Z}}$-orbit of φ. □

So, in the notation of Proposition 8.4, we have reduced to computing a set of representatives for the finitely many $G_{\mathbb{Z}}$-orbits inside the set

$$\{(\varphi, \pm1, \pm1) \in W_{\mathbb{Z}}\} = G(\mathbb{R}) \cdot \{(\varphi, \pm1, \pm1) \in W(\mathbb{R})\} \cap W_{\mathbb{Z}}.$$

8.5 Characterization of the relevant real orbits.

Now let us invoke the Albert classification: by Albert (see for example [MR08, §21]) the tuple $(R \otimes_{\mathbb{Z}} \mathbb{Q}, \tau_{\widetilde{\lambda}})$ falls into one of the following cases.

8.5.1 Type I.

In the first case $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a totally real number field and $\tau_{\widetilde{\lambda}}$ is trivial. Hence

$$\tau_\lambda : M_n(R \otimes_{\mathbb{Z}} \mathbb{Q}) \to M_n(\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Q})$$

is the standard transpose and

$$R \otimes_{\mathbb{Z}} \mathbb{R} \simeq \bigoplus_{R \hookrightarrow \mathbb{R}} \mathbb{R},$$

whence

$$M_n(R) \otimes_{\mathbb{Z}} \mathbb{R} \simeq M_n(R \otimes_{\mathbb{Z}} \mathbb{R}) \simeq \bigoplus_{R \hookrightarrow \mathbb{R}} M_n(\mathbb{R}),$$

and so

$$V(\mathbb{R}) \simeq \bigoplus_{R \hookrightarrow \mathbb{R}} M_n(\mathbb{R})$$

and similarly

$$V^{\mathrm{sym.}}(\mathbb{R}) \simeq \bigoplus_{R \hookrightarrow \mathbb{R}} \mathrm{Sym}^2(\mathbb{R}^{\oplus n})$$

under this isomorphism.

Thus $G(\mathbb{R}) \simeq \prod_{R \hookrightarrow \mathbb{R}} \mathrm{GL}_n(\mathbb{R})$, acting on each factor of $V^{\mathrm{sym.}}(\mathbb{R})$ independently via the action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathrm{Sym}^n(\mathbb{R}^{\oplus n}) \subseteq M_n(\mathbb{R})$ via $(g, x) \mapsto g \cdot x \cdot g^t$, or in other words the action of $\mathrm{GL}_n(\mathbb{R})$ on the quadratic form $v \mapsto v^t \cdot x \cdot v$.

Hence in particular from Sylvester's law of inertia we conclude that each $G(\mathbb{R})$-orbit on $W(\mathbb{R})$ intersects the following set at least once:

$$\left\{((\mathrm{diag}(x_i^{(v)})_{i=1}^n)_{v:R\hookrightarrow\mathbb{R}}, a, b) : a, b \in \mathbb{R}^\times, \forall i, v, x_i^{(v)} \in \{-1,0,1\}, \forall v, i<j, x_i^{(v)} \leq x_j^{(v)}\right\}.$$

In particular if $\varphi \in V^{\mathrm{sym.}}(\mathbb{R})$ has $\deg\varphi \neq 0$ and $\delta, \varepsilon \in \{\pm 1\}$, then there is a tuple $(k_v)_{v:R\hookrightarrow\mathbb{R}}$ with each $0 \leq k_v \leq n$ such that

$$G(\mathbb{R})\cdot(\varphi,\delta,\varepsilon) = G(\mathbb{R})\cdot\left(\mathrm{diag}\left(\underbrace{-1,\ldots,-1}_{k_v}, \underbrace{1,\ldots,1}_{n-k_v}\right), \frac{\delta}{\sqrt{\deg\varphi}}, \varepsilon\cdot\sqrt{\deg\varphi}\right).$$

Let us also note that the latter orbit is closed since $((X_v)_{v:R\hookrightarrow\mathbb{R}}, a, b)$ lies in said orbit if and only if $ab = \delta\varepsilon$, $b^2\cdot\prod_{v:R\hookrightarrow\mathbb{R}}\det(X_v) = \deg\varphi$, and each X_v has signature $(n-k_v, k_v)$ (a closed condition since $\det(X_v)\neq 0$ via the previous equality) — note that these conditions also allow us to check if a given $(\varphi, a, b) \in W(\mathbb{Q})$ with $ab\cdot\deg\varphi \neq 0$ lies in a given $G(\mathbb{R})$-orbit in finite time. Let us also note that $W(\mathbb{Q})$ does intersect each such orbit since e.g. the locus of matrices in $\mathrm{SL}_n(\mathbb{R})$ with given signature is both closed and open, and also that if $\varphi \in V^{\mathrm{sym.}}(\mathbb{C})$ has $\deg\varphi\neq 0$ and $\delta,\varepsilon\in\{\pm1\}$, then

$$G(\mathbb{C})\cdot(\varphi,\delta,\varepsilon) = G(\mathbb{C})\cdot\left(\mathrm{id}, \frac{\delta}{\sqrt{\deg\varphi}}, \varepsilon\cdot\sqrt{\deg\varphi}\right),$$

and now the latter orbit is Zariski closed because $((X_v)_{v:R\hookrightarrow\mathbb{R}}, a, b)$ lies in said orbit if and only if $ab = \delta\varepsilon$ and $b^2\cdot\prod_{v:R\hookrightarrow\mathbb{R}}\det(X_v) = \deg\varphi$.

8.5.2 Type II.

In the second case $R\otimes_{\mathbb{Z}}\mathbb{Q}$ is a quaternion algebra over a totally real field $K/\mathbb{Q}$ which splits at all real places and $\tau_{\widetilde{\lambda}}$ is trivial on K and such that there is an isomorphism of $\mathbb{R}$-algebras (computable by e.g. brute-force search for an element of $R\otimes_{\mathbb{Z}}\mathbb{Q}$ with totally real characteristic polynomial, i.e. for a totally real splitting field)

$$R\otimes_{\mathbb{Z}}\mathbb{R} \simeq \bigoplus_{K\hookrightarrow\mathbb{R}} M_2(\mathbb{R})$$

taking $\tau_{\widetilde{\lambda}}$ to the coordinatewise standard transpose on the right-hand side. Hence via the same isomorphism

$$M_n(R\otimes_{\mathbb{Z}}\mathbb{R}) \simeq \bigoplus_{K\hookrightarrow\mathbb{R}} M_n(M_2(\mathbb{R})) \simeq \bigoplus_{K\hookrightarrow\mathbb{R}} M_{2n}(\mathbb{R})$$

with τ_λ also taken to the coordinatewise transpose on the right-hand side. Thus exactly as in Section 8.5.1

$$V^{\mathrm{sym.}}(\mathbb{R}) \simeq \bigoplus_{K\hookrightarrow\mathbb{R}} \mathrm{Sym}^2(\mathbb{R}^{\oplus 2n})$$

and

$$G(\mathbb{R}) \simeq \prod_{K \hookrightarrow \mathbb{R}} \mathrm{GL}_{2n}(\mathbb{R})$$

with the coordinatewise action again given by $(g, x) \mapsto g{\cdot}x{\cdot}g^t$, and we conclude in exactly the same way as in Section 8.5.1 with explicit representatives for the $G(\mathbb{R})$-orbits on $W(\mathbb{R})$ as well as a finite-time algorithm to test membership of a given $(\varphi, a, b) \in W(\mathbb{Q})$ in each relevant orbit (all of which are seen to be closed — with the analogous statements for $G(\mathbb{C})$-orbits meant in the Zariski topology — and to intersect $W(\mathbb{Q})$).

8.5.3 Type III.

In the third case $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra over a totally real field $K/\mathbb{Q}$ which is ramified at all real places and $\tau_{\widetilde{\lambda}}$ is trivial on K and such that there is a computable isomorphism of $\mathbb{R}$-algebras

$$R \otimes_{\mathbb{Z}} \mathbb{R} \simeq \bigoplus_{K \hookrightarrow \mathbb{R}} \mathbb{H}$$

taking $\tau_{\widetilde{\lambda}}$ to coordinatewise canonical involution, where by the canonical involution on the Hamilton quaternions $\mathbb{H}$ we mean $(1, i, j, k) \mapsto (1, -i, -j, -k)$. Hence via the same isomorphism

$$M_n(R \otimes_{\mathbb{Z}} \mathbb{R}) \simeq \bigoplus_{K \hookrightarrow \mathbb{R}} M_n(\mathbb{H})$$

with τ_λ taken to coordinatewise conjugate transpose $X \mapsto X^\dagger$.

Thus now

$$V^{\mathrm{sym.}}(\mathbb{R}) \simeq \bigoplus_{K \hookrightarrow \mathbb{R}} \mathrm{Herm}_{n \times n}(\mathbb{H}),$$

with

$$\mathrm{Herm}_{n \times n}(\mathbb{H}) := \{X \in M_n(\mathbb{H}) : X^\dagger = X\},$$

and

$$G(\mathbb{R}) \simeq \prod_{K \hookrightarrow \mathbb{R}} M_n(\mathbb{H})^\times$$

with the coordinatewise action given by $(g, x) \mapsto g \cdot x \cdot g^\dagger$. Now instead of the Sylvester law of inertia we need a classification of Hermitian forms on $\mathbb{H}^{\oplus n}$, but this is routine — the same Gram-Schmidt argument one uses to classify quadratic forms over $\mathbb{R}$ works to classify Hermitian forms on $\mathbb{H}^{\oplus n}$ by the same data: $(d_0, d_+, d_-) \in \mathbb{N}^{\times 3}$ with $d_0 + d_+ + d_- = n$, with each form in the orbit equivalent to

$$(\alpha_i)_{i=1}^n \mapsto \sum_{i=d_0+1}^{d_0+d_+} |\alpha_i|^2 - \sum_{i=d_0+d_++1}^{n} |\alpha_i|^2.$$

So again exactly as in Sections 8.5.1 and 8.5.2 we find explicit representatives for the $G(\mathbb{R})$-orbits on $W(\mathbb{R})$ and a finite-time algorithm to test membership of a given element of $W(\mathbb{Q})$ in each relevant orbit, all of which are seen to be closed (in the real topology, while again for $G(\mathbb{C})$-orbits we mean in the Zariski topology) and to intersect $W(\mathbb{Q})$.

8.5.4 Type IV.

In the fourth case $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a central simple algebra over an imaginary CM field $K/\mathbb{Q}$ (with maximal totally real subfield $K^+/\mathbb{Q}$, say) and $\tau_{\widetilde{\lambda}}$ restricts to complex conjugation on K and is such that there is a (computable, in the same way as in e.g. Section 8.5.1) isomorphism of $\mathbb{R}$-algebras

$$R \otimes_{\mathbb{Z}} \mathbb{R} \simeq \bigoplus_{K^+ \hookrightarrow \mathbb{R}} M_k(\mathbb{C})$$

(with k the index of $R \otimes_{\mathbb{Z}} \mathbb{Q}$ over its centre K) taking $\tau_{\widetilde{\lambda}}$ to coordinatewise conjugate transpose $X \mapsto X^\dagger$. Hence via the same isomorphism

$$M_n(R \otimes_{\mathbb{Z}} \mathbb{R}) \simeq \bigoplus_{K^+ \hookrightarrow \mathbb{R}} M_{kn}(\mathbb{C})$$

with τ_λ taken to coordinatewise conjugate transpose as well.

Thus now

$$V^{\text{sym.}}(\mathbb{R}) \simeq \bigoplus_{K^+ \hookrightarrow \mathbb{R}} \mathrm{Herm}_{kn \times kn}(\mathbb{C}),$$

with

$$\mathrm{Herm}_{kn \times kn}(\mathbb{C}) := \{X \in M_{kn}(\mathbb{C}) : X^\dagger = X\},$$

and

$$G(\mathbb{R}) \simeq \prod_{K^+ \hookrightarrow \mathbb{R}} \mathrm{GL}_{kn}(\mathbb{C}),$$

with the coordinatewise action given by $(g, x) \mapsto g \cdot x \cdot g^\dagger$. So in this case we need a classification of Hermitian forms on $\mathbb{C}^{\oplus n}$, and again the usual Gram-Schmidt argument works to classify Hermitian forms on $\mathbb{C}^{\oplus n}$ by the same data: $(d_0, d_+, d_-) \in \mathbb{N}^{\times 3}$ with $d_0 + d_+ + d_- = n$, with each form in the orbit equivalent to

$$(\alpha_i)_{i=1}^n \mapsto \sum_{i=d_0+1}^{d_0+d_+} |\alpha_i|^2 - \sum_{i=d_0+d_++1}^{n} |\alpha_i|^2.$$

So again exactly as in Sections 8.5.1, 8.5.2, and 8.5.3 we find explicit representatives for the $G(\mathbb{R})$-orbits on $W(\mathbb{R})$ and a finite-time algorithm to test membership of a given element of $W(\mathbb{Q})$ in each relevant orbit, all of which are seen to be closed (in the real topology, while again for $G(\mathbb{C})$-orbits we mean in the Zariski topology) and to intersect $W(\mathbb{Q})$.

8.6 Proof of Proposition 8.4.

Now we may prove Proposition 8.4 and thus Theorem 7.8.

Proof of Proposition 8.4. Thanks to Section 8.5 we have an explicit description of the $G(\mathbb{R})$-orbits in

$$G(\mathbb{R}) \cdot \{(\varphi, \pm 1, \pm 1) \in W(\mathbb{R})\},$$

and we moreover may and will assume (via e.g. brute-force) that inside each such $G(\mathbb{R})$-orbit we have chosen a representative lying in $W(\mathbb{Q})$.

So let $v \in W(\mathbb{Q})$ be said representative. It suffices then to explain how to compute representatives for the $G_{\mathbb{Z}}$-orbits in

$$(G(\mathbb{R}) \cdot v) \cap W_{\mathbb{Z}}.$$

Let $q \in \mathbb{Z}^+$ be such that $q \cdot v \in W_{\mathbb{Z}}$. Let $\Gamma := \frac{1}{q} \cdot W_{\mathbb{Z}}$. Then certainly $\Gamma \subseteq W(\mathbb{R})$ is a lattice invariant under $G_{\mathbb{Z}}$. Let $X := G(\mathbb{R}) \cdot v$ — note that in Section 8.5 we saw that $X \subseteq V(\mathbb{R})$ is Zariski closed. But now we are done by Lemma 8.9, because a $G_{\mathbb{Z}}$-orbit intersects $W_{\mathbb{Z}}$ if and only if it lies entirely inside $W_{\mathbb{Z}}$. □

8.7 Making algorithmic a result of Borel and Harish-Chandra.

In this section we prove Lemma 8.9, which shows how to find all integral orbits in a given real orbit of an algebraic group given a single rational point in the real orbit. This is a matter of effectivizing [BHC62a, Theorem 6.9], using work of Grunewald and Segal [GS80].

We begin by recalling some notation.

Definition 8.5. *Fix rational numbers $t > \frac{2}{\sqrt{3}}$ and $u > 1/2$. The* standard Siegel set *is the set $\mathcal{S} \subseteq \mathrm{GL}_n(\mathbb{R})$ defined by*

$$\mathcal{S} = \mathcal{S}_{t,u} = KA_tN_u,$$

where $K = O_n(\mathbb{R})$, A_t is the set of diagonal matrices with diagonal entries a_i satisfying $a_i \leq ta_{i+1}$, and N_u is the set of unipotent upper triangular matrices, with off-diagonal entries x_{ij} satisfying $|x_{ij}| \leq u$.

(The definition of $\mathcal{S}$ depends on t and u, but we will suppress this dependence in our discussion. The reader is free to choose once and for all some particular values t and u.)

For convenience we record a simple lemma involving bounding products of matrices.

Lemma 8.6. *For every $M > 0$, let*

$$\Omega_M := \{g = (g_{ij}) \in \mathrm{GL}_n(\mathbb{R}) \mid |g_{ij}| < M \text{ and } |\det g| > 1/M\}.$$

Then: $\Omega_{M_1}\Omega_{M_2} \subseteq \Omega_{nM_1M_2}$ and $\Omega_{M_1}^{-1} \subseteq \Omega_{n! \cdot M^n}$.

Proof. Evident. □

Lemma 8.7. *Let $G = \mathrm{GL}_n$, and let $\pi\colon G \to \mathrm{GL}(V)$ be a representation of the algebraic group G, defined over $\mathbb{Q}$.*

Let $\theta\colon g \mapsto (g^{\mathsf{T}})^{-1}$ be the standard Cartan involution (transpose inverse) on G. Let $v \in V(\mathbb{R})$ be a point whose orbit under G is closed and whose isotropy group G_v is stable under θ. Let $\mathcal{S}$ be a standard Siegel set (Definition 8.5) in G. Let $\Gamma \subseteq V(\mathbb{Q})$ be a lattice.

Then one can compute algorithmically the finite set $v \cdot \pi(\mathcal{S}) \cap \Gamma$.

Remark 8.8. *This is just a matter of going carefully through the proof of [BHC62a, Lemma 5.4] in the particular case of interest to us, i.e. $G = \mathrm{GL}_n$, and making every step effective.*

(In fact, the particular case $G = \mathrm{GL}_n$ is the only situation in which Borel and Harish-Chandra use the result.)

Proof. Let A be the torus of diagonal matrices in $G = \mathrm{GL}_n$. The vector space V splits (over $\mathbb{Q}$) as a direct sum of eigenspaces V_i for the action of A, and we can explicitly compute the eigenspaces V_i by linear algebra. Choose a Euclidean norm $v \mapsto |v|$ on V for which the V_i's are mutually orthogonal.

For each eigenspace V_i, let $E_i\colon V \to V_i$ denote the projection of V onto V_i. Since V, V_i and E_i are all defined over $\mathbb{Q}$, the projection $E_i(\Gamma)$ is again a lattice in V_i, which can be computed effectively. Hence, we can compute a constant c such that if $w \in \Gamma$ and $E_i(w) \neq 0$, then $|E_i(w)| \geq c$.

Now consider variable k, a, n, with $k \in K = \mathrm{O}(n)$, $a \in A_t$, $n \in N_u$, so that

$$x = kan \in \mathcal{S}$$

is an arbitrary element of $\mathcal{S}$. (Here A_t and N_u are as in Definition 8.5.)

Let $w = v \cdot x$, and define

$$\begin{aligned} y &:= xa^{-1} = kana^{-1} \\ z &:= xa^{-2} = kana^{-2}. \end{aligned}$$

Note that ana^{-1} is a unipotent upper-triangular matrix whose off-diagonal entries are bounded in absolute value by $t^{n-1}u$. Since K is orthogonal, its entries are bounded as well (by 1), so we can compute a bound on the absolute value of the matrix entries of y. (In fact, by matrix multiplication, the entries of y are clearly bounded by $n\max(1, t^{n-1}u)$.) Since the action of G on V is explicitly presented, we can compute a bound on $|v \cdot y| = \left|w \cdot a^{-1}\right|$, independent of x. Write the bound as $|v \cdot y| \leq c'$.

It follows (see [BHC62a]) that $|E_i(v \cdot z)| \leq (c')^2/c$, for all choices of k, a, n, and for all i. Therefore, we can effectively compute a bound $|v \cdot z| \leq c''$.

Let Q be the closed ball of radius c'' about the origin in V. We want to produce a compact subset $\Omega \subseteq G$ such that

$$(v \cdot \pi(G)) \cap Q \subseteq v \cdot \pi(\Omega).$$

The existence of Ω is given by [BHC62a, Lemma 5.2], which is not effective.

To produce Ω, we will apply a theorem of Tarski (see [GS80, §1.2]). We will consider only $\Omega \subseteq G$ of the form

$$\Omega_M = \{g = (g_{ij}) \in G \mid |g_{ij}| < M \text{ and } |\det g| > 1/M\}.$$

Since every compact $\Omega \in G$ is contained in some Ω_M, we know that Ω_M has the desired property for all sufficiently large M. But now we have reduced to a standard quantifier elimination problem! We simply need to find some M for which the following statement holds:

> For every $v' \in V$ and $g \in G$ such that $|v'| \leq c''$ and $v \cdot g = v'$, there exists $g' \in \Omega_M$ such that $v \cdot g' = v'$.

Such an M must exist by [BHC62a, Proposition 5.2], so Tarski's algorithm (in the form of [GS80, Algorithm 1.2.1]) will find one. (Literally, [GS80, Algorithm 1.2.1] only finds M approximately: that is, it will give some interval $(M_{\text{approx}} - \epsilon, M_{\text{approx}} + \epsilon)$ which is guaranteed to contain an M that works. But if M has the desired property, any $M' > M$ does as well, so in particular $M' = M_{\text{approx}} + \epsilon$ will do the job.)

Returning to our effectivization of [BHC62a, Lemma 5.3], we see that for any k, a, n as above, the vector $v \cdot z$ satisfies $v \cdot z \in v \cdot \Omega_M$, so $z \in G_v \Omega_M$. In other words,

$$ka^{-1}a^2na^{-2} \in G_v \Omega_M.$$

We can compute an explicit bound on the coeffcients of a^2na^{-2} (and of course this matrix has determinant 1), whence we obtain M_1 such that

$$a^2na^{-2} \in \Omega_{M_1}.$$

Thus, we can compute (by Lemma 8.6) M_2 such that

$$ka^{-1} = ka^{-1}(a^2na^{-2})(a^2na^{-2})^{-1} \in G_v \Omega_M \Omega_{M_1} \subseteq G_v \Omega_{M_2}.$$

Applying θ, we note that $\theta(k) = k$, $\theta(a^{-1}) = a$, G_v is invariant under θ, and one can compute M_3 such that $\theta(\Omega_{M_2}) \subseteq \Omega_{M_3}$. Hence, we obtain

$$ka \in G_v \Omega_{M_3}.$$

Finally, the bounds on the coefficients of n give an M_4 such that $n \in \Omega_{M_4}$, so we can find M_5 such that

$$kan \in G_v \Omega_{M_5}.$$

Thus $w = v \cdot x = v \cdot kan \in v \cdot \Omega_{M_5}$, so one can compute effective bounds on $|w|$. This gives a computable finite list of possible vectors w, which is guaranteed to contain the finite set $v \cdot \pi(\mathcal{S}) \cap \Gamma$.

Finally, we test each vector w on our list, using Tarski's algorithm [GS80, Algorithm 1.2.1] to determine whether it lies in $\pi(\mathcal{S})$. □

Lemma 8.9. *Let G be a connected reductive group defined over $\mathbb{Q}$, $\pi\colon G \to \mathrm{GL}(V)$ a representation defined over $\mathbb{Q}$, Γ a $\mathbb{Z}$-lattice in $\mathbb{Q}$-vector space V invariant under $G_{\mathbb{Z}}$, and X a closed orbit of $G_{\mathbb{R}}$ on $V_{\mathbb{R}}$. Suppose $v_0 \in \Gamma \cap X$ is a given point.*

There is an algorithm that takes as input G, π, Γ, v_0, and returns a list of points

$$v_0, v_1, \ldots, v_n \in \Gamma \cap X$$

such that

$$\Gamma \cap X = \bigcup_{i=0}^{n} G_{\mathbb{Z}} \cdot v_i.$$

Remark 8.10. *This is essentially just a matter of making effective the proof of [BHC62b, 6.9]. That proof has one essential ineffectivity: it does not say how to determine whether $\Gamma \cap X$ is empty. We do not know how to solve this problem algorithmically, in general; we solve it explicitly in the cases we need (Section 8.5).*

In fact, [BHC62b, 6.5 (i)] is made algorithmic by [GS80, 5.3.1], so we need only explain how to reduce [BHC62b, 6.9] to [BHC62b, 6.5 (i)].

Proof. G is given as a subgroup, defined over $\mathbb{Q}$, of some $G' = GL_n$. Let $H \subseteq G$ be the stabilizer of v_0. By [GS80, Algo. 5.1.1], we can find a rational representation

$$\rho\colon G' \to GL(W),$$

and a vector $w \in W$, such that

1. H is the stabilizer of w in W, and
2. $w \cdot \rho(G')$ is closed in W.

Let $X' = w \cdot \rho(G)$ be the orbit of w under the subgroup $G \subseteq \mathrm{GL}_n$. There is a unique G-equivariant isomorphism of $\mathbb{Q}$-schemes $\varphi\colon X \to X'$ such that $\varphi(v_0) = w$ (see the proof of [BHC62b, 6.9]). In fact, since X and X' are both affine schemes, the coordinates of φ can be written explicitly as polynomials. Choosing coordinates x_i on V and y_i on W, the map φ is given by polynomials $(P_1, \ldots, P_s)$ with rational coefficients such that $y_i(\varphi(x_1, \ldots, x_r)) = P_i(x_1, \ldots, x_r)$. The inverse morphism φ^{-1} is given by polynomials over $\mathbb{Q}$ as well. The pair (φ, φ^{-1}) can be computed by brute-force search.

Let $\Gamma' \subseteq W$ be a $\mathbb{Z}$-lattice, containing $\varphi(\Gamma)$ and invariant under the action of the group $G'_{\mathbb{Z}} = \mathrm{SL}_n(\mathbb{Z})$.

(The next step effectivizes [BHC62b, Lemma 6.8].) First, find (by brute-force search) an $a \in \mathrm{SL}_n(\mathbb{R} \cap \overline{\mathbb{Q}})$ such that aGa^{-1} and aHa^{-1} are self-adjoint as subgroups of SL_n. Such an a is guaranteed to exist: [BHC62b, Lemma 1.9] gives the existence of an $a \in \mathrm{SL}_n(\mathbb{R})$ such that aGa^{-1} and aHa^{-1} are self-adjoint. But the condition that aGa^{-1} and aHa^{-1} be self-adjoint is an algebraic condition on a, so in fact we can take a to have coefficients algebraic numbers.

By [GS80, Algorithm 5.3.1], we can find finitely many elements $b_i \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$G(\mathbb{R}) = \bigcup_i \left(G(\mathbb{R}) \cap a^{-1}\mathcal{S}b_i\right) \dot{G}(\mathbb{Z}),$$

where $\mathcal{S}$ is the standard Siegel set (Definition 8.5).

Now apply Lemma 8.7 (to the group GL_n, the representation W, the lattice Γ', and the vector $w \cdot a^{-1}$ to determine the finite set $w \cdot a^{-1}\mathcal{S} \cap \Gamma$. (By the choice of a, the stabilizer aHa^{-1} of $w \cdot a^{-1}$ is self-adjoint under the standard Cartan involution on GL_n; the other hypotheses of Lemma 8.7 are immediate.)

For each i, apply b_i to $w \cdot a^{-1}\mathcal{S} \cap \Gamma$ to obtain the finite set $w \cdot a^{-1}\mathcal{S}b_i \cap \Gamma$. Compute the union F_0 of these finite sets, over all the b_i computed earlier. Since $G(\mathbb{R}) = \bigcup_i \left(G(\mathbb{R}) \cap a^{-1}\mathcal{S}b_i\right) \dot{G}(\mathbb{Z})$, the set F_0 contains a representative for each orbit of $G(\mathbb{Z})$ on X'. Test each point of F_0 to determine whether it lies in X'; let $F_1 = F_0 \cap X'$.

Finally, apply the isomorphism $\varphi^{-1} \colon X' \to X$ to each point in F_1, and test the resulting points to determine which lie in the lattice Γ. Let F be the set of point of $\varphi^{-1}(F_1)$ lying in Γ; this F is the desired set. □

9 The homology of an abelian variety.

In this section we show how to explicitly compute the singular homology of an abelian variety over $\mathbb{C}$, which enables us to perform computations on endomorphisms and polarizations in exact integer coordinates.

Lemma 9.10 gives the action of an endomorphism on singular homology; we use it in the computation of the endomorphism ring. Lemma 9.11 enables us to write the Chern class of a polarization in exact integer coordinates.

Lemma 9.1. *There is an algorithm that takes as input an abelian variety A over a number field K, and returns a K-basis for $\Gamma(A, \Omega^1_A)$.*

Proof. Let e be the origin on A. Let $u_1, \ldots, u_g$ for a basis for $(T_e A)^\vee$, the cotangent space to A at e.

For each $1 \leq i \leq g$, compute ω_i by "translating u_i around A". Concretely, let

$$\Delta = \{(x, -x) \mid x \in A\} \subseteq A \times A$$

be the antidiagonal, and let $m \colon A \times A \to A$ be the multiplication map, so that $\Delta = m^{-1}(e)$, and $m^* u_i \in T(A \times A)^\vee|_\Delta$ is a differential vanishing along Δ.

With the natural identification

$$T(A \times A)^\vee = \pi_1^* T_A \oplus \pi_2^* T_A,$$

let ι_1 denote the projection onto the first factor:

$$\iota_1(\pi_1^* \omega_1 + \pi_2^* \omega_2) = \pi_1^* \omega_1.$$

Finally, let $\delta \colon A \to \Delta$ be the inclusion

$$\delta(x) = (x, -x).$$

Then (for $1 \leq i \leq g$)

$$v_i = \delta^* \iota_1 (m^* u_i)$$

is a translation-invariant section of $\Omega_1(A)$ restricting to u_1 at e; the sections $v_1, \ldots, v_g$ form the desired basis of $\Gamma(A, \Omega_1(A))$. □

Notation 9.2. *Let A be an abelian variety of dimension g over a number field K, and suppose given some complex embedding of K. Suppose $\omega_1, \ldots, \omega_g$ form a basis for $\Gamma(A, \Omega^1_A)$.*

Then there is a unique complex-analytic map $\exp \colon \mathbb{C}^g \to A$ *such that* $\exp^* \omega_i = dz_i$ *for each i.*

(In other words: A is uniformized by $\mathbb{C}^g$; the uniformizing map $\exp \colon \mathbb{C}^g \to A$ *is well-defined up to linear automorphisms of $\mathbb{C}^g$, and we use the basis ω_i of $\Gamma(A, \Omega^1_A)$ to specify the map* $\exp$*.)*

We call this $\exp$ *the* uniformization of A corresponding to the basis ω_i.

Lemma 9.3. *(Effective inverse function theorem.)*

Suppose $U \subseteq \mathbb{C}^n$ is a neighborhood of a point e, and $f\colon U \to \mathbb{C}^n$ is a holomorphic function.

Suppose the differential df_e of f at e is invertible, and suppose ϵ and $c < 1$ are chosen such that, for all $x \in B_\varepsilon(e)$,

$$\|df_e^{-1}(df_x - df_e)\| \leq c.$$

Then:

- *f is injective on $B_\varepsilon(e)$.*
- *$f(e) + df_e(B_{(1-c)\varepsilon}(0))) \subseteq f(B_\varepsilon(e)) \subseteq f(e) + df_e(B_{(1+c)\varepsilon}(0)))$.*
- *The inverse function of f can be computed effectively: for any $y \in f(e) + df_e(B_{(1-c)\varepsilon}(0)))$, one can compute to arbitrary precision its unique inverse image $f^{-1}(y) \in B_\varepsilon(e)$.*

Proof. This is a standard application of the contraction mapping principle (see for example [Tao16, Lemma 6.6.6]). To compute $f^{-1}(y)$, simply iterate the contraction mapping

$$x \mapsto x + df_e^{-1}(y - f(x)).$$

□

Lemma 9.4. *Let $X \subseteq \mathbb{A}^N$ be an algebraic variety of dimension g over a number field K (with fixed complex embedding) and let e be a smooth point of X. Equip $\mathbb{A}^N(\mathbb{C}) = \mathbb{C}^N$ with the standard Euclidean metric.*

There is an algorithm to find some g of the N coordinates on $\mathbb{A}^N$ – say $x_{i_1}, x_{i_2}, \ldots, x_{i_g}$ – so that the resulting map $\pi\colon X \to \mathbb{A}^g$ is invertible in a neighborhood of e (for the classical topology on X^{an}).

Furthermore, there is an algorithm to find an ϵ such that, if $B_\varepsilon(e)$ is the ball of radius ϵ about e, then

- *the restriction of π to $B_\varepsilon(e) \cap X$ is invertible, and*
- *$B_\varepsilon(e) \cap X$ is contained in a contractible subset of X.*

Finally, there is an algorithm to find an ϵ_1 such that $B_{\epsilon_1}(\pi(e)) \subseteq \pi(B_\varepsilon(e))$. The inverse function to π can be computed algorithmically on $B_{\epsilon_1}(\pi(e))$ (to arbitrary precision).

Proof. The algebraic variety X comes presented as the vanishing locus of a collection of polynomials in N variables. That X is smooth at e implies that there are $N-g$ of these polynomials, say $f_1, \ldots, f_{N-g}$, whose differentials are linearly independent in $(T_e\mathbb{A}^N)^\vee$; these polynomials can be found (among the finitely many defining polynomials for X) by standard methods of linear algebra.

One can then choose indices $i_1, \ldots, i_g$ so that $df_1, \ldots, df_{N-g}, dx_{i_1}, \ldots, dx_{i_g}$ form a basis for $(T_e\mathbb{A}^N)^\vee$.

For dimension reasons, X locally coincides which the vanishing locus $Z = Z(f_1, \dots, f_{N-g})$; in other words, there is some open set $U \ni e$ such that

$$X \cap U = Z \cap U.$$

We will apply an effective form of the inverse function theorem to the map $F \colon \mathbb{C}^n \to \mathbb{C}^n$ given by

$$F(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_{N-g}(x_1, \dots, x_n), x_{i_1}, \dots, x_{i_g}).$$

We have arranged that $dF_e \colon \mathbb{C}^N \to \mathbb{C}^N$ is invertible.

Let $Y \subseteq \mathbb{C}^N$ be the set of points whose first $N - g$ coordinates vanish, so we have the relations

$$X \subseteq Z = F^{-1}(Y).$$

Equip $\mathbb{C}^N$ with the standard Euclidean metric. For variable $x \in \mathbb{C}^n$, consider the linear transformation

$$G(x) = dF_e^{-1} \circ (dF_x - dF_e).$$

We have $G(e) = 0$. Since G is continuous, we can find ϵ such that, whenever $|x - e| < \epsilon$, all matrix entries of $G(x)$ are less than $1/2g^2$. (In fact the matrix entries of G are polynomials in x, and so one can find such ϵ algorithmically.)

Now by Lemma 9.3 F is invertible on $B_\varepsilon(e)$. Hence, F maps $B_\varepsilon(e)$ invertibly to some neighborhood of $F(e)$. By Lemma 9.3 again,

$$B_{\varepsilon/4}(e) \subseteq F^{-1}B' \subseteq B_\varepsilon(e),$$

where B' is the image of $B_{\varepsilon/2}(e)$ under the affine-linear map

$$x \mapsto F(e) + dF_e(x - e).$$

Now B' is an ellipsoid, so its intersection with any coordinate plane is also an ellipsoid. In particular, $Y \cap B'$ is simply connected. Since F is a homeomorphism on $F^{-1}(B')$, the set

$$F^{-1}(Y \cap B') = Z \cap F^{-1}(B')$$

is simply connected as well. In particular, $Z \cap F^{-1}(B')$ is contained in a single irreducible component of Z, so $Z \cap F^{-1}(B') \subseteq X$.

It now follows that $B_{\epsilon/4}(e)$ satisfies the conditions of the lemma: the restriction of π to $B_{\epsilon/4}(e) \cap X$ is invertible, and $B_{\epsilon/4}(e) \cap X$ is contained in a contractible subset of X.

Let $\frac{1}{4}B'$ be the image of $B_{\varepsilon/8}(e)$ under $x \mapsto F(e) + dF_e(x - e)$. By Lemma 9.3 yet again,

$$\frac{1}{4}B' \subseteq \pi(B_{\epsilon/4}(e)).$$

Thus if we take ϵ_1 small enough that $B_{\epsilon_1}(\pi(e)) \subseteq \frac{1}{4}B'$, we have $B_{\epsilon_1}(\pi(e)) \subseteq \pi(B_\varepsilon(e))$.

Computability of the inverse function follows from Lemma 9.3. □

Lemma 9.5. *Let A be an abelian variety over a number field with chosen complex embedding. Suppose a basis for $\Gamma(A, \Omega_A^1)$ has been chosen as in Lemma 9.1, and let $\exp\colon \mathbb{C}^g \to A$ be the uniformizing map defined in Notation 9.2.*

One can explicitly compute an open ball $B = B_\varepsilon(0)$ about the origin in $\mathbb{C}^g$ and an open neighborhood B' of e in A such that $\exp(B) \subseteq B'$, and B' is contained in a simply connected subset of A. Furthermore, the map $\exp$ can be computed algorithmically to arbitrary precision on B.

Proof. Apply Lemma 9.4 to the smooth point e of the smooth variety A; Lemma 9.4 returns a projection

$$\pi\colon U \to \mathbb{A}^g$$

from some open $U \subseteq A$ onto some g of the N standard coordinates on an affine coordinate patch $\mathbb{A}^N \subseteq \mathbb{P}^N$, as well as an algorithmically-computable ϵ_0 such that $B' = B_{\varepsilon_0}(e) \cap A$ is contained in some simply-connected subset Ω of A.

Since $\exp\colon \mathbb{C}^g \to A$ is the universal cover of A, we can invert $\exp$ canonically on Ω by requiring that $\exp^{-1}(e) = 0$; this gives a well-defined inverse $\exp^{-1}$ on B', which we will use without further comment.

$$\begin{tikzcd}
\exp^{-1}(B') \arrow[r, "\exp"] \arrow[d, hook] & B' \arrow[r, "\gamma"] \arrow[d, hook] & \mathbb{C}^g \\
\mathbb{C}^g \arrow[r] & A &
\end{tikzcd}$$

Now we want to apply Lemma 9.3 to the map

$$\exp^{-1} \circ \gamma^{-1}\colon \gamma(B') \to \mathbb{C}^g.$$

To estimate $d(\exp^{-1} \circ \gamma^{-1})$, we will work with differentials on A. At any $a \in B \subseteq A$, we can express each ω_i as a linear combination of the differentials $\gamma^* dt_i$. Specifically, one can compute (exactly) rational functions M_{ij} on A such that

$$\omega_i = \sum_i M_{ij} \gamma^* t_j.$$

But now these M_{ij} exactly give the differential of $\exp^{-1} \circ \gamma^{-1}$! Specifically, if $M(x)$ denotes the matrix whose i, j entry is $M_{ij}(x)$, we have

$$d(\exp^{-1} \circ \gamma^{-1})_a = M(\gamma^{-1}(a)).$$

Now apply Lemma 9.3. We can find ϵ such that, if $x \in \gamma^{-1}C$, then

$$\|M(e)^{-1}(M(x) - M(e))\| < 1/2.$$

And we are done! Specifically: Lemma 9.3 tells us that $M(e)^{-1}B_{\epsilon/2}(0) \subseteq \exp^{-1} \circ \gamma^{-1}(\exp^{-1} \circ \gamma^{-1})$, so any ball B contained in $M(e)^{-1}B_{\epsilon/2}(0)$ does the job.

Finally, note that both $\gamma \circ \exp$ and γ^{-1} can be computed numerically by Lemma 9.4, so their composition $\exp$ can as well. □

Lemma 9.6. *There is an algorithm to compute the inverse of the uniformizing map* $\exp$ *on the open set $B' \subseteq A$ computed in Lemma 9.5. Specifically, the algorithm takes as input $x \in B' \subseteq A$, and returns an estimate to arbitrary precision of the unique inverse image* $\exp^{-1}(x) \in B \subseteq \mathbb{C}^g$.

Proof. Numerical integration.

We have

$$\exp^{-1}(x) = \int_e^x (\omega_1, \ldots, \omega_g);$$

the path from e to x is uniquely determined because B' is simply connected. □

Lemma 9.7. *(compute* $\exp$ *of a point)*

There is an algorithm to compute $\exp(x) \in A$ *to arbitrary precision, for any* $x \in \mathbb{C}^g$.

Proof. This follows from Lemma 9.5 and the fact that $\exp$ is a group homomorphism.

Find some integer n such that $\frac{1}{n}x \in B$, and compute

$$\exp(x) = [n]\exp\left(\frac{1}{n}x\right),$$

where $[n]\colon A \to A$ is multiplication by n. □

Lemma 9.8. *Equip $\mathbb{R}^n$ with the standard Euclidean metric, and let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Suppose r is large enough that $B_r(0) \cap \Lambda$ contains n linearly independent vectors. Then:*

1. *Let $a_n = \frac{\sqrt{n}}{2}$. For any $w \in \mathbb{R}^n$, the intersection $B_{a_n}(w) \cap \Lambda$ is nonempty.*
2. *Let $b_n = \max(1, a_n)$. Then $B_{b_n r}(0) \cap \Lambda$ contains a set of vectors that generates Λ.*

Proof. Induction on n. (The base case, either $n = 0$ or $n = 1$, is trivial.)

Let $v_1, \ldots, v_n$ be the n independent vectors in $B_r(0) \cap \Lambda$. For convenience, perform an orthogonal change of coordinates on $\mathbb{R}^n$ so that $v_1, \ldots, v_{n-1}$ have $x_n = 0$. The projection of Λ onto the x_n-axis is a one-dimensional lattice, generated by, say, $z > 0$. Note that $|z| < r$.

We begin with (1). Translating w by some element of Λ, we may assume that w has x_n-coordinate $|x_n(v)| \leq z/2 < r/2$. Apply the inductive hypothesis to w', the (orthogonal) projection of w onto the hyperplane $x_n = 0$; this produces some $\lambda \in \Lambda$ with

$$|\lambda - w'| < r\sqrt{n-1}/2,$$

whence

$$|\lambda - w| < r\sqrt{n}/2.$$

This proves (1).

We now turn to (2). Let Λ_0 be the intersection of Λ with the hyperplane $x_n = 0$. By the inductive hypothesis, Λ_0 is generated by $B_{nr}(0) \cap \Lambda_0$.

The projection of Λ onto the x_n-axis is a one-dimensional lattice, generated by, say, $z > 0$. Suppose v_n has x_n-coordinate kz, for some nonzero $k \in \mathbb{Z}$. We need to show that $B_{b_n r}(0) \cap \Lambda$ contains some vector with x_n-coordinate z.

If $k = \pm 1$ then v_n is the desired vector and there is nothing to prove. Hence we may assume that $|k| \geq 2$, which implies that $|z| < r/2$. Now the intersection of Λ with the hyperplane $x_n = z$ is a torsor for Λ. By part (1), this torsor contains some point λ within $a_{n-1}r$ of the point $(0, 0, \ldots, 0, z)$. Then this λ has length at most $b_n r$, and the proof is complete. □

Lemma 9.9. *One can explicitly compute, to any desired precision, a basis for $H_1(A, \mathbb{Z})$ as a lattice in the uniformizing space $\mathbb{C}^g$.*

Proof. We can identify $H_1(A, \mathbb{Z})$ with the kernel of $\exp$. The idea is simply to evaluate $\exp$ on points in a sufficiently fine mesh.

Let $B \subseteq \mathbb{C}^g$ and $B' \subseteq A$ be as in Lemma 9.5. That is, $B \subseteq \mathbb{C}^g$ is a ball on which $\exp$ is invertible, and the inverse is explicitly computable (Lemmas 9.5 and 9.6).

Let a_n and b_n be the (explicit) constants in Lemma 9.8. Suppose B has radius ϵ. Consider the lattice

$$\Lambda = \frac{\epsilon}{a_n}(\mathbb{Z} + i\mathbb{Z})^g \subseteq \mathbb{C}^g.$$

For any $x \in H_1(A, \mathbb{Z})$, the set $B_\epsilon(x) \cap \Lambda$ is nonempty by Lemma 9.8. That is, there exists λ "near x", in the lattice Λ, for which $\exp(\lambda) \in B'$. Conversely, if $\exp(\lambda) \in B'$, by Lemma 9.6, we can compute (to arbitrary precision some x "near λ" such that $x \in H_1(A, \mathbb{Z})$.

To finish, we simply perform a brute-force search over points $\lambda \in \Lambda$ (sorted by length). For each $\lambda \in \Lambda$, we compute $\exp(\lambda)$; if $\exp(\lambda) \in B'$, we compute x near λ with $x \in H_1(A, \mathbb{Z})$. Eventually, this procedure will generate a set of g linearly-independent vectors x; let r be the maximum of their lengths.

These g vectors will span $H_1(A, \mathbb{Z})$ as a $\mathbb{Q}$-vector space, but maybe not as a $\mathbb{Z}$-lattice. To find generators as a $\mathbb{Z}$-lattice, search all vectors $\lambda \in \Lambda$ of length $\leq b_n r + \epsilon$ to find all $x \in H_1(A, \mathbb{Z})$ of length at most $b_n r$. By Lemma 9.8, these vectors x will generate $H_1(A, \mathbb{Z})$. □

Lemma 9.10. *Let $f : A \to B$ be abelian varieties over a number field K, and suppose given some complex embedding of K. Then one can explicitly compute the action of f on homology, as a map $H_1(A, \mathbb{Z}) \to H_1(B, \mathbb{Z})$, in exact integers, in terms of a basis given by Lemma 9.9.*

Proof. Compute $f^* : \Gamma(B, \Omega^1(B)) \to \Gamma(A, \Omega^1(A))$ in exact coordinates over the number field K. Lemma 9.9 gives approximate coordinates (to arbitrary precision) for the isomorphism

$$H_1(A, \mathbb{Z}) \cong \Gamma(A, \Omega^1(A))^\vee,$$

and similarly for B (where $H_1(A,\mathbb{Z})$ is represented in terms of an integral basis, and $\Gamma(A,\Omega^1(A))^\vee$ in terms of Kähler differentials defined over K). Composing the three maps, we obtain approximate coordinates for

$$H_1(f) : H_1(A,\mathbb{Z}) \to H_1(B,\mathbb{Z}).$$

But since this is a morphism of $\mathbb{Z}$-modules, we can determine the coordinates as exact integers. □

Lemma 9.11. *Let A be a projectively embedded abelian variety over a number field K equipped with a choice of complex embedding $K \hookrightarrow \mathbb{C}$.*

One can compute (in terms of exact integers) the Chern class of $\mathcal{O}(1)|A$ as an element of $H^2(A,\mathbb{Z}) = \wedge^2 H_1(A,\mathbb{Z})^\vee$ (in terms of a basis for $H_1(A,\mathbb{Z})^\vee$ given e.g. by Lemma 9.9).

Proof. Numerical integration.

Let ω be the $(1,1)$-form on the ambient projective space given by the Fubini–Study metric. Concretely, let $\mathbb{P}^N$ be described by projective coordinates $[Z_0 : Z_1 : \cdots : Z_N]$, and on the affine patch given by points of the form $(1, z_1, z_2, \ldots, z_n)$, the differential form ω is given by

$$\omega = \frac{1}{\pi}\frac{1}{\left(1+\sum_i |z_i|^2\right)^2}\sum_i dz_i \wedge d\overline{z_i}.$$

(Make the obvious modifications to determine ω on the other N standard affine patches that cover $\mathbb{P}^N$.)

To determine the class of ω in $H^2(A)$, it suffices to compute

$$\int_{\gamma_1\times\gamma_2} \omega(x_1+x_2)$$

as γ_1, γ_2 range over a basis for $H_1(A)$. (In other words: we have a map $\gamma_1 \times \gamma_2 \to A$ given by $(x_1,x_2) \mapsto x_1 + x_2$, where addition represents the group law on A. We pull ω back to the torus $\gamma_1 \times \gamma_2$ and integrate.) By numerical integration we can determine this integral to arbitrary precision; in particular, since its value is guaranteed to be an integer, we can determine its value exactly. □

10 Algorithmic decomposition of $\mathbb{Q}_\ell$-algebras.

In this and the following section, all algebras and vector spaces considered are finite-dimensional.

Proposition 10.1. *There is a finite-time algorithm which, on input $(N, E_{\mathbb{Q}}, V_{\mathbb{Q}}, \rho_{\mathbb{Q}})$ with $N \in \mathbb{Z}^+$, $E_{\mathbb{Q}}$ a semisimple algebra over $\mathbb{Q}$, $V_{\mathbb{Q}}$ a $\mathbb{Q}$-vector space, and $\rho_{\mathbb{Q}} : E_{\mathbb{Q}} \to \operatorname{End}_{\mathbb{Q}}(V_{\mathbb{Q}})$, outputs $(s, (\widetilde{e}_i)_{i=1}^s, (n_i)_{i=1}^s, (V_i)_{i=1}^s,)$ with $s \in \mathbb{N}$, $\widetilde{e}_i \in E_{\mathbb{Q}}$, $n_i \in \mathbb{Z}^+$, and the V_i pairwise distinct simple E-modules such that there is an isomorphism*

$$V \cong \bigoplus_{i=1}^{s} V_i^{\oplus n_i} \tag{1}$$

of E-modules, and such that $\widetilde{e}_i \equiv e_i \pmod{\ell^N}$ with each e_i projection onto the i-th summand (i.e. $V_i^{\oplus n_i}$), where $E := E_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ and $V := V_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

Proposition 10.2. *There is a finite-time algorithm which, on input E a semisimple algebra over $\mathbb{Q}_\ell$, outputs $(s, (\widetilde{e}_i)_{i=1}^s, (n_i)_{i=1}^s, (K_i)_{i=1}^s, (q_i)_{i=1}^s)$, where*

$$E \cong \bigoplus_{i=1}^{s} M_{n_i}(E_i). \tag{2}$$

Here E_i is the central simple algebra over the field K_i with invariant q_i, and $\widetilde{e}_i$ is an approximate idempotent in E projecting onto $M_{n_i}(E_i)$.

We will begin with a general structure theorem.

Proposition 10.3. *Let E be a semisimple algebra over $\mathbb{Q}_\ell$. Then we have a decomposition $E \cong \bigoplus_i M_{n_i}(E_i)$, where each E_i is a division algebra over a finite extension of $\mathbb{Q}_\ell$. (The E_i's need not be distinct.)*

For each summand $M_{n_i}(E_i)$ in the decomposition, $E_i^{\oplus n_i}$ is a simple left E-module, and all simple left E-modules are of this form.

Each of the division algebras E_i has a unique maximal order $\mathcal{O}_{E_i}$. The maximal orders of E are exactly the conjugates in E of $\bigoplus_i M_{n_i}(\mathcal{O}_{E_i})$.

The trace pairing $(x, y) \mapsto \operatorname{Tr}_{E/\mathbb{Q}_\ell}(xy)$ defines a perfect $\mathbb{Q}_\ell$-bilinear pairing $E \times E \to \mathbb{Q}_\ell$.

Proof. Let $Z(E)$ be the center of E. This $Z(E)$ decomposes as a direct sum of fields. Let $e_1, \ldots, e_k \in Z(E)$ be elementary idempotents, so each $e_i Z(E)$ is a field summand of $Z(E)$. Then the e_i's are orthogonal idempotents in E as well, so we have the decomposition $E = \bigoplus_i e_i E$.

Passing to a direct summand, we may assume that $Z(E)$ is a field. In other words, E is a central simple algebra over the field $Z(E)$. In this case, it is well-known (see for example [Wei95, IX.1, Theorem 1]) that E must be of the form $M_n(E_0)$, for E_0 a division ring over $Z(E)$, and every simple left E-module is isomorphic to $E_0^{\oplus n}$.

Next we turn to the question of maximal orders. It is well-known ([Wei95, I.4, Theorem 6]) that each division algebra E_i has a unique maximal order $\mathcal{O}_{E_i}$.

Consider first the situation $E \cong M_n(E_0)$; we claim that any order $\mathcal{O}$ in E is conjugate in E to a suborder of $M_n(\mathcal{O}_{E_0})$. Now $E_0^{\oplus n}$ has the structure of simple left E-module, whose ring of E_0-linear endomorphisms coincides with E. It is enough to check that $E_0^{\oplus n}$ has an $\mathcal{O}$-stable lattice; we can easily construct such a lattice by taking the $\mathcal{O}$-span of any basis for $E_0^{\oplus n}$. This proves that every maximal order in $M_n(E_0)$ is conjugate to $M_n(\mathcal{O}_{E_0})$; the claim for general E follows easily.

Finally, the statement about the trace pairing follows from the corresponding statement for division algebras, which is again standard. □

Next let us show how to algorithmically find maximal orders in E.

Lemma 10.4. *Let E be a semisimple algebra over $\mathbb{Q}_\ell$, and let $\mathcal{O} \subsetneq \mathcal{O}'$ be two orders in E. Then there exists an order $\mathcal{O}''$ such that $\mathcal{O} \subsetneq \mathcal{O}'' \subseteq \mathcal{O}'$ and $\mathcal{O}'' \subseteq \frac{1}{\ell}\mathcal{O}$.*

Proof. Let $r \geq 1$ be the smallest integer such that $\ell^r \mathcal{O}' \subseteq \mathcal{O}$, and let $\mathcal{O}'' := \ell^{r-1}\mathcal{O}' + \mathcal{O}$. An order is just a $\mathbb{Z}_\ell$-lattice that is closed under multiplication. We only need to check that $\mathcal{O}''$ is closed under multiplication, and for this it is enough to note that $\ell^{r-1}\mathcal{O}' \cdot \mathcal{O} \subseteq \ell^{r-1}\mathcal{O}' \cdot \mathcal{O}' \subseteq \ell^{r-1}\mathcal{O}'$. □

Lemma 10.5. *There is a finite-time algorithm to find a maximal order in a semisimple $\mathbb{Q}_\ell$-algebra E, presented as $E := E_\mathbb{Q} \otimes_\mathbb{Q} \mathbb{Q}_\ell$ with $E_\mathbb{Q}$ a semisimple $\mathbb{Q}$-algebra.*

The algorithm takes as input a presentation of $E_\mathbb{Q}$ over $\mathbb{Q}$, and outputs an integral basis for an order $\mathcal{O}_0 \subseteq E_\mathbb{Q}$ such that $\mathcal{O}_0 \otimes_\mathbb{Z} \mathbb{Z}_\ell \subseteq E$ is maximal.

Proof. We begin by finding some order, and then enlarge it to a maximal order using Lemma 10.4.

First, choose some basis $e_1, \dots, e_n$ for $E_\mathbb{Q}$ over $\mathbb{Q}$. Write the multiplication rule as $e_i e_j =: \sum_k \alpha_{i,j,k} e_k$. If all the α's are ℓ-integral, then $e_1, \dots, e_n$ span an order in E. If not, we can find some r such that $\ell^r \alpha_{i,j,k}$ is ℓ-integral for all i, j, k. Then the span of $\ell^r e_1, \dots, \ell^r e_n$ is an order in E.

Once we have found one order $\mathcal{O}$, we iteratively enlarge it. Specifically, there are finitely many $\mathbb{Z}_\ell$-lattices $\mathcal{O}'$ with $\mathcal{O} \subsetneq \mathcal{O}' \subseteq \frac{1}{\ell}\mathcal{O}$. Indeed, these lattices are in bijection with the finitely many $\mathbb{F}_\ell$-vector subspaces of $\frac{1}{\ell}\mathcal{O}/\mathcal{O}$, which can be enumerated algorithmically. For each lattice, it is a finite computation to determine whether it is closed under multiplication: simply choose a basis e_i, and compute the constants $\alpha_{i,j,k}$ as above.

At any time, if a larger order $\mathcal{O}'$ is found, we replace $\mathcal{O}$ with $\mathcal{O}'$ and repeat.

We claim that this process must terminate. If not, there is an infinite ascending chain of orders $\mathcal{O}_1 \subsetneq \mathcal{O}_2 \subsetneq \mathcal{O}_3 \subsetneq \cdots$. But the trace pairing must take integral values on any order, so each $\mathcal{O}_n$ is contained in the dual under the trace pairing of $\mathcal{O}_1$, a contradiction.

Hence, the algorithm terminates, giving some order $\mathcal{O}$ such that no order $\mathcal{O}'$ satisfies $\mathcal{O} \subsetneq \mathcal{O}' \subseteq \frac{1}{\ell}\mathcal{O}$. By Lemma 10.4, $\mathcal{O}$ is maximal. □

Lemma 10.6. *There is a finite-time algorithm that determines the decomposition of a commutative étale $\mathbb{Q}_\ell$-algebra as a direct sum of fields.*

Specifically, the algorithm takes as input a commutative étale $\mathbb{Q}_\ell$-algebra E, presented as $E := E_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ with $E_{\mathbb{Q}}$ a commutative étale $\mathbb{Q}$-algebra. It outputs ℓ-adic approximations to elementary idempotents $e_1, \ldots, e_n$, such that $E = \bigoplus_i e_i E$ is the decomposition of E as a direct sum of fields; these e_i's can be computed to any desired ℓ-adic precision.

Proof. The algorithm is in two steps. First, we determine elements $\widetilde{e}_i \in \mathcal{O}_E$ such that $\widetilde{e}_i$ is a unit in $\mathcal{O}_{E_i}$, but has strictly positive valuation in $\mathcal{O}_{E_j}$ for all $j \neq i$. Then, we show how to produce successively better approximations to the true idempotents e_i.

First, use Lemma 10.5 to compute a maximal order $\mathcal{O}_E$ in E. Since E is commutative, $\mathcal{O}_E$ is unique; it is the direct sum of the maximal orders $\mathcal{O}_{E_j}$ in the number field summands of E.

The quotient $\mathcal{O}_E/\ell\mathcal{O}_E$ is a finite $\mathbb{F}_\ell$-algebra. Let $\mathfrak{N}$ be its nilradical; this can be computed in finite time (for example, by computing characteristic polynomials). The quotient of $\mathcal{O}_E/\ell\mathcal{O}_E$ by $\mathfrak{N}$ is the direct sum of the residue fields of the rings $\mathcal{O}_{E_i}$. By a finite search, we can find all idempotent elements of this quotient ring. There will be 2^n of them, where n is the number of fields in the decomposition of E. They form a lattice in which the join of two elements is given by their product; the elementary idempotents are minimal nonzero elements in this lattice. Clearly, these elementary idempotents can be computed in finite time. Choosing lifts to $\mathcal{O}_E$ gives us elements $\widetilde{e}_1, \ldots, \widetilde{e}_n$, such that each $\widetilde{e}_i$ is a unit in $\mathcal{O}_{E_i}$, congruent to 1 modulo its maximal ideal, and is contained in the maximal ideal of each $\mathcal{O}_{E_j}$ for $j \neq i$.

The absolute ramification degree of each E_i is bounded above by $[E : \mathbb{Q}_\ell]$. It follows (by a calculation in each field E_i) that $\widetilde{e}_i^{\,\ell^{r[E:\mathbb{Q}_\ell]}}$ is congruent to the i-th idempotent e_i modulo ℓ^r. □

Definition 10.7. *Let $E = \bigoplus_i E_i$ be a commutative étale $\mathbb{Q}_\ell$-algebra. An* approximate elementary idempotent *is an element $\widetilde{e}_i \in \mathcal{O}_E$ that is a nonunit in E_j for all $j \neq i$, and that is congruent to 1 modulo the maximal ideal of $\mathcal{O}_{E_i}$.*

The proof of Lemma 10.6 shows that an approximate elementary idempotent determines the field E_i, and given an approximate elementary idempotent $\widetilde{e}_i$, we can compute arbitrarily accurate ℓ-adic approximations to the idempotent that projects onto E_i.

Lemma 10.8. *There is a finite-time algorithm which, on input E a semisimple algebra over $\mathbb{Q}_\ell$, presented as $E := E_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ with $E_{\mathbb{Q}}$ a semisimple algebra over $\mathbb{Q}$, outputs the center $Z(E) = Z(E_{\mathbb{Q}}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, with output a basis for $Z(E_{\mathbb{Q}})$.*

Proof. Let $a_1, \ldots, a_n$ be a basis for $E_{\mathbb{Q}}$ over $\mathbb{Q}$. Then $Z(E_{\mathbb{Q}})$ is the set of solutions z to the system of simultaneous linear equations $za_i = a_i z$; finding a basis for this solution set is a routine problem in linear algebra. □

Lemma 10.9. *Let E be a semisimple algebra over $\mathbb{Q}_\ell$. Let $Z(E)$ be the center of E, and let e_i be an elementary idempotent in $Z(E)$. Then $Z_i = e_i Z(E)$ is a field, and $e_i E$ is a central algebra over Z_i. In particular, we have an isomorphism $e_i E \cong M_{n_i}(D_i)$,* *where D_i is a central simple algebra over Z_i; the integer n_i and the isomorphism class of D_i are uniquely determined.*

Proof. Apply Proposition 10.3. □

Lemma 10.10. *There is a finite-time algorithm which, on input $(E, \widetilde{e})$, with E a semisimple algebra over $\mathbb{Q}_\ell$, presented as $E := E_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ with $E_{\mathbb{Q}}$ a semisimple algebra over $\mathbb{Q}$, and $\widetilde{e} \in E$ an approximate elementary idempotent, outputs the integer n_i such that $e_i E \cong M_{n_i}(D_i)$ for some division algebra D_i, and the invariant of the algebra D_i.*

Proof. Let $\mathcal{O}$ be a maximal order in E, let e_i be the elementary idempotent corresponding to $\widetilde{e}$, and let $\mathcal{O}_i := e_i\mathcal{O}$. We'll show that it is enough to compute the number of elements in the (unique) maximal two-sided ideal of $\mathcal{O}_i/\ell\mathcal{O}_i \simeq (\widetilde{e}\mathcal{O})/\ell(\widetilde{e}\mathcal{O})$.

For D_i, a central simple algebra over a p-adic field, standard structure results imply that there is a valuation v on D_i, unique up to scaling, and all ideals of $\mathcal{O}_{D_i}$ are powers of the maximal ideal $\mathfrak{m}$. It follows by a routine calculation that all two-sided ideals of $M_{n_i}(\mathcal{O}_{D_i})$ are of the form $M_{n_i}(\mathfrak{m}^k)$. In particular, $M_{n_i}(\mathcal{O}_{D_i})$ has a unique maximal ideal $M_{n_i}(\mathfrak{m})$, which contains ℓ.

Suppose D_i has dimension d_i^2 over its center $Z(D_i) = e_i Z(E)$, so $[e_i E : \mathbb{Q}_\ell] = d_i^2 n_i^2 [e_i Z(E) : \mathbb{Q}_\ell]$. The structure theory of central simple algebras over p-adic fields gives that D_i has ramification degree d_i over its center. It follows that $\dim_{\mathbb{F}_\ell} M_{n_i}(\mathcal{O}_{D_i})/M_{n_i}(\mathfrak{m}) = d_i n_i^2 [Z(D_i)^{\text{ur.}} : \mathbb{Q}_\ell]$, where $Z(D_i)^{\text{ur.}}$ is the maximal unramified subfield of $Z(D_i)$.

Similarly, taking $\mathfrak{m}_{Z(D_i)}$ to be the unique maximal ideal in $\mathcal{O}_{Z(D_i)}$, we have

$$\dim_{\mathbb{F}_\ell}(\mathcal{O}_{Z(D_i)}/\mathfrak{m}_{Z(D_i)}) = [Z(D_i)^{\text{ur.}} : \mathbb{Q}_\ell].$$

Finally we turn to the invariant of D_i. Recall the theory of division algebras over a local field: The quotient $k_i = D_i/\mathfrak{m}_{Z(D_i)}$ is a finite field – in fact, the finite field of order p^{d_i}. There exist a uniformizer π (i.e. a generator of $\mathfrak{m}_{Z(D_i)}$) and a unique integer r with $1 \leq r \leq d_i$ such that conjugation by π^r induces the Frobenius endomorphism on k_i – in other words,

$$\pi^r x \equiv x^p \pi^r (\text{mod } \pi^{r+1})$$

for all $x \in \mathcal{O}_{D_i}$. The invariant of D_i is, by definition, r/d_i.

Now the quotient

$$(\mathcal{O}_{D_i})/M_{n_i}(\mathfrak{m})$$

is isomorphic to $M_{n_i}(k_i)$, so its center

$$Z((\mathcal{O}_{D_i})/M_{n_i}(\mathfrak{m}))$$

is isomorphic to k_i (it is the set of diagonal matrices). Choose some $x \in Z((\mathcal{O}_{D_i})/M_{n_i}(\mathfrak{m}))$ that generates the field k_i. Then a calculation shows that, for any $a \in \mathbb{Z}$ and any

$$M \in \mathfrak{m}^a_{Z(D_i)} - \mathfrak{m}^{a+1}_{Z(D_i)}$$

we have

$$Mx \equiv x^{p^b} M (\text{mod } \mathfrak{m}_{Z(D_i)}^{a+1}),$$

where $ra \equiv b$ (mod d_i) and r is the integer defined above (i.e. r/d_i is the invariant of the algebra D_i).

Now we explain the algorithm. Use Lemma 10.5 to find a maximal order $\mathcal{O}$ in E. The quotient ring $\mathcal{O}_i/\ell\mathcal{O}_i$ is finite, so we can compute a presentation for it. It is a finite calculation to determine a maximal ideal $\mathfrak{m}$ in $\mathcal{O}_i/\ell\mathcal{O}_i$, and hence compute $\dim_{\mathbb{F}_\ell} M_{n_i}(\mathcal{O}_{D_i})/M_{n_i}(\mathfrak{m})$.

Similarly, let Z be the center of $\mathcal{O}$; by Lemmas 10.8 and 10.5, we can compute the maximal order $\mathcal{O}_Z$ in Z. Again by a finite computation, we can compute the maximal ideal in $\widetilde{e}(\mathcal{O}_Z/\ell\mathcal{O}_Z)$; call it $\mathfrak{m}_{Z_i}$. From this we determine $\dim_{\mathbb{F}_\ell}(\mathcal{O}_{Z(D_i)}/\mathfrak{m}_{Z(D_i)})[Z(D_i)^{\text{ur.}} : \mathbb{Q}_\ell]$.

Having determined $[Z(D_i)^{\text{ur.}} : \mathbb{Q}_\ell]$, $d_i n_i^2[Z(D_i)^{\text{ur.}} : \mathbb{Q}_\ell]$, and $d_i^2 n_i^2[e_i Z(E) : \mathbb{Q}_\ell]$, it is straightforward to determine n_i.

Finally, to determine the invariant r/d_i of D_i, we simply choose

$$M \in \mathfrak{m}_{Z(D_i)} - \mathfrak{m}_{Z(D_i)}^2,$$

take x to generate the field $Z((\mathcal{O}_{D_i})/M_{n_i}(\mathfrak{m}))$, find the unique $b \in \mathbb{Z}/d_i\mathbb{Z}$ such that

$$Mx \equiv xM^b (\text{mod } \mathfrak{m}_{Z(D_i)}^2),$$

and take r the multiplicative inverse of b modulo d_i. □

We may now prove Propositions 10.1 and 10.2.

Proof of Proposition 10.1. We are given the semisimple algebra E and its action on the vector space V. By Lemmas 10.8 and 10.6, we can find a system of approximate elementary idempotents for the center $Z(E)$; by Lemma 10.10 we can find the integers n_i in the decomposition $E \cong \bigoplus M_{n_i}(E_i)$.

Next let us show how to approximate the trace of any element $\alpha \in E$ on any simple E-module $E_i^{\oplus n_i}$. This trace is simply $\text{Tr}(e_i\alpha)$, where e_i is the elementary idempotent of E projecting onto $M_{n_i}(E_i)$. By the remark following Lemma 10.6, we can approximate e_i to any desired ℓ-adic precision. We need to control the precision on $\text{Tr}(e_i\alpha)$; scaling α by a power of ℓ, we may assume that α has all eigenvalues integral. In this setting, if $\widetilde{e}_i \equiv e_i \ (\text{mod } \ell^n Z(E))$, then $\text{Tr}(\widetilde{e}_i\alpha) \equiv \text{Tr}(e_i\alpha) \ (\text{mod } \ell^n)$.

All that remains is to determine the decomposition of a given E-module V in terms of the simple E-modules; for this it is enough to determine the multiplicity of a single $E_i^{\oplus n_i}$ as a factor of V. For this, we consider the action of an approximate elementary idempotent $\widetilde{e}_i$ on V. We know that $\widetilde{e}_i$ acts on $E_i^{\oplus n_i}$ with eigenvalues that are ℓ-adic units, while the eigenvalues of its actions on any other simple E-module are zero modulo ℓ. We can compute the number of nonzero eigenvalues of $\widetilde{e}_i$ on V; this number will be exactly $m_i \dim_{\mathbb{Q}_\ell} E_i^{\oplus n_i}$, where m_i is the multiplicity we want to find. □

Proof of Proposition 10.2. Apply Lemmas 10.8, 10.6, and 10.10. □

11 Algorithmic decomposition of semisimple algebras over number fields.

Proposition 11.1. *There is a finite-time algorithm which, on input (K, E) with E a semisimple algebra over a number field $K/\mathbb{Q}$, outputs $(s, (e_i)_{i=1}^s, (n_i)_{i=1}^s, (E_i)_{i=1}^s)$, where*

$$E \cong \bigoplus_{i=1}^{s} M_{n_i}(E_i), \tag{3}$$

with each E_i a division algebra, and each $e_i \in E$ the elementary idempotent projecting onto the i-th summand.

Lemma 11.2. *There is a finite-time algorithm which, on input (K, E) with E a semisimple central algebra over a number field $K/\mathbb{Q}$, outputs the elementary idempotents e_i projecting onto each summand in the decomposition* (3)*.*

Proof. By linear algebra we can compute a presentation for the center $Z(E)$. This center decomposes as a sum of fields $Z(E) = \bigoplus_i Z(E_i)$; the idempotents we are looking for are exactly the projectors onto the summands. Hence we are reduced to the problem of decomposing a commutative étale K-algebra as a sum of fields, which is standard. □

Lemma 11.3. *There is a finite-time algorithm which, on input E a semisimple central algebra over $\mathbb{R}$ (thus E is either a matrix algebra over $\mathbb{R}$ or over the Hamilton quaternions $\mathbb{H}$), presented as $E := E_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R}$ with $E_{\mathbb{Q}}$ a semisimple central algebra over $\mathbb{Q}$, outputs true if and only if E is a matrix algebra over $\mathbb{R}$.*

Proof. We may assume $\dim_{\mathbb{R}} E = (2n)^2$. The trace pairing defines a quadratic form on E, whose signature is $(2n^2 + n, 2n^2 - n)$ if $E \cong M_{2n}(\mathbb{R})$, and $(2n^2 - n, 2n^2 + n)$ if $E \cong M_n(\mathbb{H})$. Given E, one can determine the signature of the trace pairing by the Gram-Schmidt process. □

Lemma 11.4. *There is a finite-time algorithm which, on input (K, E) with E a semisimple central algebra over a number field $K/\mathbb{Q}$, outputs a finite list of places of K such that the local invariant of E at any place not on the list is* 0*.*

Proof. Choose any order $\mathcal{O}$ in E (not necessarily maximal), and compute its discriminant N with respect to the trace pairing. Return the set of finite places dividing N, plus all the archimedean places. □

Lemma 11.5. *There is a finite-time algorithm which, on input (K, E) with E a semisimple central algebra over a number field $K/\mathbb{Q}$, outputs all the nonzero local invariants of E.*

Proof. The invariant of E at any complex place is zero; at a real place it is 0 or $1/2$, depending whether the associated division algebra is $\mathbb{R}$ or $\mathbb{Q}$. By Lemma 11.3 we can determine which case holds at each real place. This settles the archimedean places.

By Lemma 11.4, we only need to find the invariants of E at finitely many nonarchimedean places; to find the invariant of a nonarchimedean localization of E, we apply Proposition 10.2. □

Now we may prove Proposition 11.1.

Proof of Proposition 11.1. The algorithm works as follows. First we decompose $Z(E)$ into fields (Lemma 11.2); this determine the decomposition of E into simple algebras. Passing to one simple factor, we may assume that E is simple, with center K'. Then $E \cong M_{n_1}(E_1)$ is a matrix algebra over a division ring E_1. If $\dim_{K'} E_1 = d_1^2$, then $\dim_K E = d_1^2 n_1^2$; since the latter dimension can be read off from our presentation, we just need to compute the number d_1.

Global class field theory describes the structure of the central simple algebra E_1. Its localization at each place (finite or infinite) of K' is determined by an invariant in $\mathbb{Q}/\mathbb{Z}$. All but finitely many of these invariants vanish, and their least common denominator is d_1. We can compute the nonzero invariants by Lemma 11.5, and we are done. □

12 Mumford coordinates.

Here we collect some results that enable us to work algorithmically with the moduli space of abelian varieties. We use Mumford's explicit description of the moduli of abelian varieties with δ-markings [Mum66].

A δ-marking is a certain type of level structure, introduced by Mumford. Any abelian variety with δ-marking can be canonically embedded in projective space; we say that the resulting projectively embedded abelian variety is in *Mumford form* (Definition 12.7). For fixed level δ, any abelian variety admits only finitely many embeddings in Mumford form. We will make algorithmic several basic tasks involving moduli spaces:

Lemma 12.8 allows us to test whether an abelian scheme is in Mumford form (which enables us to find Mumford forms for arbitrary abelian schemes, by brute-force search).

Lemma 12.14 Given an abelian variety A over a characteristic-zero field K, can compute (for given δ) all Mumford embeddings of A.

Lemma 12.15 Given a family of abelian varieties and a fixed abelian variety A, one can compute all fibers of the family that are isomorphic to A.

12.1 Introduction.

We will start with Mumford's explicit description of abelian varieties, and their moduli, in terms of (algebraic) theta functions and theta-zero values. The material is classical – it was known, in some form, to Riemann – but we will use Mumford's presentation. The material we need is in [Mum66, §§1-3] and [Mum67, §6].

Given a choice of "level" δ, a polarization on A, and some additional discrete data (a "δ-marking"), Mumford defines a *canonical* embedding of A into a certain projective space depending only on δ. This embedding has the pleasant property that the line bundle $\mathcal{L} = \mathcal{O}(1)$ on A is invariant under pullback both by the inversion $x \mapsto -x$ on A and by a certain torsion subgroup (the "δ-torsion") of A. Inversion and these torsion translations on A extend to linear maps of the ambient projective space, and in fact these linear maps can be described by universal equations independent of the abelian variety A.

Since the projective embedding is canonical, the coordinates Q_x of the origin of A define invariants of A (with its δ-marking). One can write down equations for A as a subscheme of projective space, whose coefficients depend only on the Q_x. In other words, the coordinates Q_x can be used as coordinates on the moduli space of abelian varieties (with suitable polarization and δ-marking).

However, the addition law on A does not have a simple form in Mumford's coordinates.

12.2 δ-markings.

(In [Mum67] the constructions are carried out over $\mathbb{Z}[1/\prod d_i]$, but we will only need the results in characteristic 0.)

We begin by recalling some notation from [Mum66, §§1-3] and [Mum67, §6]. Let $\delta = (d_1, \ldots, d_g)$ be a collection of elementary divisors; that is, they are positive integers such that $d_{i+1}|d_i$. We also assume that all the d_i are divisible by 8. (For the purposes of this paper, it is fine to assume $\delta = (8, 8, \ldots, 8)$.) We will write $2\delta = (2d_1, \ldots, 2d_g)$ and

$$|\delta| := \prod_{i=1}^{g} d_i.$$

Let

$$K(\delta) := \bigoplus_{i=1}^{k} \mathbb{Z}/(d_i\mathbb{Z}).$$

Note that there is a natural inclusion $K(\delta) \subseteq K(2\delta)$, given by multiplication by two on the individual factors

$$\mathbb{Z}/(d_i\mathbb{Z}) \to \mathbb{Z}/(2d_i\mathbb{Z}).$$

Also, let $Z_2 \subseteq K(\delta)$ be the subgroup of points that are divisible by 2.

Next we define the group scheme $\mathcal{G}(\delta)$. As a set, the S-points of $\mathcal{G}(\delta)$ (for connected schemes S) are tuples (t, a, ℓ) such that:

1. t is a section of $\mathbb{G}_{m,S}$,
2. $a \in K(\delta)$,
3. $\ell \in K(\delta)^\vee = \operatorname{Hom}(K(\delta), \mathbb{G}_m)$ – or more concretely, $\ell = (\ell_1, \ldots, \ell_g)$, where each ℓ_i is a d_i-th root of unity in $\mathbb{G}_{m,S}$. (We will write the group law in $K(\delta)^\vee$ additively.)

Remark 12.1. *There is a natural pairing*

$$K(\delta) \times K(\delta)^\vee \to \mathbb{G}_m,$$

which we will write as

$$(a, \ell) \mapsto \langle a, \ell \rangle$$

We will write the group law on $K(\delta)^\vee$ additively.

The group structure on $\mathcal{G}(\delta)$ is given by

$$(t_1, a_1, \ell_1) \cdot (t_2, a_2, \ell_2) = (t_1 t_2 \langle a_2, \ell_1 \rangle, a_1 + a_2, \ell_1 + \ell_2).$$

We note that the injection $\mathbb{G}_m \mapsto \mathcal{G}(\delta)$ given by $t \mapsto (t, 0, 0)$ gives rise to an exact sequence

$$0 \to \mathbb{G}_m \to \mathcal{G}(\delta) \to K(\delta) \oplus K(\delta)^\vee \to 0.$$

Furthermore, the commutator on G descends to the pairing $e(-,-)$ on $K(\delta) \oplus K(\delta)^\vee$ given by

$$e((a_1,\ell_1),(a_2,\ell_2)) = \frac{\langle a_1,\ell_2\rangle}{\langle a_2,\ell_1\rangle}. \tag{4}$$

Given an abelian scheme A over a base S of characteristic zero and a line bundle $\mathcal{L}$ on A, we define a group scheme $\mathcal{G}(\mathcal{L})$ over S as follows. For any S-scheme T, $\mathcal{G}(\mathcal{L})(T)$ is the group of pairs (s,α), where s is a section of $A \times_S T \to T$, and

$$\alpha \colon T_s^* L \to L$$

is an isomorphism. (Here $T_s \colon A \to A$ is translation by s.)

We note again that there is an injection $\mathbb{G}_m \mapsto \mathcal{G}(\mathcal{L})$, given by $\alpha \mapsto (0,\alpha)$; that is, by the usual action of $\mathbb{G}_m$ by multiplication on the line bundle $\mathcal{L}$; this injection gives rise to an exact sequence

$$0 \to \mathbb{G}_m \to \mathcal{G}(\mathcal{L}) \to A[\mathcal{L}] \to 0,$$

where $A[\mathcal{L}]$ is the image of the map $\mathcal{G}(\mathcal{L}) \to A$ given by $(s,\alpha) \mapsto s$.

Definition 12.2. *Let A be an abelian scheme of dimension g over a $\mathbb{Q}$-scheme S. A δ-*marking *on A is the following data:*

1. *A symmetric, very ample line bundle $\mathcal{L}$ on A. ("Symmetric" means that there is an isomorphism $\mathcal{L} \cong \mathcal{L}^{-1}$.)*
2. *An isomorphism $\beta \colon \mathcal{G}(\mathcal{L}) \to \mathcal{G}(\delta)$ which is the identity on the subgroup $\mathbb{G}_{m,S}$.*

The Néron–Severi class *(or* polarization*) of δ is simply the Néron–Severi class of $\mathcal{L}$ in $H^2(A)$.*

Given A and δ, there are finitely many δ-markings on A of given Néron–Severi class; see Lemmas 12.4 and 12.5.

We note that any δ-marking gives rise to an identification of the torsion subgroup $A[\delta]$ with $K(\delta) \oplus K(\delta)^\vee$.

12.3 Let us count the ways (to put Mumford coordinates on an abelian variety).

We begin with a short discussion of the structure of the group $\mathcal{G}(\delta)$.

Definition 12.3. *Let*

$$\operatorname{Aut}_{\mathbb{G}_m} \mathcal{G}(\delta) = \{f \in \operatorname{Aut} \mathcal{G}(\delta) \mid f(x) = x \textit{ for all } x \in \mathbb{G}_m\}$$

be the group of automorphisms of $\mathcal{G}(\delta)$ acting trivially on $\mathbb{G}_m$.

Our goal is to compute all automorphisms in $\operatorname{Aut}_{\mathbb{G}_m} \mathcal{G}(\delta)$.

To start with, let $a_{(i)}$ be the standard generator of $\mathbb{Z}/(d_i\mathbb{Z}) \subseteq K(\delta)$ (that is, the image of 1 under the inclusion of the i-th summand

$$\mathbb{Z}/(d_i\mathbb{Z}) \hookrightarrow \bigoplus_{j=1}^{k} \mathbb{Z}/(d_j\mathbb{Z}) = K(\delta)).$$

Choose, for each i, a primitive d_i-th root of unity ζ_i, and let $\ell_{(i)} \in (\mathbb{Z}/(d_i\mathbb{Z}))^\vee \subseteq K(\delta)^\vee$ be such that

$$\langle a_{(i)}, \ell_{(i)} \rangle = \zeta_i.$$

Note that $\mathcal{G}(\delta)$ is generated by $\mathbb{G}_m$ and the elements $(1, a_{(i)}, 0)$ and $(1, 0, \ell_{(i)})$, subject to the relations that

$$(1, a_{(i)}, 0)^{d_i} = (1, 0, \ell_{(i)})^{d_i} = (1, 0, 0),$$

$$(1, 0, \ell_{(i)})(1, a_{(i)}, 0) = \zeta_i (1, a_{(i)}, 0)(1, 0, \ell_{(i)}),$$

and all other pairs of generators commute.

It follows that we can specify an automorphism in $\mathrm{Aut}_{\mathbb{G}_m} \mathcal{G}(\delta)$ by giving the image of $(1, a_{(i)}, 0)$ and $(1, 0, \ell_{(i)})$.

Let $\mathrm{Sp}(K(\delta) \oplus K(\delta)^\vee)$ denote the set of automorphisms σ of $K(\delta) \oplus K(\delta)^\vee$ that respect the pairing e, that is, that satisfy

$$e(\sigma(x), \sigma(x')) = e(x, x')$$

for all $x, x' \in K(\delta) \oplus K(\delta)^\vee$.

Lemma 12.4. *There are finitely many automorphisms f of $\mathcal{G}(\delta)$ that act as the identity on $\mathbb{G}_m$; each such f can be written explicitly as follows.*

Suppose given any

$$\sigma \in \mathrm{Sp}(K(\delta) \oplus K(\delta)^\vee).$$

Let

$$\sigma(a_{(i)}) = (b_i, m_i),$$

and let ψ_i be such that

$$\psi_i^{d_i} = \langle b_i, m_i \rangle^{\frac{d_i(d_i-1)}{2}}.$$

Similarly, let

$$\sigma(\ell_{(i)}) = (b'_i, m'_i),$$

and let ω_i be such that

$$\omega_i^{d_i} = \langle b'_i, m'_i \rangle^{\frac{d_i(d_i-1)}{2}}.$$

Note that there are d_i choices for each of ψ_i and ω_i, and that all choices can be computed explicitly in terms of roots of unity.

Then there is a unique automorphism f of $\mathcal{G}(\delta)$, acting as the identity on $\mathbb{G}_m$ and as σ on $\mathrm{Sp}(K(\delta) \oplus K(\delta)^\vee)$, such that

$$f((1, a_{(i)}, 0)) = (\psi_i, b_i, m_i)$$

and

$$f((1, 0, \ell_{(i)})) = (\omega_i, b'_i, m'_i).$$

Proof. A calculation shows that $f((1, a_{(i)}, 0))$ and $f((1, 0, \ell_{(i)}))$ satisfy the requisite relations, and hence that f extends to an automorphism of $\mathcal{G}(\delta)$.

To see that all f arise in this way, note that any $f \in \mathrm{Aut}_{\mathbb{G}_m} \mathcal{G}(\delta)$ descends to an automorphism σ of the quotient $\mathcal{G}(\delta)/\mathbb{G}_m = K(\delta) \oplus K(\delta)^\vee$. The commutator of any two elements $(t, a, \ell), (t', a', \ell') \in \mathcal{G}(\delta)$ is given by

$$e((a, \ell), (a', \ell')) \in \mathbb{G}_m \subseteq \mathcal{G}(\delta),$$

so σ must preserve the pairing e.

Finally, if we write

$$f((1, a_{(i)}, 0)) = (\psi_i, b_i, m_i)$$

and

$$f((1, 0, \ell_{(i)})) = (\omega_i, b'_i, m'_i),$$

the relations

$$(1, a_{(i)}, 0)^{d_i} = (1, 0, \ell_{(i)})^{d_i} = (1, 0, 0)$$

imply that

$$\psi_i^{d_i} = \langle b_i, m_i \rangle^{\frac{d_i(d_i-1)}{2}}$$

and

$$\omega_i^{d_i} = \langle b'_i, m'_i \rangle^{\frac{d_i(d_i-1)}{2}}.$$

□

For the reader's convenience, we give a more abstract reformulation of Lemma 12.4 below, though it is not used in the sequel.

Lemma 12.5. *Consider the group*

$$\mathrm{Aut}_{\mathbb{G}_m} \mathcal{G}(\delta) = \{f \in \mathrm{Aut}\, \mathcal{G}(\delta) \mid f(x) = x \textit{ for all } x \in \mathbb{G}_m\}$$

of automorphisms of $\mathcal{G}(\delta)$ acting trivially on $\mathbb{G}_m$.

This group sits in an exact sequence

$$0 \to (K(\delta) \oplus K(\delta)^\vee)^\vee \to \mathrm{Aut}\, \mathcal{G}(\delta) \to \mathrm{Sp}(K(\delta) \oplus K(\delta)^\vee) \to 0.$$

12.4 Representation theory of the group $\mathcal{G}(\delta)$.

Mumford's projective embeddings of abelian varieties and their moduli are based on the following result, which describes the action of $\mathcal{G}(\mathcal{L})$ on the global sections $\Gamma(\mathcal{L})$.

Lemma 12.6. *[Mum66, §1, Prop. 3 and Thm. 2] The group $\mathcal{G}(\delta)$ has (up to isomorphism) a unique irreducible representation $V(\delta)$ on which $\mathbb{G}_m \subseteq \mathcal{G}(\delta)$ acts via the identity (i.e. on which any $\lambda \in \mathbb{G}_m$ acts by multiplication by λ).*

The representation $V(\delta)$ can be described (over any field k of characteristic zero) as follows: As a vector space, $V(\delta)$ is the space of k-valued functions on $K(\delta)$; the action of $\mathcal{G}(\delta)$ is given by

$$((t, a, \ell) \cdot f)(x) = t\langle x, \ell\rangle f(x + a).$$

The group $\mathcal{G}(\mathcal{L})$ acts on the space of global sections $\Gamma(\mathcal{L})$; if there is an isomorphism $\mathcal{G}(\mathcal{L}) \cong \mathcal{G}(\delta)$, then $\Gamma(\mathcal{L})$ and $V(\delta)$ are isomorphic as representations of $\mathcal{G}(\delta)$.

As in Lemma 12.6, let $V(\delta)$ be the vector space of $\mathbb{Q}$-valued functions on $K(\delta)$. Let

$$\mathbb{P}(V(\delta)) = \operatorname{Proj}\operatorname{Sym} V(\delta);$$

this is a projective $\mathbb{Q}$-scheme whose points are in bijection with linear functionals on $V(\delta)$.

For all $a \in K(\delta)$, let $X_a \in V(\delta)$ be the function that is 1 at a and 0 elsewhere; this is naturally a section of $\mathcal{O}(1)$ on $\mathbb{P}(V(\delta))$, and the sections X_a (for $a \in K(\delta)$) give a set of projective coordinates on $\mathbb{P}(V(\delta))$.

Suppose $(\mathcal{L}, \beta)$ is a δ-marking on an abelian scheme A over some base $\mathbb{Q}$-scheme S. By Lemma 12.6, we can identify $\Gamma(\mathcal{L})$ with $V(\delta)$ in a $\mathcal{G}(\delta)$-equivariant way. This identification is unique up to scaling (by Schur's lemma), so it gives rise to an embedding

$$A \hookrightarrow \mathbb{P}(V(\delta)).$$

This is quite a strong statement! The embedding of A is defined, not (as might be imagined) up to automorphisms of projective space, but as a specific map into the space $\mathbb{P}(V(\delta))$. The projective coordinates $X_a(e)$ of the identity point of A are an invariant of the abelian variety A, depending only on the discrete choices of the line bundle $\mathcal{L}$ and the δ-marking β.

Definition 12.7. *An* abelian scheme in Mumford form *is an abelian subscheme A of $\mathbb{P}(V(\delta))_S$ arising from the construction above.*

Its Mumford coordinates *$Q_a = Q_a(A) = Q_a(A, \mathcal{L}, \beta)$ are the projective coordinates $X_a(e)$ of the origin $e \in A$ in $\mathbb{P}(V(\delta))$, given as functions on S.*

12.5 Characterizing δ-markings.

Suppose A is an abelian variety in Mumford form, coming from a δ-marking $(A, \mathcal{L}, \beta)$. Let $(a, \ell) \in K(\delta) \oplus K(\delta)^\vee$. The δ-marking gives an isomorphism

$$K(\delta) \oplus K(\delta)^\vee \cong A[\mathcal{L}];$$

let s be the image of (a, ℓ) under this isomorphism.

Translation by s is an automorphism T_s of the scheme A (though not an automorphism of the abelian variety: T_s does not fix the identity or respect the addition law). Since $T_s^*(\mathcal{O}(1)) \cong \mathcal{O}(1)$, the automorphism T_s of A extends to a linear automorphism f_s of the ambient projective space $\mathbb{P}(V(\delta))$. This linear automorphism is determined by the action of $\mathcal{G}(\delta)$ on $\Gamma(\mathcal{L})$; its action on projective coordinates is given (up to scaling) by

$$f_s^*(X_b) = \langle b, \ell\rangle X_{a+b}. \tag{5}$$

Lemma 12.8. *Let A be an abelian scheme of dimension g over a $\mathbb{Q}$-scheme S, presented as a subscheme $A \subseteq \mathbb{P}(V(\delta)) \times S$ of the projective space on $V(\delta)$.*

This $A \subseteq \mathbb{P}(V(\delta)) \times S$ is an abelian scheme in Mumford form if and only if A satisfies the following conditions.

1. *A is not contained in any hyperplane in $\mathbb{P}(V(\delta))$.*

2. *The degree of the line bundle $\mathcal{L} = \mathcal{O}(1)|_A$ is $|\delta|$.*

3. *The automorphisms f_s of $\mathbb{P}(V(\delta))$ defined above (Equation (5)), for $s \in K(\delta) \oplus K(\delta)^\vee$, map A into itself.*

4. *If e is the identity section of A, then the map $f_s \colon A \to A$ coincides with translation by the section $f_s(e)$.*

5. *The inverse map $A \to A$ extends to a linear automorphism of $\mathbb{P}(V(\delta))$.*

Proof. For any line bundle $\mathcal{L}$ on A, the cokernel $H_\mathcal{L}$ of $\mathbb{G}_m \to \mathcal{G}(\mathcal{L})$ coincides with the kernel of the map $\varphi_\mathcal{L} \colon A \to A^\vee$ defined by

$$\varphi_\mathcal{L} = T_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \in \operatorname{Pic}^0(A) = A^\vee.$$

This group $H_\mathcal{L}$ has order

$$|H_\mathcal{L}| = d(\mathcal{L})^2,$$

where $d(\mathcal{L})$ is the degree of $\mathcal{L}$. Furthermore, we have the equality

$$\dim \Gamma(\mathcal{L}) = d(\mathcal{L}).$$

Returning our setting, suppose A satisfies the list of conditions. since the embedding of A in $\mathbb{P}(V(\delta))$ has degree $|\delta|$, the line bundle $\mathcal{L}$ on A has

$$\dim \Gamma(\mathcal{L}) = |\delta|.$$

Since A is embedded in a $(|\delta| - 1)$-dimensional projective space and does not lie in any hyperplane, the pullback map

$$\Gamma(\mathbb{P}(V(\delta)), \mathcal{O}(1)) \to \Gamma(A, \mathcal{L})$$

is an isomorphism. In other words, the embedding of A in $\mathbb{P}(V(\delta))$ is precisely the embedding given by the very ample line bundle $\mathcal{L}$.

The hypothesis on the inverse map implies that $\mathcal{L}$ is symmetric.

To finish, we just have to check that there is an isomorphism

$$\mathcal{G}(\delta) \cong \mathcal{G}(\mathcal{L})$$

with respect to which

$$\Gamma(\mathbb{P}(V(\delta)), \mathcal{O}(1)) \to \Gamma(A, \mathcal{L})$$

is equivariant. But this is clear: The action of $\mathcal{G}(\delta)$ on $\mathbb{P}(V(\delta))$ descends to A by assumption. Moreover, the action of $\mathcal{G}(\delta)$ on $\mathcal{O}(1)$ by linear automorphisms descends to an action on $\mathcal{L}$, equivariant over the action on A. That is, our setup naturally gives rise to a homomorphism $\mathcal{G}(\delta) \cong \mathcal{G}(\mathcal{L})$. This homomorphism is clearly injective and acts as the identity on the common subgroup $\mathbb{G}_m$; since $\mathbb{G}_m$ has the same index $|\delta|^2$ in both $\mathcal{G}(\delta)$ and $\mathcal{G}(\mathcal{L})$, the homomorphism $\mathcal{G}(\delta) \cong \mathcal{G}(\mathcal{L})$ is an isomorphism, so A is indeed embedded in Mumford form.

The converse is easy: Suppose A is in Mumford form. Then (1) follows because the projective embedding of A is given by sections of a line bundle; (2) from the degree calculation above; (3) and (4) from the discussion preceding Equation (5), and (5) from the symmetry of the line bundle $\mathcal{L}$. □

Next we recall a useful lemma from [Mum66]: the Mumford coordinates of the origin determine the abelian variety.

Lemma 12.9. *Let $Z_2 \subseteq K(\delta)$ be the subgroup of points that are divisible by 2.*

Suppose A is an abelian variety in its Mumford embedding, and let Q_a be the coordinates of the origin on A (as a ranges over $K(\delta)$). Then the variety A in the projective space $\mathbb{P}(V(\delta))$ is cut out by the following quadratic equations (in variables X_a):

$$\begin{aligned}&\left(\sum_{\eta\in Z_2} l(\eta)Q_{c+d+\eta}Q_{c-d+\eta}\right)\left(\sum_{\eta\in Z_2} l(\eta)X_{a+b+\eta}X_{a-b+\eta}\right)\\ -&\left(\sum_{\eta\in Z_2} l(\eta)Q_{c+b+\eta}Q_{c-b+\eta}\right)\left(\sum_{\eta\in Z_2} l(\eta)X_{a+d+\eta}X_{a-d+\eta}\right) \quad \in \Gamma(\mathcal{O}(2)_{\mathbb{P}(V(\delta))}\otimes\mathcal{M}^2),\end{aligned}$$

for each tuple (a,b,c,d,l), where $a,b,c,d \in K(2\delta)$ are all congruent modulo $K(\delta)$, and $l\colon Z_2 \to \{\pm 1\}$ is a group homomorphism.

In particular, knowledge of the projective coordinates Q_a alone determines the abelian variety A.

12.6 Different Mumford coordinates on the same abelian variety.

We want to use Mumford embeddings to detect whether two polarized abelian varieties are isomorphic. To this end, we want to be able to find all Mumford embeddings of a given A with given polarization.

Lemma 12.10. *Let*

$$\rho\colon \mathcal{G}(\delta) \to \mathrm{GL}(V(\delta))$$

be the standard representation of $\mathcal{G}(\delta)$ on $V(\delta)$ (Lemma 12.6).

For any automorphism φ of $\mathcal{G}(\delta)$, the two representations ρ and $\varphi\circ\rho$ of $\mathcal{G}(\delta)$ are isomorphic. Furthermore, the isomorphism can be computed explicitly: one can compute (working with exact arithmetic over a cyclotomic field) a $\mathcal{G}(\delta)$-equivariant map

$$f\colon (V(\delta),\rho) \to (V(\delta),\varphi\circ\rho)$$

from the representation ρ to the representation $\varphi\circ\rho$.

Proof. The group $\mathcal{G}(\delta)$ has only the one irreducible representation (up to isomorphism) on which $\mathbb{G}_m$ acts as the identity (Lemma 12.6), so $\varphi \circ \rho$ must be isomorphic to this representation ρ. This gives existence of f.

Once f is known to exist, it can be computed by linear algebra. □

Lemma 12.11. *Given $(A, \mathcal{L}, \beta)$ an abelian variety in Mumford embedding over a number field $K/\mathbb{Q}$, one can compute all Mumford embeddings $(A, \mathcal{L}', \beta')$ over K of the same abelian variety A/K such that $\mathcal{L}'$ belongs to the same Neron–Severi class as $\mathcal{L}$.*

Proof. Given $(A, \mathcal{L}, \beta)$, the choice of another Mumford embedding belonging to the same Neron–Severi class amounts to the choice of:

- a symmetric line bundle $\mathcal{L}'$ belonging to the same Neron–Severi class as $\mathcal{L}$, and
- an isomorphism $\mathcal{G}(\delta) \cong \mathcal{G}(\mathcal{L})'$.

We will proceed in two steps: first we will describe how to fine one Mumford embedding for each line bundle $\mathcal{L}'$; then we will describe how, given a single Mumford embedding for $\mathcal{L}'$, to find all of them.

To say that $\mathcal{L}'$ is a symmetric line bundle in the Neron–Severi class of $\mathcal{L}$ means that $\mathcal{L}' \otimes \mathcal{L}^{-1}$ is a two-torsion point on the dual abelian variety $A^\vee = \mathrm{Pic}^0(A)$. There are 2^{2g} such $\mathcal{L}'$; they are all given as

$$T_x^* \mathcal{L}$$

for $x \in A(\overline{\mathbb{Q}})$ such that $2x \in H_{\mathcal{L}}$, and we can compute them by Lemma 7.1.

Given any such x, the tuple $(A, \mathcal{L}', \beta \circ T_x)$ is a Mumford embedding of A.

Now given $(A, \mathcal{L}', \beta_0)$, all other Mumford embeddings for this fixed $\mathcal{L}'$ are given by

$$\beta' = \varphi \circ \beta_0$$

for some automorphism φ of $\mathcal{G}(\delta)$ acting as the identity on $\mathbb{G}_m$. All such automorphisms φ are described explicitly in Lemmas 12.4 and 12.5. For each such φ, let $f_\varphi \colon V(\delta) \to V(\delta)$ be an equivariant morphism from $V(\delta)$ (with $\mathcal{G}(\delta)$-action given by ρ) to itself (with $\mathcal{G}(\delta)$-action given by $\rho \circ \varphi$). (Note that f_φ can be computed exactly by Lemma 12.10.)

Since f_φ is a linear transformation of $V(\delta)$, it acts on the projective space $\mathbb{P}(V(\delta))$, the Mumford embedding

$$(A, \mathcal{L}', \beta')$$

is given by postcomposing $A \to \mathbb{P}(V(\delta))$ with f_φ. □

Remark 12.12. *The choice of x such that $T_x^* \mathcal{L} \cong \mathcal{L}'$ is not unique: it is only unique up to $H_{\mathcal{L}}$. Translation by $H_{\mathcal{L}}$ on the Mumford-embedded A is given by linear transformations f_s of the ambient projective space (see Equation* (5) *in Section 12.5). These are precisely the f_φ arising from φ an inner automorphism of $\mathcal{G}(\delta)$.*

12.7 Detecting an abelian variety in a family.

Lemma 12.13. *Let $\mathcal{A} \to S$ be an abelian scheme, where S is quasiprojective over a number field K, and the map $\mathcal{A} \to S$ and the structure maps of $\mathcal{A}$ are defined over K.*

There is an algorithm that produces an étale cover S' of S, an abelian scheme $\mathcal{A}'/S'$ in Mumford embedding, and an isomorphism $\mathcal{A}' \cong \mathcal{A} \times_S S'$ of S'-schemes.

Proof. Brute-force search (see Section 5.3). By Lemma 12.8, we can detect whether a given $A \subseteq \mathbb{P}(V(\delta)) \times S$ is an abelian variety in Mumford form. □

Lemma 12.14. *Let (A, ν) be an abelian variety with given polarization over a number field K, and fix a δ as in §12.2. (Assume δ is the invariants of the polarization.)*

There is an algorithm that takes A and δ as input, and returns the Mumford coordinates of all δ-markings on A of polarization ν.

Proof. Find a single Mumford form by Lemma 12.13, and then find all the others by Lemma 12.11. □

Lemma 12.15. *There is an algorithm that takes as input a polarized abelian scheme $\mathcal{A} \to S$, where S is quasiprojective over a number field K, and a polarized abelian variety A over K, and determines all $s \in S(\overline{\mathbb{Q}})$ such that $\mathcal{A}_s$ and A are geometrically isomorphic (by an isomorphism that respects the polarization).*

Proof. By multiplying the polarization on $\mathcal{A}$ by 8, we may assume that its invariant $\delta = (d_1, \ldots, d_g)$ is such that $8 \mid d_i$ for each i; similarly for the polarization on A. We may assume that both polarizations have the same invariant; otherwise $\mathcal{A}_s$ and A cannot ever be isomorphic as polarized abelian varieties.

Apply Lemma 12.13 to $\mathcal{A} \to S$ to get a family $\mathcal{A}' \to S'$ in Mumford embedding, and let

$$Q_{\mathcal{A}'} \colon S' \to \mathbb{P}(V(\delta))$$

be the corresponding Mumford coordinates.

Note that $\mathcal{A}_s$ and A are geometrically isomorphic if and only if there is some choice of δ-marking on A for which its Mumford coordinates agree with $Q_{\mathcal{A}'}(s)$ (Lemma 12.9).

By Lemmas 12.13 (applied with $S = \operatorname{Spec} K$) and 12.14, we can find all Mumford coordinates $Q_{(A,\mathcal{L},\beta)}$ on A (for the given polarization). Then we simply compute, for each $(\mathcal{L}, \beta)$, the inverse image of $Q_{(A,\mathcal{L},\beta)} \in \mathbb{P}(V(\delta))$ under $Q_{\mathcal{A}'}$. □

References.

[Alp20] Levent Hasan Ali Alpöge. *Points on Curves*. ProQuest LLC, Ann Arbor, MI, 2020. Thesis (Ph.D.)–Princeton University.

[Alp21] Levent Alpöge. Modularity and effective mordell i, 2021.

[Bak66] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika*, 13:204–216; ibid. **14** (1967), 102–107; ibid. **14** (1967), 220–228, 1966.

[BC70] A. Baker and J. Coates. Integer points on curves of genus 1. *Proc. Cambridge Philos. Soc.*, 67:595–602, 1970.

[BHC62a] Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Annals of Mathematics*, 75(3):485–535, 1962.

[BHC62b] Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math. (2)*, 75:485–535, 1962.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[Bos96] Jean-Benoît Bost. Périodes et isogénies des variétés abéliennes sur les corps de nombres. In *Séminaire Bourbaki : volume 1994/95, exposés 790-804*, number 237 in Astérisque. Société mathématique de France, 1996. talk:795.

[Cb23a] N. Chebotarev (Н. Чеботарёв). Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок. I. Известия Российской Академии Наук. *VI*, 17:205–230, 1923.

[Cb23b] N. Chebotarev (Н. Чеботарёв). Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок. II. Известия Российской Академии Наук. *VI*, 17:231–250, 1923.

[Coh00] H. Cohen. *Advanced Topics in Computational Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer, 2000.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Ann. of Math. (2)*, 74:425–436, 1961.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[FM95] Jean-Marc Fontaine and Barry Mazur. Geometric galois representations. In John Coates and S.T̃. Yau, editors, *Elliptic Curves, Modular Forms, & Fermat's Last Theorem*. 1995.

[Gas21] William Gasarch. Hilbert's tenth problem: Refinements and variants, 2021.

[GR14] Éric Gaudron and Gaël Rémond. Polarisations et isogénies. *Duke Math. J.*, 163(11):2057–2108, 2014.

[GS80] Fritz Grunewald and Daniel Segal. Some general algorithms. I. Arithmetic groups. *Ann. of Math. (2)*, 112(3):531–583, 1980.

[LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

[LV20] Brian Lawrence and Akshay Venkatesh. Diophantine problems and p-adic period mappings. *Inventiones Mathematicae*, 221:893–999, 2020.

[Mb70] Y. V. Matiyasevich (Ю. В. Матиясевич). Диофантовость перечислимых множеств. Ленинградское отделение Математического института им. В. А. Стеклова АН СССР, 191:279–282, 1970.

[Moo19] Ben Moonen. A remark on the tate conjecture. *J. Algebraic Geom*, 28:599–603, 2019.

[MR08] D. Mumford and C.P. Ramanujam. *Abelian Varieties*. Studies in mathematics. Hindustan Book Agency, 2008.

[Mum66] D. Mumford. On the equations defining abelian varieties, i. *Invent. math.*, 1:287–354, 1966.

[Mum67] D. Mumford. On the equations defining abelian varieties, ii. *Invent. math.*, 3:75–135, 1967.

[MW93] David Masser and Gisbert Wustholz. Isogeny estimates for abelian varieties, and finiteness theorems. *Annals of Mathematics*, 137:459–472, 1993.

[NN81] M. S. Narasimhan and M. V. Nori. Polarisations on an abelian variety. *Proc. Indian Acad. Sci. Math. Sci.*, 90(2):125–128, 1981.

[PVZ16] Stefan Patrikis, José Voloch, and Yuri Zarhin. Anabelian geometry and descent obstructions on moduli spaces. *Algebra Number Theory*, 10(6):1191–1219, 2016.

[Sun92] Zhi Wei Sun. A new relation-combining theorem and its application. *Z. Math. Logik Grundlag. Math.*, 38(3):209–212, 1992.

[Sun21] Zhi-Wei Sun. Further results on Hilbert's tenth problem. *Sci. China Math.*, 64(2):281–306, 2021.

[Tao16] Terence Tao. *Analysis. II*, volume 38 of *Texts and Readings in Mathematics*. Hindustan Book Agency, New Delhi; Springer, New Delhi, third edition, 2016. Electronic edition of [MR3310023].

[Wei95] André Weil. *Basic Number Theory, Third Edition*. Springer-Verlag, 1995.