SURJECTIVITY OF GALOIS REPRESENTATIONS IN RATIONAL FAMILIES OF ABELIAN VARIETIES

AARON LANDESMAN, ASHVIN A. SWAMINATHAN, JAMES TAO, AND YUJIE XU

ABSTRACT. In this article, we show that for any non-isotrivial family of abelian varieties over a rational base with big monodromy, those members that have adelic Galois representation with image as large as possible form a density-1 subset. Our results can be applied to a number of interesting families of abelian varieties, such as rational families dominating the moduli of Jacobians of hyperelliptic curves, trigonal curves, or plane curves. As a consequence, we prove that for any dimension $g \geq 3$, there are infinitely many abelian varieties over $\mathbb{Q}$ with adelic Galois representation having image equal to all of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$.

1. INTRODUCTION AND STATEMENT OF RESULTS

1.1. **Background.** One of the most significant breakthroughs in the theory of Galois representations came in 1972, when Serre proved the Open Image Theorem for elliptic curves in his seminal paper [Ser72]. Serre's theorem states that for any elliptic curve E over a number field K without complex multiplication, the image of the associated *adelic* Galois representation ρ_E is an open subgroup of the general symplectic group $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$.[1] The Open Image Theorem not only gives rise to many important corollaries – from the simple consequence that the image of ρ_E has finite index in $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$, to the intriguing result that the density of supersingular primes of E is 0 – but recently, within the past two decades, the theorem has also inspired a body of research concerning the following question:

Question. *How large can the image of the adelic Galois representation associated to an elliptic curve be, and how often do elliptic curves attain this largest possible Galois image?*

The first major result addressing the above question was achieved by Duke in [Duk97]. He proved that for "most" elliptic curves E over $\mathbb{Q}$ in the standard family with Weierstrass equation $y^2 = x^3 + ax + b$, the image of the *mod-ℓ reduction* of ρ_E is all of $\mathrm{GSp}_2(\mathbb{Z}/\ell\mathbb{Z})$ for every prime number ℓ; here and in what follows, "most" means a density-1 subset of curves ordered by naïve height. Duke's result does not imply, however, that ρ_E surjects onto $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$ for most E. In fact, as Serre observes in [Ser72], the image of ρ_E has index divisible by 2 in $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$ for every elliptic curve $E/\mathbb{Q}$. Nonetheless, Jones proves in [Jon10, Theorem 4] that most elliptic curves E in the standard family over $\mathbb{Q}$ have *adelic* Galois representations with image as large as possible (i.e., with index 2 in $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$).

The obstruction to having surjective adelic Galois representation faced by elliptic curves over $\mathbb{Q}$ does not occur over other number fields. In [Gre10, Theorem 1.5], Greicius constructed the first explicit example of an elliptic curve over a number field with Galois image

---

[1]Recall that $\mathrm{GSp}_2(\widehat{\mathbb{Z}}) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$; here, we prefer to use the less common symplectic notation so as to highlight the analogy between the elliptic curve case and that of higher dimensional abelian varieties.

equal to all of $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$. Greicius' example is not the only elliptic curve with this property: in [Zyw10a, Theorem 1.2], Zywina employs the above result of Jones to show that most elliptic curves in the standard family over a number field $K \neq \mathbb{Q}$ have Galois image equal to all of $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$ as long as $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$, where $\mathbb{Q}^{\mathrm{cyc}}$ is the maximal cyclotomic extension of $\mathbb{Q}$. Subsequently, in [Zyw10b, Theorem 1.15], Zywina achieves an intriguing generalization of this result: using a variant of Hilbert's Irreducibility Theorem, he shows that most members of *every* non-isotrivial rational family of elliptic curves over *any* number field have Galois image as large as possible given the constraints imposed by the arithmetic and geometric properties of the family. Further results over $\mathbb{Q}$ were obtained in [Gra00], [CH05], and [CGJ11] (see [Zyw10b, p. 6] for a more detailed overview).

Given that the above question is so well-studied in the context of elliptic curves, it is natural to ask whether any of the aforementioned theorems extend to abelian varieties of higher dimension. As it happens, explicit examples of curves whose Jacobians have maximal Galois image have been constructed: it follows from the results of [Die02] and [Zyw15] that one can algorithmically write down equations of abelian surfaces and three-folds over $\mathbb{Q}$ with Galois image as large as possible. Moreover, there are several results showing that in a family of abelian varieties, "most" fibers lying over closed points of the base have Galois image with finite index in the Galois image of the family. For instance, in [Cad15], (see also [CM15]) the author shows that the set of fibers lying over K-points of the base for which the associated Galois image does *not* have finite index in that of the family is a thin set. Furthermore, in [CT12] and [CT13], the authors show that when the base of the family is a curve, the set of fibers lying over K-points of the base (and more generally closed points of bounded degree) for which the associated Galois image does *not* have finite index in that of the family is a finite set. However, we are not aware of any results in the literature describing the density of higher-dimensional abelian varieties whose adelic Galois representations have maximal image (as opposed to merely having finite index) in that of the family.

1.2. **Main Result.** The primary objective of this article is to prove that an analogue of Zywina's result for rational families of elliptic curves in [Zyw10b, Theorem 1.15] holds for abelian varieties of arbitrary dimension, subject to a mild hypothesis on the *monodromy* (i.e., Galois image) of the family under consideration. Before stating our theorems, we must establish some of the requisite notation; we expatiate upon this and other important background material in Section 3.1, where precise definitions are provided.

Let K be a number field with fixed algebraic closure $\overline{K}$, let $U \subset \mathbb{P}_K^r$ be a dense open subscheme, and let $A \to U$ be a family of g-dimensional principally polarized abelian varieties (henceforth, PPAVs). Let $H_A \subset \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ be the monodromy of the family and let $H_{A_u} \subset H_A$ be the monodromy of the fiber A_u over $u \in U$. Finally, to facilitate our enumeration of PPAVs, let $\mathrm{Ht} \colon \mathbb{P}^r(\overline{K}) \to \mathbb{R}_{>0}$ denote the absolute multiplicative height on projective space,[2] and define a height function $\| - \|$ on the lattice $\mathcal{O}_K^r$ sending $(t_1, \ldots, t_r) \mapsto \max_{\sigma, i} |\sigma(t_i)|$, where σ varies over all field embeddings $\sigma \colon K \hookrightarrow \mathbb{C}$. Our main result is stated as follows:

Theorem 1.1. *Let B, n be arbitrary positive real numbers, and suppose that the rational family $A \to U$ is non-isotrivial and has big monodromy, meaning that H_A is open in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. Let $\delta_{\mathbb{Q}}$ be the index of the closure of the commutator subgroup of H_A in $H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, and let $\delta_K = 1$ for $K \neq \mathbb{Q}$. Then $[H_A : H_{A_u}] \geq \delta_K$ for all $u \in U(K)$, and we have the following*

---

[2]See [HS00, Section B.2, p. 174] for the definition.

asymptotic statements:

$$\frac{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B, [H_A : H_{A_u}] = \delta_K\}|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|} = 1 + O((\log B)^{-n}), \;\; and$$

$$\frac{|\{u \in U(K) : \mathrm{Ht}(u) \leq B, [H_A : H_{A_u}] = \delta_K\}|}{|\{u \in U(K) : \mathrm{Ht}(u) \leq B\}|} = 1 + O((\log B)^{-n}),$$

where the implied constants depend only on $A \to U$ and n.

Remark 1.1. Notice that Theorem 1.1 holds trivially in dimension 0. In [Zyw10b, Theorem 1.15], where the 1-dimensional case of Theorem 1.1 is treated, Zywina bounds the error more sharply, by $O((\log B)B^{-1/2})$ as opposed to our bound of $O((\log B)^{-n})$. In what follows, we shall primarily restrict ourselves to the case where the dimension g is at least 2.

Remark 1.2. In [Wal14], Wallace studies a variant of Theorem 1.1 in the 2-dimensional case. Unfortunately, his argument relies upon a mistaken Masser-Wüstholz-type result of Kawamura, [Kaw03, Main Theorem 2]. Although Wallace describes in [Wal14, p. 468] how to correct some of the errors in Kawamura's proof, the modified argument still appears to be mistaken; see [Lom16, p. 27] for a description of one error in Kawamura's argument that Wallace does not adequately address. Using the result stated in Appendix A, written by Davide Lombardo, we are able to patch this error in Wallace's argument.

Remark 1.3. The locus of $u \in U(K)$ with $[H_A : H_{A_u}] > \delta_K$ will not in general be Zariski-closed, so the "sparseness" of this locus can only be quantified by an asymptotic statement. To see why, consider the family of elliptic curves over K given by the Weierstrass equations $y^2 = x^3 + x + a$ for $a \in K$. Note that the mod-2 reduction of the monodromy is nontrivial for the family but is trivial for infinitely many members of the family, namely those for which the defining polynomial $x^3 + x + a$ factors completely over K.

We now outline the proof of Theorem 1.1. Hilbert's Irreducibility Theorem is the prototype for results like Theorem 1.1, but it only applies in the setting of finite groups. Indeed, the phenomenon that Galois representations associated to elliptic curves over $\mathbb{Q}$ *never* surject onto $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$ shows that Hilbert's Irreducibility Theorem cannot hold for infinite groups. However, when $A \to U$ has *big monodromy*, in the sense that H_A is open in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$, the problem is essentially reduced to showing that, for most $u \in U(K)$, the mod-ℓ reduction of H_{A_u} contains $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for each sufficiently large prime ℓ. This reduction uses an infinite version of Goursat's lemma. Since these mod-ℓ reductions are *finite* groups, the naïve expectation is that Hilbert's Irreducibility Theorem can be applied once for each ℓ. Unfortunately, the sum of the resulting error terms does not *a priori* converge to zero.

To overcome this problem, we divide the primes ℓ into three regions.

(a) We handle all sufficiently large primes by means of a delicate argument involving the large sieve that allows us to apply a recent result of Lombardo (namely, [Lom15, Theorem 1.2] and Proposition A.2).

(b) For the smaller primes, Wallace's effective version of the Hilbert Irreducibility Theorem gives sufficiently good error terms. His approach is to complete $\phi : U \to \mathrm{Spec}\, K$ to a map $\widetilde{\phi} : \mathcal{U} \to \mathrm{Spec}\, \mathcal{O}_K$ (see Section 3.2), and then to apply the large sieve using information gleaned from the special fibers of $\widetilde{\phi}$. To ensure that the monodromy maps associated to special fibers of $\widetilde{\phi}$ capture enough information about the monodromy of the whole family, we assume the family is non-isotrivial and has big

monodromy. Our main contribution to this step is an application of the Grothendieck Specialization Theorem, which shows that Wallace's Property (A2)—concerning the relation between the monodromy maps associated to a geometric *special* fiber and to a geometric *generic* fiber—holds in a very general setting.
   (c) Lastly, to handle the finitely many primes that remain, the Cohen-Serre version of the Hilbert Irreducibility Theorem suffices.
We encourage the reader to refer to Section 4.1 for a more detailed discussion of the intricate arguments outlined above.

Remark 1.4. Note that the proof strategy outlined above is greatly influenced by the methods that Zywina employed in [Zyw10b] to handle the case where $g = 1$ and also by unpublished work of Zureick-Brown and Zywina. In particular, the idea of formulating the problem in terms of monodromy groups and solving it by applying effective versions of Hilbert's Irreducibility Theorem and Serre's Open Image Theorem is largely due to them.

Zureick-Brown and Zywina were the first to state a version of Theorem 1.1. Indeed, in a 2013 talk at the Institute for Advanced Study, Zywina announced that he and Zureick-Brown had proven a result very much like Theorem 1.1 using a strategy similar to that outlined above. Following this talk, Deligne suggested a potential way to strengthen the result by removing the hypothesis that the family has big monodromy, and it is our understanding that Zywina has been attempting to remove this hypothesis by following Deligne's suggestion and that his work is still in progress. As the details of the work of Zureick-Brown and Zywina are not available, we have worked out a modified approach that utilizes recent results of Wallace ([Wal14]) and Lombardo ([Lom15]) that had not been published at the time of Zywina's talk. In light of the above, we would like to extend a special acknowledgment to Zureick-Brown and Zywina for formulating the questions that motivated our work and for introducing the ideas that inspired our proof of Theorem 1.1.

1.3. **Applications.** We record a number of interesting applications of our main result. These and several further applications are stated and proven in Theorem 5.4.

Theorem 1.2 (Abbreviation of Theorem 5.4). *Let $\mathscr{A}_g$ denote the moduli stack of g-dimensional PPAVs, suppose $A \to U$ is a rational family, and let V be the smallest locally closed substack of $\mathscr{A}_g$ through which $U \to \mathscr{A}_g$ factors. The conclusion of Theorem 1.1 holds if V is normal and contains a dense open substack of any of the following loci:*
   (a) *the substack of Jacobians of hyperelliptic curves, or*
   (b) *the substack of Jacobians of trigonal curves, or*
   (c) *the substack of Jacobians of plane curves of degree d (see Remark 5.1 for a more precise description of this substack), or*
   (d) *the substack of Jacobians of all curves in $\mathscr{M}_g$, or*
   (e) *the moduli stack $\mathscr{A}_g$.*

Theorem 1.2 has the following noteworthy corollary:

Corollary 1.3. *For every $g > 2$, there exist infinitely many PPAVs A over $\mathbb{Q}$ with the property that $\rho_A(G_{\mathbb{Q}}) = \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$.*

Proof. Let $\mathscr{T}^g(g \bmod 2) \subset \mathscr{A}_g$ denote the locus of trigonal curves over $\mathbb{Q}$ of lowest Maroni invariant (as defined at the beginning of Section 5.2). We have that $\mathscr{T}^g(g \bmod 2)$ is rational and normal when $g > 2$ (by Theorem 5.4 (b)) and has monodromy equal to all of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$

when $g > 2$ (by Remark 5.2). Since $\mathscr{T}^g(g \bmod 2)$ is a dense open substack of the locus Jacobians of trigonal curves, Theorem 1.2 implies that Theorem 1.1 applies to $\mathscr{T}^g(g \bmod 2)$. $\square$

Remark 1.5. The above proof of Corollary 1.3 is not constructive. For explicit examples of 1-, 2-, and 3-dimensional PPAVs with maximal adelic Galois representations, see [Gre10, Theorem 1.5] and [Ser72, Sections 5.5.6-8], [LSTX17a], and [Zyw15, Theorem 1.1], respectively.

We conclude this section with a representative example, which has incidentally enjoyed significant discussion in the literature.

Example 1.4. In this example, we take our family to be the Hilbert scheme $\mathscr{H}_4$ of plane curves of degree 4 over $\mathbb{Q}$. There is quite a bit of earlier work concerning Galois representations associated to Jacobians of such curves. For instance, a single example of a plane quartic such that the adelic Galois representation associated to its Jacobian has image equal to $\mathrm{GSp}_6(\widehat{\mathbb{Z}})$ is given in [Zyw15, Theorem 1.1]. In [ALS16, Corollary 1.1], an example of a genus-3 hyperelliptic curve whose Jacobian has mod-ℓ monodromy equal to $\mathrm{GSp}_6(\mathbb{Z}/\ell\mathbb{Z})$ for primes $\ell \geq 3$ is constructed. For any $\ell \geq 13$, [AdRAK$^+$16, Theorem 0.1] gives an infinite family of 3-dimensional PPAVs with mod-ℓ monodromy equal to $\mathrm{GSp}_6(\mathbb{Z}/\ell\mathbb{Z})$. All of these existence statements are subsumed by the main results of the present article: indeed, from Remark 5.2 and Theorem 1.2, we obtain the considerably stronger statement that a density-1 subset of this family has Galois representation with image equal to $\mathrm{GSp}_6(\widehat{\mathbb{Z}})$.

The rest of this paper is organized as follows. In Section 2, we define the symplectic group and prove properties concerning its open and closed subgroups. In Section 3, we introduce the basic definitions and properties associated to Galois representations of abelian varieties and families thereof. These definitions and properties are used heavily in Section 4, which is devoted to proving the main theorem of this article, Theorem 1.1. In Section 5, we show that Theorem 1.1 can be applied to study many interesting families of PPAVs, and in so doing, we prove a result that implies Theorem 1.2. Finally, in Appendix A, Davide Lombardo proves a key input that we employ in Section 4 to handle the genus-2 case of Theorem 1.1.

2. Definitions and Properties of Symplectic Groups

In this section, we first detail the basic definitions and properties of symplectic groups, and we then proceed to prove a few group-theoretic lemmas that are used in our proof of the main result of this paper, Theorem 1.1. The reader should feel free to proceed to Section 3 upon reading the statements of Propositions 2.5 and 2.6.

2.1. **Symplectic Groups.** Fix a commutative ring R, a free R-module M of rank $2g$ for some positive integer g, and a non-degenerate alternating bilinear form $\langle -, - \rangle \colon M \times M \to R$. Define the *general symplectic group* (alternatively, the *group of symplectic similitudes*) $\mathrm{GSp}(M)$ to be the subgroup of $\mathrm{GL}(M)$ consisting of all R-automorphisms S such that there exists some $m_S \in R^\times$, called the *multiplier* of S, satisfying $\langle Sv, Sw \rangle = m_S \cdot \langle v, w \rangle$ for all $v, w \in M$. One readily observes that the *mult* map

$$\mathrm{mult} \colon \mathrm{GSp}(M) \to R^\times$$
$$S \mapsto m_S$$

is a group homomorphism, and its kernel is the *symplectic group*, denoted by $\mathrm{Sp}(M)$.

By choosing a suitable R-basis for M, we can arrange for the corresponding matrix of the inner product $\langle -, - \rangle$ to be given by

$$\Omega_{2g} = \left[\begin{array}{c|c} 0 & \mathrm{id}_g \\ \hline -\mathrm{id}_g & 0 \end{array} \right],$$

where id_g denotes the $g \times g$ identity matrix. From this choice of basis we obtain an identification $\mathrm{GL}(M) \simeq \mathrm{GL}_{2g}(R)$. We then define $\mathrm{GSp}_{2g}(R)$ to be the image of $\mathrm{GSp}(M)$ and $\mathrm{Sp}_{2g}(R)$ to be the image of $\mathrm{Sp}(M)$ under this identification. Let $\det \colon \mathrm{GL}_{2g}(R) \to R^\times$ be the determinant map. Since the diagram

$$\mathrm{GSp}(M) \overset{\sim}{\longrightarrow} \mathrm{GSp}_{2g}(R)$$
$$\underset{\mathrm{mult}^g}{\searrow} \quad \downarrow{\scriptstyle \det}$$
$$R^\times$$

commutes, where the diagonal map is the multiplier map raised to the gth power, one deduces that $\mathrm{GSp}_{2g}(R)$ is in fact the subgroup of $\mathrm{GL}_{2g}(R)$ consisting of all invertible matrices S satisfying $S^T \Omega_{2g} S = (\mathrm{mult}\, S)\, \Omega_{2g}$ and that $\mathrm{Sp}_{2g}(R) = \ker(\mathrm{mult} \colon \mathrm{GSp}_{2g}(R) \to R^\times)$.

Let $\mathrm{Mat}_{2g \times 2g}(R)$ denote the space of $2g \times 2g$ matrices with entries in R. In subsequent subsections, we will make heavy use of the "Lie algebra" $\mathfrak{sp}_{2g}(R)$, which is defined by

$$\mathfrak{sp}_{2g}(R) := \{ M \in \mathrm{Mat}_{2g \times 2g}(R) : M^T \Omega_{2g} + \Omega_{2g} M = 0 \}.$$

It is easy to see that $M^T \Omega_{2g} + \Omega_{2g} M = 0$ is equivalent to M being a block matrix with $g \times g$ blocks of the form

$$M = \left[\begin{array}{c|c} A & B \\ \hline C & -A^T \end{array} \right],$$

where B and C are symmetric.

For the purpose of studying Galois representations associated to PPAVs, we will be primarily interested in the cases where the ring R is the profinite completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$, the ring of ℓ-adic integers $\mathbb{Z}_\ell$ for a prime number ℓ, or the finite cyclic ring $\mathbb{Z}/m\mathbb{Z}$ for a positive integer m. Note in particular that we have the identifications

$$(2.1) \qquad\qquad \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \simeq \varprojlim_k \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}) \quad \text{and}$$

$$(2.2) \qquad\qquad \prod_{\mathrm{prime}\ \ell} \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \simeq \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \simeq \varprojlim_m \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}).$$

From (2.1) and (2.2), we obtain the ℓ-adic projection map $\pi_\ell \colon \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ and the mod-m reduction map $r_m \colon \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$. Observe that (2.1) and (2.2) both hold with GSp_{2g} replaced by Sp_{2g}.

2.2. **Notation.** In what follows, we study subquotients of $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$, and $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})$ for ℓ a prime number and k a positive integer. We use the following notational conventions:

- Let $H \subset \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ be a closed subgroup.
- Let $H_\ell := \pi_\ell(H) \subset \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ be the ℓ-adic reduction of H. More generally, for any set S of prime numbers, let H_S denote the projection of H onto $\prod_{\ell \in S} \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$.

- Let $H(m) = r_m(H) \subset \mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ be the mod-m reduction of H. We often take $m = \ell^k$.
- Let $\Gamma_{\ell^k} = \ker(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}))$. Notice that the map $M \mapsto \mathrm{id}_{2g} + \ell^k M$ gives an isomorphism of groups

$$\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \simeq \ker(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^{k+1}\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}))$$

  for every $k \geq 1$, so we will use $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ to denote the above kernel.
- For any group G, let $[G, G]$ be its commutator subgroup, and let $G^{\mathrm{ab}} := G/[G, G]$ be its abelianization.
- For any group G, let $\mathrm{Quo}(G)$ the set of isomorphism classes of finite non-abelian simple quotients of G, and let $\mathrm{Occ}(G)$ be the set of isomorphism classes of finite non-abelian simple *sub*quotients of G.
- For any positive integer m, let S_m denote the symmetric group on m letters.

2.3. **Generalizing Goursat's Lemma.** In Sections 2.4 and 2.5, it will be crucial for us to have a theorem that allows us to express a subgroup of $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ as (roughly) the product of its ℓ-adic projections. A natural tool for doing this is Goursat's lemma, but in much of the literature (e.g., [Rib76, Lemma 5.2.1] and [Zyw10a, Lemma A.4]), this result is stated for *finite* products or for *finite* groups. This section is devoted to proving Lemma 2.2, which generalizes Goursat's lemma to apply in the setting that we need, namely for *countable* products of *profinite* groups.

Lemma 2.1. *Let $G = \prod_{i=1}^n G_i$ be a product of profinite groups. Then every finite simple quotient of G is a finite simple quotient of G_i for some i, and vice versa.*

Proof. Consider a finite simple quotient $\phi : G \twoheadrightarrow H$. Since each $G_i \subset G$ is normal, the image $\phi(G_i) \subset H$ is also normal. For any i, if $\phi(G_i)$ is larger than $\{1\}$, then it equals H since H is simple, and the composition $G_i \hookrightarrow G \twoheadrightarrow H$ expresses H as a quotient of G_i. If no such i exists, then $\ker \phi = G$, contradiction. The "vice versa" statement is obvious. $\square$

Lemma 2.2 (Generalized Goursat's Lemma). *Let A be a countable set, and suppose $\{G_\alpha\}_{\alpha \in A}$ is a collection of profinite groups such that, for all pairs $\alpha, \beta \in A$ with $\alpha \neq \beta$, the groups G_α and G_β have no finite simple quotients in common. Let $G := \prod_{\alpha \in A} G_\alpha$, and let $\pi_\alpha : G \to G_\alpha$ be the natural projections. If $H \subset G$ is a closed subgroup with $\pi_\alpha(H) = G_\alpha$ for all $\alpha \in A$, then $H = G$.*

Proof. First take $A = \{1, 2\}$, so that $G = G_1 \times G_2$. The subgroup $N_1 \times \{1\} := (G_1 \times \{1\}) \cap H \subset G$ is normal because $\pi_1(H) = G_1$. This means N_1 is a normal subgroup of G_1. Similarly for the subgroup $\{1\} \times N_2$. With these definitions, the closed subgroup $H/(N_1 \times N_2) \subset (G_1/N_1) \times (G_2/N_2)$ surjects onto each factor via the natural projections. We have thereby reduced to the case $N_1 = N_2 = 0$. By [Rib76, Lemma 5.2.1], we know that $G_1 \simeq G_2$ as profinite groups. The result follows because two isomorphic profinite groups have a nontrivial finite simple quotient in common (and any quotient of G_i/N_i is *a priori* a quotient of G_i).

Now take $A = \{1, 2, \ldots, n\}$ for $n \geq 3$, and suppose (by induction) that the result has been proven for $n - 1$. For any $H \subset G = \prod_{i=1}^n G_i$ satisfying the hypotheses of the theorem, let H' be the image of H under the projection $G \twoheadrightarrow \prod_{i=1}^{n-1} G_i$. Then H' satisfies the hypotheses for $n - 1$, so we conclude that $H' = \prod_{i=1}^{n-1} G_i$. By Lemma 2.1, the groups $\prod_{i=1}^{n-1} G_i$ and G_n have no finite simple quotients in common, so the $n = 2$ case tells us that $H = G$.

The only remaining case is $A = \{1, 2, \ldots\}$. Consider $H \subset G$ satisfying the hypotheses of the theorem. For each n, let $H_{\{1,2,\ldots,n\}}$ be the image of H under the projection $G \twoheadrightarrow \prod_{i=1}^{n} G_i$. By the finite case prove above, we know that $H_{\{1,2,\ldots,n\}} = \prod_{i=1}^{n} G_i$ for each $n \geq 1$. Fix an element $g := (g_i)_{i \geq 1} \subset G$, and define a sequence $\{h_1, h_2, \ldots\}$ of elements of H as follows: let h_n be any element of H whose image in $\prod_{i=1}^{n} G_i$ equals $(g_1, \ldots, g_n)$. In the product topology, $h_n \to g$ as $n \to \infty$, so $g \in H$ since H is closed. Since $g \in G$ was arbitrary, we conclude that $H = G$. $\qquad\square$

2.4. **Closed Subgroups of** $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$**.** As before, let $H \subset \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ be a closed subgroup. The main result of this section is Proposition 2.5, which shows that properties of H can be deduced from corresponding properties of the ℓ-adic projections $H_\ell \subset \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ as ℓ ranges over the prime numbers. We use Proposition 2.5 crucially in our proof of the main theorem, Theorem 1.1, and more specifically in the proof of Proposition 4.2.

The next lemma enables us to verify the conditions required for applying Lemma 2.2:

Lemma 2.3. *If $g > 2$ or $\ell > 2$, we have* $\mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) = \{\mathrm{PSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})\}$. *Moreover, for all $g \geq 2$, we have* $\mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) \cap \mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}_{\ell'})) = \varnothing$ *if $\ell \neq \ell'$.*

Proof. Since Γ_ℓ is a pro-ℓ group, we have that $\mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) = \mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}))$. Furthermore, quotienting by $\{\pm \mathrm{id}_{2g}\}$, we have that $\mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})) = \mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})/\{\pm \mathrm{id}_{2g}\})$. By [O'M78, Theorem 3.4.1], we have $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})/\{\pm \mathrm{id}_{2g}\} = \mathrm{PSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is simple for $g > 2$ or $\ell > 2$. It follows that $\mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) = \{\mathrm{PSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})\}$ in this case.

To finish the proof, note that $\mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) \cap \mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}_{\ell'})) = \varnothing$ for $g > 2$ or $\ell, \ell' > 2$ because $\mathrm{PSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \neq \mathrm{PSp}_{2g}(\mathbb{Z}/\ell'\mathbb{Z})$ for $\ell \neq \ell'$ because their orders are different. The only remaining case is where $g = 2$, $\ell = 2$, and $\ell' > 2$. In this case, observe that $\mathrm{PSp}_{2g}(\mathbb{Z}/\ell'\mathbb{Z}) \notin \mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z}))$ for $\ell' > 2$, since the order of $\mathrm{PSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ exceeds that of $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. $\quad\square$

We next prove Proposition 2.4, which we then use to deduce the main result of this section, Proposition 2.5.

Proposition 2.4. *Let $g \geq 2$ and let $H \subset \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ be a closed subgroup. Suppose there is a prime number $p \geq 2$ so that $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell > p$. Then we have that*

$$(2.3) \qquad\qquad H = H_{\{\ell \leq p\}} \times \prod_{\ell > p} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell).$$

Idea of Proof. The idea of the proof is to apply Lemma 2.2 to conclude that if the group surjects onto each factor, then it surjects onto the product. We verify the hypotheses of Lemma 2.2 using Lemma 2.3 and the fact that all simple quotients of $H_{\{\ell \leq p\}}$ have smaller order than $\mathrm{PSp}_{2g}(\mathbb{Z}_\ell)$ for $\ell > p$.

Proof. The case where $g = 1$ is handled by [Zyw10b, Lemma 7.6], so take $g \geq 2$. By [LSTX17b, Theorem 1], the fact that $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ implies that $H_\ell = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for all $\ell > p$.

The proposition follows upon applying Lemma 2.2 to the product $H_{\{\ell \leq p\}} \times \prod_{\ell > p} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. However, to apply it, we must check that no two of the groups $H_{\{\ell \leq p\}}$ and $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for $\ell > p$ have any finite simple quotients in common. From [LSTX17b, Proposition 1, part (a)], we have that the group $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ has trivial abelianization for $\ell > 2$ and thus has no finite abelian simple quotients. Thus, it remains to verify that the sets of nonabelian simple quotients $\mathrm{Quo}(H_{\{\ell \leq p\}})$ and $\mathrm{Quo}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell))$ for $\ell > p$ are all pairwise disjoint. Our strategy

for checking this condition is to bound the sizes of the groups appearing in $\mathrm{Quo}(H_{\{\ell \leq p\}})$. First, observe that

$$\mathrm{Quo}(H_{\{\ell \leq p\}}) \subset \mathrm{Occ}\left(\prod_{\ell \leq p} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)\right) = \bigcup_{\ell \leq p} \mathrm{Occ}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)),$$

where the last step follows from the first displayed equation of [Ser98, p. IV-25]. But $\mathrm{Occ}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) = \mathrm{Occ}(\Gamma_\ell) \cup \mathrm{Occ}(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}))$, and $\mathrm{Occ}(\Gamma_\ell) = \varnothing$ because Γ_ℓ is a pro-ℓ group, so $\mathrm{Occ}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) = \mathrm{Occ}(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}))$. Because $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is not simple, every element of $\mathrm{Occ}(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}))$ is bounded in size by $|\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|/2$, so every element of $\mathrm{Quo}(H_{\{\ell \leq p\}})$ is bounded in size by $|\mathrm{Sp}_{2g}(\mathbb{Z}/p\mathbb{Z})|/2$. Observing that

$$\frac{1}{2} \cdot |\mathrm{Sp}_{2g}(\mathbb{Z}/p\mathbb{Z})| < |\mathrm{PSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|$$

for every $\ell > p$, the desired condition follows by applying Lemma 2.3. $\qquad\square$

Proposition 2.5. *Let $G \subset \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ be an open subgroup. There exists a positive integer M such that, for every closed subgroup $H \subset G$, we have $H = G$ if and only if $H(M) = G(M)$ and $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for every prime $\ell \nmid M$.*

Idea of Proof. The idea of the proof is to find a sufficiently large M so that if $H(M) = G(M)$ then $H_{\{\ell \nmid M\}} = G_{\{\ell \nmid M\}}$, which reduces the problem to the situation of Proposition 2.4.

Proof. Again, the case where $g = 1$ is handled in [Zyw10b, Lemma 7.6], so take $g \geq 2$. Let p be any prime such that $G(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for all primes $\ell > p$. Observe that the groups Γ_{ℓ^k} are open in $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ because they have finite index in $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. Since $G \subset \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ is open, the group $G_{\{\ell \leq p\}} \subset \prod_{\ell \leq p} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ is open too, so there exist exponents $e(\ell) \geq 1$ with the property that

$$\prod_{\ell \leq p} \Gamma_{\ell^{e(\ell)}} \subset G_{\{\ell \leq p\}}.$$

Since the groups Γ_{ℓ^k} are finitely generated pro-ℓ open normal subgroups of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$, condition (ii) from [Ser97, Proposition 10.6] is satisfied. Hence, the equivalence of conditions (ii) and (iv) from [Ser97, Proposition 10.6] implies that the Frattini subgroup defined by

$$\Phi(G_{\{\ell \leq p\}}) := \bigcap_{\substack{S \subset G_{\{\ell \leq p\}} \\ S \text{ maximal closed in } G_{\{\ell \leq p\}}}} S$$

is open and normal in $G_{\{\ell \leq p\}}$. This means we can find exponents $e'(\ell) \geq 1$ such that

$$\prod_{\ell \leq p} \Gamma_{\ell^{e'(\ell)}} \subset \Phi(G_{\{\ell \leq p\}}).$$

Define $M := \prod_{\ell \leq p} \ell^{e'(\ell)}$. Then $H(M) = G(M)$ implies that $H_{\{\ell \leq p\}} = G_{\{\ell \leq p\}}$.

Now take H satisfying $H(M) = G(M)$ and $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for every prime $\ell \nmid M$. We have that

$$H \subset G \subset H_{\{\ell \leq p\}} \times \prod_{\ell > p} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell).$$

To show that $H = G$, we need only verify

$$H = H_{\{\ell \leq p\}} \times \prod_{\ell > p} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell),$$

which follows immediately from Proposition 2.4. $\qquad\square$

2.5. **Open Subgroups of** $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$**.** We now return to studying the general symplectic group $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. The main result of this subsection tells us that the closure of the commutator subgroup of an open subgroup of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ is open:

Proposition 2.6. *Let $g \geq 2$, and let $H \subset \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ be an open subgroup. Then the closure of $[H, H]$ is an open subgroup of $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$.*

In order to prove Proposition 2.6, we shall require a number of preliminary lemmas, which are stated and proven in Sections 2.5.1 and 2.5.2.

2.5.1. *Openness Condition.* The next two lemmas give us a criterion for openness in $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$:

Lemma 2.7. *Let S be a finite set of prime numbers, and let $H \subset \prod_{\ell \in S} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ be a closed subgroup. If each $H_\ell \subset \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ is open, then $H \subset \prod_{\ell \in S} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ is open.*

Proof. There exists a finite-index subgroup $H' \subset H$ such that $H'(\ell)$ is trivial for every $\ell \in S$, namely the intersection of the kernels of the mod-ℓ reductions maps $H \to H(\ell)$. Since each H'_ℓ is a pro-ℓ group, Lemma 2.2 implies that $H' = \prod_{\ell \in S} H'_\ell$. Thus, H contains an open subgroup and is therefore itself open. $\qquad\square$

Lemma 2.8. *Let $g \geq 2$ and let $H \subset \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ be a closed subgroup. If $H_{\ell'}$ is open in $\mathrm{Sp}_{2g}(\mathbb{Z}_{\ell'})$ for all ℓ' and $H_\ell = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for all but finitely many ℓ, then H is open in $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$.*

Proof. Let p be the largest prime with $H_p \neq \mathrm{Sp}_{2g}(\mathbb{Z}_p)$. By Lemma 2.7, we have that $H_{\{\ell \leq p\}} \subset \prod_{\ell \leq p} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ is an open subgroup. The result then follows from Proposition 2.4. $\qquad\square$

2.5.2. *Two Computational Lemmas.* The next two results are used in the proof of Proposition 2.6. The following lemma describes the commutator of an element of Γ_{ℓ^m} with an element of Γ_{ℓ^n}.

Lemma 2.9. *Let $n \leq m$ be positive integers, and let $\mathrm{id}_{2g} + \ell^n U$ and $\mathrm{id}_{2g} + \ell^m V$ be elements of $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. Then we have*

$$(\mathrm{id}_{2g} + \ell^n U)^{-1}(\mathrm{id}_{2g} + \ell^m V)(\mathrm{id}_{2g} + \ell^n U)(\mathrm{id}_{2g} + \ell^m V)^{-1} \equiv \mathrm{id}_{2g} + \ell^{n+m}(VU - UV) \pmod{\ell^{2n+m}}.$$

Proof. We have

$$
\begin{aligned}
(\mathrm{id}_{2g} + \ell^m V)(\mathrm{id}_{2g} + \ell^n U)(\mathrm{id}_{2g} + \ell^m V)^{-1} &= \mathrm{id}_{2g} + \ell^n(\mathrm{id}_{2g} + \ell^m V)U(\mathrm{id}_{2g} + \ell^m V)^{-1} \\
&= \mathrm{id}_{2g} + \ell^n(\mathrm{id}_{2g} + \ell^m V)U\left(\sum_{i=0}^{\infty}(-1)^i \ell^{im} V^i\right) \\
&= \mathrm{id}_{2g} + \ell^n \sum_{i=0}^{\infty}\left[(-1)^i \ell^{im} UV^i + (-1)^i \ell^{(i+1)m} VUV^i\right] \\
&= \mathrm{id}_{2g} + \ell^n U + \ell^{n+m}(VU - UV)(\mathrm{id}_{2g} + \ell^m V)^{-1}.
\end{aligned}
$$

Multiplying on the left by $(\mathrm{id}_{2g} + \ell^n U)^{-1}$ gives the desired result. $\qquad\square$

In the next proposition, we show the commutator subalgebra of $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is sufficiently large for all primes ℓ.

Proposition 2.10. *We have the following results:*

(a) *For all $g \geq 1$ and $\ell \geq 3$ we have $[\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}), \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})] = \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.*

(b) *For all $g \geq 1$ we have $[\mathfrak{sp}_{2g}(\mathbb{Z}/4\mathbb{Z}), \mathfrak{sp}_{2g}(\mathbb{Z}/4\mathbb{Z})] \supset 2 \cdot \mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$.*

Proof. Statement (a) follows immediately from [Ste61, Theorem 2.6], which states that $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is simple for $\ell \geq 3$. It remains to prove Statement (b). For this, we compute several commutators and make deductions based on each one. For convenience, let $\mathfrak{g} = [\mathfrak{sp}_{2g}(\mathbb{Z}/4\mathbb{Z}), \mathfrak{sp}_{2g}(\mathbb{Z}/4\mathbb{Z})]$, let A, D denote arbitrary $g \times g$ matrices, and let B, C, E, F denote symmetric $g \times g$ matrices. Since

$$(2.4) \qquad \left[\left[\begin{array}{c|c} A & 0 \\ \hline 0 & -A^T \end{array} \right], \left[\begin{array}{c|c} D & 0 \\ \hline 0 & -D^T \end{array} \right] \right] = \left[\begin{array}{c|c} AD - DA & 0 \\ \hline 0 & A^T D^T - D^T A^T \end{array} \right],$$

all block-diagonal matrices in $\mathfrak{sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$ with every diagonal entry equal to 0 are contained in $\mathfrak{g}$. This can be seen by taking A and D to be various elementary matrices. Furthermore,

$$(2.5) \qquad \left[\left[\begin{array}{c|c} 0 & B \\ \hline C & 0 \end{array} \right], \left[\begin{array}{c|c} 0 & E \\ \hline F & 0 \end{array} \right] \right] = \left[\begin{array}{c|c} BF - EC & 0 \\ \hline 0 & CE - FB \end{array} \right],$$

so we can arrange that $BF - EC$ is an elementary matrix with a single nonzero entry on the diagonal. Summing matrices from (2.4) and (2.5) tells us that all block-diagonal matrices are contained in $\mathfrak{g}$. Additionally,

$$(2.6) \qquad \left[\left[\begin{array}{c|c} \mathrm{id}_g & 0 \\ \hline 0 & -\mathrm{id}_g \end{array} \right], \left[\begin{array}{c|c} 0 & B \\ \hline 0 & 0 \end{array} \right] \right] = \left[\begin{array}{c|c} 0 & 2B \\ \hline 0 & 0 \end{array} \right].$$

Repeating the computation from (2.6) with the other off-diagonal block nonzero implies that 2 times any matrix in $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ whose diagonal blocks are 0 is an element of $\mathfrak{g}$. The desired result follows because $2 \cdot \mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ is contained in the subspace generated by the matrices from (2.4), (2.5), and (2.6). $\square$

2.5.3. *Completing the Proof.* In order to prove Proposition 2.6, we require the following lemma, which states that the closure of the commutator $[\Gamma_{\ell^k}, \Gamma_{\ell^k}]$ is large.

Lemma 2.11. *Fix $k \geq 1$. Then if $\ell \neq 2$, the closure of $[\Gamma_{\ell^k}, \Gamma_{\ell^k}]$ contains $\Gamma_{\ell^{2k}}$ and if $\ell = 2$, the closure of $[\Gamma_{\ell^k}, \Gamma_{\ell^k}]$ contains $\Gamma_{\ell^{2k+1}}$.*

Proof. First suppose $\ell \geq 3$. Statement (1) of Proposition 2.10 implies that for any $W' \in \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, there exist $U', V' \in \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ so that $V'U' - U'V' = W'$. Choosing lifts W, U, V of W', U', V', it follows from Lemma 2.9 that for every i and for every such

$$\mathrm{id}_{2g} + \ell^{2k+i}W \in \Gamma_{\ell^{2k+i}}, \quad \mathrm{id}_{2g} + \ell^k U \in \Gamma_{\ell^k}, \quad \text{and} \quad \mathrm{id}_{2g} + \ell^{k+i}V \in \Gamma_{\ell^{k+i}},$$

we have that

$$(\mathrm{id}_{2g} + \ell^k U)^{-1}(\mathrm{id}_{2g} + \ell^{k+i}V)(\mathrm{id}_{2g} + \ell^k U)(\mathrm{id}_{2g} + \ell^{k+i}V)^{-1} \equiv \mathrm{id}_{2g} + \ell^{2k+i}W \pmod{\ell^{2k+i+1}}.$$

Take $M_0 \in \Gamma_{\ell^{2k}}$. There exists $X_1 \in [\Gamma_{\ell^{2k}}, \Gamma_{\ell^{2k}}]$ and $M_1 \in \Gamma_{\ell^{2k+1}}$ with the property that $M_0 = X_1 M_1$. Proceeding inductively in this manner, we obtain sequences $\{X_i : i = 1, 2, \dots\} \subset [\Gamma_{\ell^k}, \Gamma_{\ell^k}]$ and $\{M_i : i = 0, 1, 2, \dots\}$ with $M_i \in \Gamma_{\ell^{2k+i}}$ such that $M_i = X_{i+1} M_{i+1}$ for each i. Then we have the following equalities of matrices in $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$:

$$M_0 = \lim_{i \to \infty} \left(\prod_{j=1}^{i} X_j \right) M_i = \prod_{j=1}^{\infty} X_j.$$

It follows that $\Gamma_{\ell^{2k}}$ is contained in the closure of $[\Gamma_{\ell^k}, \Gamma_{\ell^k}]$.

Now suppose $\ell = 2$. Observe that for each $k \geq 2$ we have

$$\mathrm{id}_{2g} + 2^k \cdot \mathfrak{sp}_{2g}(\mathbb{Z}/4\mathbb{Z}) = \ker(\mathrm{Sp}_{2g}(\mathbb{Z}/2^{k+2}\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/2^k\mathbb{Z})).$$

It follows from Statement (2) of Proposition 2.10 and Lemma 2.9 that for every choice of $\mathrm{id}_{2g} + 2^{2k+i+1} W \in \Gamma_{2^{2k+i+1}}$ and for each nonnegative integer i, there exist $\mathrm{id}_{2g} + 2^k U \in \Gamma_{2^k}$ and $\mathrm{id}_{2g} + 2^{k+i} V \in \Gamma_{2^{k+i}}$ with the property that

$$(\mathrm{id}_{2g} + 2^k U)^{-1} (\mathrm{id}_{2g} + 2^{k+i} V)(\mathrm{id}_{2g} + 2^k U)(\mathrm{id}_{2g} + 2^{k+i} V)^{-1} \equiv \mathrm{id}_{2g} + 2^{2k+i+1} W \pmod{\ell^{2k+i+2}}.$$

One may now finish the proof by applying a similar inductive argument to the one used in the case $\ell \geq 3$. $\qquad\square$

We are finally in position to prove the main result of this section.

Proof of Proposition 2.6. By Lemma 2.8, it suffices to prove the following two statements:

(a) The closure of $[H, H]$ surjects onto $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for all but finitely many ℓ.
(b) The closure of $[H, H]$ maps onto an open subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for each ℓ.

For Statement (a), notice that H surjects onto $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ for all but finitely many ℓ. Note that for $\ell \geq 3$, we have $[\mathrm{GSp}_{2g}(\mathbb{Z}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)] = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ because, by [LSTX17b, Proposition 1], we have that

$$\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) = [\mathrm{Sp}_{2g}(\mathbb{Z}_\ell), \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)] \subset [\mathrm{GSp}_{2g}(\mathbb{Z}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)] \subset \mathrm{Sp}_{2g}(\mathbb{Z}_\ell).$$

Thus, $[H, H]$ itself surjects onto $[\mathrm{GSp}_{2g}(\mathbb{Z}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)] = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for all $\ell \geq 3$.

To show statement (b), we prove that the closure of $[H', H']$ is open in $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for any open subgroup $H' \subset \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. Since H' is open, there exists some $k \geq 1$ such that $\Gamma_{\ell^k} \subset H'$, so by Lemma 2.11, there exists $m \geq 2k$ such that $\Gamma_{\ell^m} \subset [\Gamma_{\ell^k}, \Gamma_{\ell^k}] \subset [H', H']$. Thus, $[H', H']$ contains an open subgroup and must therefore itself be open, as desired. $\quad\square$

3. Background on Galois Representations of PPAVs

This section is devoted to describing the basic definitions and properties concerning Galois representations associated to families of PPAVs. Specifically, in Section 3.1, we construct these Galois representations and provide precise definitions for the various monodromy groups discussed in Section 1.2. Then, in Section 3.2, we explain how a family of PPAVs over a number field K may be extended to a family over the number ring $\mathcal{O}_K$. The notation introduced in this section will be utilized throughout the rest of the paper.

3.1. **Defining Galois Representations for Families of PPAVs.** Let K be a number field, and let $g \geq 0$ be an integer. Fix a base scheme T (we usually take T to be Spec K or an open subscheme of Spec $\mathcal{O}_K$), and let U be an integral T-scheme with generic point η (we usually take U to be an open subscheme of $\mathbb{P}_K^r$ or $\mathbb{P}_{\mathcal{O}_K}^r$). Let $A \to U$ be a *family* of g-dimensional PPAVs, by which we mean the following:

- The morphism $A \to U$ is flat, proper, and finitely presented with smooth geometrically connected fibers of dimension g.
- A is a group scheme over U, and the resulting abelian scheme is equipped with a principal polarization.

Note that $A \to U$ is automatically abelian, smooth, and projective, and further observe that the fiber A_u over any point $u \in U$ is a PPAV of dimension g over the residue field $\kappa(u)$ of u.

Choose a geometric generic point $\overline{\eta}$ for U. If $\kappa(\eta)$ has characteristic prime to m, the action of the étale fundamental group $\pi_1(U, \overline{\eta})$[3] on the geometric generic fiber $A_{\overline{\eta}}[m]$ gives rise to a continuous linear representation whose image is constrained by the Weil pairing to lie in the general symplectic group $\mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$. We denote this *mod-$m$ representation* by

$$(3.1) \qquad \rho_{A,m} \colon \pi_1(U, \overline{\eta}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}).$$

The map in (3.1) is well-defined up to the choice of base-point $\overline{\eta}$, and choosing a different such $\overline{\eta}$ would only alter the image of $\rho_{A,m}$ by an inner automorphism of $\mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$. For this reason, when it will not lead to confusion, we may omit the basepoint from our notation and write $\pi_1(U)$ for $\pi_1(U, \overline{\eta})$.

If ℓ is a prime not dividing the characteristic of $\kappa(\eta)$, then we can take the inverse limit of the mod-ℓ^k representations to obtain the *ℓ-adic representation*

$$(3.2) \qquad \rho_{A,\ell^\infty} \colon \pi_1(U) \to \varprojlim_k \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}).$$

Moreover, if $\kappa(\eta)$ has characteristic 0, we can take the inverse limit of all the mod-m representations (or equivalently the product of all the ℓ-adic representations) to obtain an *adelic* or *global representation*

$$(3.3) \qquad \rho_A \colon \pi_1(U) \to \varprojlim_m \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}) \simeq \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}).$$

Remark 3.1. In the situation that $U = \mathrm{Spec}\, K$, the choice of $\overline{\eta}$ corresponds to a choice of algebraic closure $\overline{K}$ of K. Taking $G_K := \mathrm{Gal}(\overline{K}/K)$ to be the absolute Galois group, we have that $\pi_1(U, \overline{\eta}) = G_K$. This recovers the notion of a Galois representation of a PPAV over a field as a map $\rho_A : G_K \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$.

Remark 3.2. For a commutative ring R, recall from the definition of the general symplectic group that we have a multiplier map $\mathrm{mult} \colon \mathrm{GSp}_{2g}(R) \to R^\times$. Let χ_m be the mod-m cyclotomic character, and let χ be the cyclotomic character. If $U = \mathrm{Spec}\, k$, (with k an arbitrary characteristic 0 field) it follows from G_k-invariance of the Weil pairing that $\chi_m = \mathrm{mult} \circ \rho_{A,m}$ and $\chi = \mathrm{mult} \circ \rho_A$. More generally, if U is normal and integral, and $\phi : \pi_1(U) \to \pi_1(\mathrm{Spec}\, K)$, then $\chi \circ \phi = \mathrm{mult} \circ \rho_A$, which holds because it holds for the generic fiber $A_\eta \to \mathrm{Spec}\, K(\eta)$, and the map $\pi_1(\eta) \to \pi_1(U)$ is surjective.

---

[3]For a general foundational reference on the étale fundamental group, see [GR71a].

We now define the monodromy groups associated to the representations defined above. We call the image of $\rho_A \colon \pi_1(U) \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ the *monodromy* of the family $A \to U$, and we denote it by H_A. When the base scheme is $T = \mathrm{Spec}\, K$, we also define the *geometric monodromy*, denoted by H_A^{geom}, to be the image of the adelic representation $\rho_{A_{\overline{K}}} \colon \pi_1(U_{\overline{K}}) \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ associated to the base-changed family $A_{\overline{K}} \to U_{\overline{K}}$. Since the cyclotomic character is trivial on $G_{\overline{K}}$, it follows that H_A^{geom} is actually a subgroup of $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$. We write $H_A(m)$ and $H_A^{\mathrm{geom}}(m)$ for the mod-m reductions of the above-defined monodromy groups. We say $A \to U$ has big monodromy if H_A is open in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ and $A \to U$ has big geometric monodromy if H_A^{geom} is open in $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$.

In particular, for each $u \in U$, H_{A_u} and $H_{A_u}^{\mathrm{geom}}$ are the monodromy groups associated to the family $A_u \to \mathrm{Spec}\, \kappa(u)$. Since A_u is the pullback of A along $\iota : u \to U$, $\rho_{A_u} = \iota \circ \rho_A$ and we obtain an inclusion $H_{A_u} \subset H_A$. Note that if U is normal, then the map $\pi_1(\eta) \to \pi_1(U)$ is surjective, so we have that $H_{A_\eta} = H_A$.

3.2. Extending Families over K to $\mathcal{O}_K$.

Recall that, for a single abelian variety A_u over $u = \mathrm{Spec}\, K$, good reduction for A_u at a prime $\mathfrak{p} \in \Sigma_K$ implies that the Galois representation $\rho_{A_u,m} \colon G_K \to \mathrm{GSp}(\mathbb{Z}/m\mathbb{Z})$ is unramified at $\mathfrak{p}$, provided that $\mathfrak{p}$ does not divide m. All but finitely many primes $\mathfrak{p}$ are primes of good reduction for A_u. Similarly, for a family $A \to U$ over $\mathrm{Spec}\, K$, extending the definition of this family "across" a prime $\mathfrak{p} \in \Sigma_K$ reveals constraints on the monodromy of that family and its subfamilies. The purpose of this section is to explain why any family $A \to U$ can be extended across most primes in Σ_K. The constructions introduced here become particularly important in Section 4.6, where we apply the results of [Wal14]. A similar treatment of these constructions can be found in [Wal14, p. 460-462].

Retain the setting of Theorem 1.1. Start with a family $A \to U$ of PPAVs over $\mathrm{Spec}\, K$. Using standard spreading out techniques as in [Gro66a, §8] (see in particular [Gro66a, 8.10.5(xii)], [Gro66a, 9.7.7(ii)], and [Gro67, 17.7.8(ii)]), we can extend the family $A \to U$ to a family $\mathcal{A} \to \mathcal{U}$, where $\mathcal{U}$ is an open subscheme of $\mathbb{P}^r_{\mathcal{O}_K}$, whose generic fiber over $\mathrm{Spec}\, K \to \mathrm{Spec}\, \mathcal{O}_K$ is just $A \to U$. Recall from Section 3.1 that the term "family" means that $\mathcal{A} \to \mathcal{U}$ is smooth and proper with geometrically connected fibers and that $\mathcal{A}$ is an abelian scheme over $\mathcal{U}$ with a principal polarization. This construction is depicted in the following commutative diagram:

$$
\begin{array}{ccccc}
A & \longrightarrow & \mathcal{A} & & \\
\downarrow & & \downarrow & & \\
U & \longrightarrow & \mathcal{U} & \overset{\text{open emb.}}{\hookleftarrow} & \mathbb{P}^r_{\mathcal{O}_K} \\
\downarrow & & \downarrow & & \\
\mathrm{Spec}\, K & \longrightarrow & \mathrm{Spec}\, \mathcal{O}_K & &
\end{array}
$$

Let $Z := \mathbb{P}^r_K \setminus U$ be the locus where the original family is not defined, and let $\mathcal{Z}$ denote the closure of Z in $\mathbb{P}^r_{\mathcal{O}_K}$. Since the bottom square in the diagram above is Cartesian, each irreducible component of $\mathbb{P}^r_{\mathcal{O}_K} \setminus \mathcal{U}$ that is not contained in $\mathcal{Z}$ cannot map generically onto $\mathrm{Spec}\, \mathcal{O}_K$ and must therefore map to a single prime $\mathfrak{p} \in \Sigma_K$. Since there are finitely many irreducible components of $\mathcal{Z}$, the set S of primes $\mathfrak{p} \in \mathrm{Spec}\, \mathcal{O}_K$ for which $\mathbb{P}^r_{\mathbb{F}_\mathfrak{p}} \setminus \mathcal{U}_{\mathbb{F}_\mathfrak{p}} \neq \mathcal{Z}_{\mathbb{F}_\mathfrak{p}}$ is a finite set. The primes in S can be thought of as the "bad primes" for the family: the

smoothness of $\mathcal{A} \to \mathcal{U}$ implies that any abelian variety A_u for $u \in U(K)$ will have good reduction away from the primes in S and the primes lying under the (finite) intersection $\overline{\{u\}} \cap \mathcal{Z} \subset \mathbb{P}^r_{\mathcal{O}_K}$.

3.2.1. *Monodromy groups of subfamilies.* Let $m \in \mathbb{Z}$, let $P_m \subset \Sigma_K$ be the set of primes dividing m, and let Spec $\mathcal{O}_{P_m}$ be the complement of P_m in Spec $\mathcal{O}_K$. Then the base change $\mathcal{U}_{\mathcal{O}_{P_m}}$ of $\mathcal{U}$ from Spec $\mathcal{O}_K$ to Spec $\mathcal{O}_{P_m}$ is the open subset of $\mathcal{U}$ on which $\mathcal{A}[m] \to \mathcal{U}$ is unramified and hence finite étale. Therefore, we obtain a finite étale cover $\mathcal{A}_{\mathcal{O}_{P_m}}[m] \to \mathcal{U}_{\mathcal{O}_{P_m}}$ and hence a map $\rho \colon \pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ just as in 3.1. The original family of interest can be thought of as a subfamily of this one: we have maps $U_{\overline{K}} \to U \to \mathcal{U}_{\mathcal{O}_{P_m}}$, from which we obtain maps

$$\pi_1(U_{\overline{K}}) \longrightarrow \pi_1(U) \longrightarrow \pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \xrightarrow{\ \rho\ } \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}).$$

Lemma 3.1. *The continuous map $\pi_1(U) \to \pi_1(\mathcal{U}_{\mathcal{O}_{P_m}})$ is surjective.*

Proof. This lemma is a consequence of [GR71a, Exposé V, Proposition 8.2]; we nonetheless include a proof because it helps illustrate the constructions introduced in this section. It suffices to show that the composition of this map with any surjective continuous map $\pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \to G$ onto a finite group G is surjective. According to [Sta16, Tag 03SF], a finite quotient of the étale fundamental group corresponds to a connected finite Galois cover, so let $\mathcal{V}_m \to \mathcal{U}_{\mathcal{O}_{P_m}}$ be the cover corresponding to our chosen surjection. By [Sta16, Tag 0DV6], the composed map $\pi_1(U) \to \pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \to G$ gives a $\pi_1(U)$-action on G which corresponds to the pulled back cover $(\mathcal{V}_m)_K \to U$. The latter is connected if and only if the composed map is surjective. Since $\mathcal{V}_m$ is connected and étale over Spec $\mathcal{O}_{P_m}$, it is irreducible, which implies that $(\mathcal{V}_m)_K$ is irreducible (its generic points correspond to those of $\mathcal{V}_m$), hence connected. □

By [Sta16, Tag 0DV6], the resulting monodromy representation $\pi_1(U) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ equals that obtained from the pullback of the finite étale cover $\mathcal{A}_{\mathcal{O}_{P_m}}[m] \to \mathcal{U}_{\mathcal{O}_{P_m}}$ to U. But the pullback is just the family $A[m] \to U$, so this monodromy representation equals $\rho_{A,m}$, and its image equals $H_A(m)$. The lemma therefore implies that the image of the map $\pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ equals $H_A(m)$. Similarly, the map $\pi_1(U_{\overline{K}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ has image equal to $H_A^{\mathrm{geom}}(m)$.

Moreover, for $\mathfrak{p} \in \Sigma_K$ not dividing m, we can also consider the subfamilies $\mathcal{U}_{\overline{\mathbb{F}}_{\mathfrak{p}}} \to \mathcal{U}_{\mathbb{F}_{\mathfrak{p}}} \to \mathcal{U}_{\mathcal{O}_{P_m}}$ obtained by extending scalars along the maps $\mathcal{O}_{P_m} \to \mathbb{F}_{\mathfrak{p}} \to \overline{\mathbb{F}}_{\mathfrak{p}}$ for some algebraic closure $\overline{\mathbb{F}}_{\mathfrak{p}}$ of $\mathbb{F}_{\mathfrak{p}}$. As before, we obtain maps

$$\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_{\mathfrak{p}}}) \longrightarrow \pi_1(\mathcal{U}_{\mathbb{F}_{\mathfrak{p}}}) \longrightarrow \pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \xrightarrow{\ \rho\ } \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}).$$

We denote by $H_{A,\mathfrak{p}}(m)$ and $H_{A,\mathfrak{p}}^{\mathrm{geom}}$ the images of the maps $\pi_1(\mathcal{U}_{\mathbb{F}_{\mathfrak{p}}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ and $\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_{\mathfrak{p}}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$, respectively.

3.2.2. *Notation for Galois étale covers.* As explained in the proof of Lemma 3.1, finite quotients of the étale fundamental group correspond to connected finite Galois étale covers. We now fix notation for the Galois étale covers introduced in the proof of Lemma 3.1 that will be used later in Section 4 to state and verify Wallace's criteria [Wal14].

- Let $\mathcal{V}_m$ be the cover of $\mathcal{U}_{\mathcal{O}_{P_m}}$ corresponding to the map $\pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$.
- Let V_m be the cover of U corresponding to the map $\pi_1(U) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$.

Here, each map from $\pi_1(-)$ to a finite group gives a quotient of $\pi_1(-)$ as its image. By the reasoning of Lemma 3.1, $V_m = (\mathcal{V}_m)_K$.

Remark 3.3. The result of Lemma 3.1 is special to the base change $\mathcal{O}_K \to K$. In general, the other maps of $\pi_1(-)$s will not be surjective, nor will the finite Galois étale covers $(V_m)_{\overline{K}}$, $(\mathcal{V}_m)_{\mathbb{F}_{\mathfrak{p}}}$, and $(\mathcal{V}_m)_{\overline{\mathbb{F}}_{\mathfrak{p}}}$ be connected.

4. Proof of the Theorem 1.1

4.1. **Outline of the Proof.** With the view of making the proof of Theorem 1.1 more readily comprehensible, we now briefly describe the key aspects of the argument. We encourage the reader to refer to Figure 1 for a schematic diagram illustrating the argument.

We begin in Section 4.2 by proving Proposition 4.1, showing that a non-isotrivial family with big monodromy also has big geometric monodromy. Then, in Section 4.3, we introduce some of the notation and standing assumptions employed in the proof. In particular, since our family has big geometric monodromy, by Proposition 4.1, we are able to define the constant C in point (b) of Section 4.3, which will later be needed to apply the results of [Wal14] (see Section 4.6.1).

Then, in Section 4.4, we reduce the problem to checking that for an appropriately chosen integer M' depending on the family, most members of the family have the same mod-M' image as that of the family; and (2) that for all sufficiently large primes ℓ, most members of the family have the same mod-ℓ image as that of the family.

The mod-M' image is dealt with in Section 4.5 using Proposition 4.3, which is the Cohen-Serre version of the Hilbert Irreducibility Theorem. For dealing with the mod-ℓ images, there are two regimes of primes to consider, a medium regime and a high regime, when ℓ is bigger than a suitable power of $\log B$. We handle both of these regimes in Section 4.6 by applying a result of Wallace, [Wal14, Theorem 3.9], for which we must verify the following four conditions: (G), (A1), (A2), and (A3). The rest of Section 4 is devoted to verifying that these conditions hold in our setting.

Conditions (G) and (A1), which are fairly easy to check, are treated in Sections 4.6 and 4.7. Next, condition (A2) is dealt with in Section 4.8 by applying the Grothendieck Specialization Theorem in Proposition 4.10. These first three conditions together essentially yield an effective version of the Hilbert Irreducibility Theorem, which allows us to check primes ℓ in the medium regime. Finally, in Section 4.9, we verify condition (A3), which allows us to dispense with primes in the high regime. The key input to checking this condition is a recent result of Lombardo, stated in Theorem 4.11. In order to apply Lombardo's result to our setting, as is done in Proposition 4.12, we must verify two hypotheses and relate the naïve height we are using to the Faltings height used in Theorem 4.11. The first hypothesis is verified in Lemma 4.13 using [EEHK09, Proposition 5]. The second hypothesis is a somewhat trickier condition, and we verify it in Lemma 4.16 using the large sieve, Theorem 4.14. In order to apply the large sieve, we must bound contributions at each prime, which is done in Proposition 4.19 using a general scheme-theoretic result of Ekedahl [Eke90, Lemma 1.2] together with Proposition 4.17. We conclude the section with a brief appendix concerning the relationship between the naïve height and the Faltings height (see Lemma 4.22).

4.2. **Equivalence of Big Geometric Monodromy and Big Monodromy.** In the course of the proof, it will be useful to know that our given family $A \to U$ not only has big monodromy, but also has big geometric monodromy. In particular, this is crucially needed
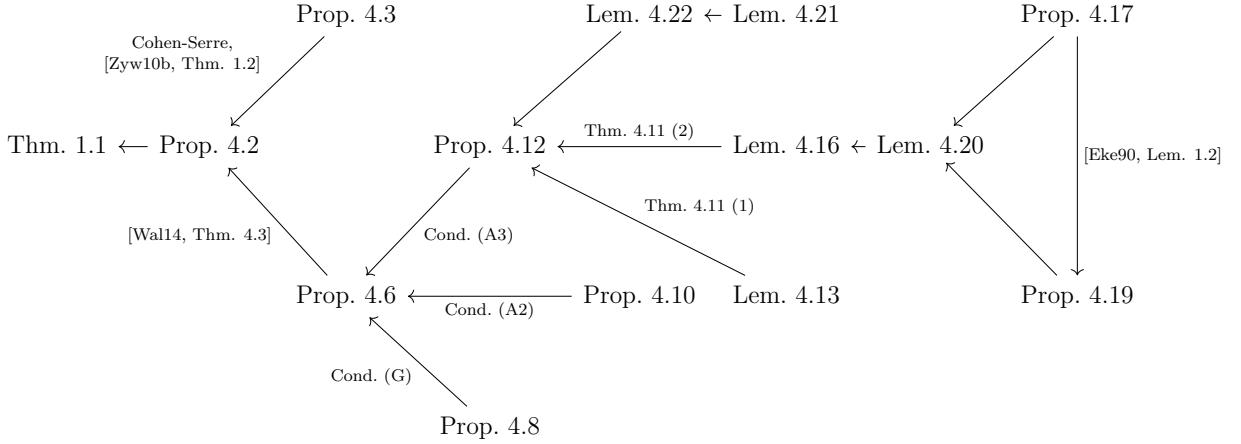
Figure 1. A schematic diagram for the proof of the main theorem, Theorem 1.1.

to define the constant C in point (b) of Section 4.3, which is used in applying the results of [Wal14] (see Section 4.6.1). We now prove the following result, implying that our given family has big geometric monodromy.

Proposition 4.1. *Suppose $A \to U$ is a non-isotrivial family of abelian varieties of relative dimension $g \geq 2$, with U a smooth geometrically connected scheme over a number field K. Then, A has big geometric monodromy if and only if it has big monodromy.*

Proof. We first show the easier direction: if the family $A \to U$ has big geometric monodromy then $A \to U$ also has big monodromy, in the sense that H_A is open in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. To see this, consider the exact sequence

$$0 \longrightarrow \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}) \longrightarrow \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \xrightarrow{\mathrm{mult}} \widehat{\mathbb{Z}}^{\times} \longrightarrow 0.$$

Since $H_A^{\mathrm{geom}} \subset H_A$, the big geometric monodromy assumption tells us that $H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ is open in $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$. It therefore suffices to show that $\mathrm{mult}(H_A)$ is open in $\widehat{\mathbb{Z}}^{\times}$. But $\mathrm{mult}(H_A) = \chi(G_K)$, as mentioned in Remark 3.2, and $\chi(G_K)$ has finite index because $K/\mathbb{Q}$ has finite degree.

It only remains to prove that if the family has big monodromy and is non-isotrivial, it has big geometric monodromy. To show this, from the exact sequence

$$1 \longrightarrow \pi_1(U_{\overline{K}}) \longrightarrow \pi_1(U) \longrightarrow \pi_1(K) \longrightarrow 1$$

$\pi_1(U_{\overline{K}}) \subset \pi_1(U)$ is normal. Therefore, H_A^{geom} is a normal subgroup of H_A, and hence also a normal subgroup of $H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$. Let $\psi : \mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ denote the natural profinite completion map. Since $H_A^{\mathrm{geom}} \subset H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ is normal, it follows that $\psi^{-1}(H_A^{\mathrm{geom}}) \subset \psi^{-1}(H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}))$ is normal. Since H_A has finite index in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$, $\psi^{-1}(H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}))$ has finite index in $\mathrm{Sp}_{2g}(\mathbb{Z})$. Since $g \geq 2$ (so that $\mathrm{Sp}_{2g}(\mathbb{Z})$ has rank at least 2), by the Margulis normal subgroup theorem, (see, for example [Mor01, Theorem 17.1.1],) $\psi^{-1}(H_A^{\mathrm{geom}})$ either has finite index in $\psi^{-1}(H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}))$ or is finite. We will show that in the first case A has big geometric monodromy and in the second case A is isotrivial.

In the case that $\psi^{-1}(H_A^{\mathrm{geom}})$ has finite index in $\psi^{-1}(H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}))$, $\psi^{-1}(H_A^{\mathrm{geom}})$ also has finite index in $\mathrm{Sp}_{2g}(\mathbb{Z})$. Then, since H_A^{geom} is closed, the finite set $\mathrm{Sp}_{2g}(\mathbb{Z})/\psi^{-1}(H_A^{\mathrm{geom}})$ is dense in the profinite space $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})/H_A^{\mathrm{geom}}$. It follows that H_A^{geom} also has finite index in $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, meaning A has big geometric monodromy.

To conclude the proof, it only remains to show that if $\psi^{-1}(H_A^{\mathrm{geom}})$ is finite, then A is isotrivial. In this case, let M_A^{geom} denote the image of the topological monodromy representation $\pi_1^{\mathrm{top}}(U_{\mathbb{C}}) \to \mathrm{Sp}_{2g}(\mathbb{Z})$. By [GR71b, Exposé XIII, Proposition 4.6], we have $\pi_1(U_{\mathbb{C}}) \simeq \pi_1(U_{\overline{K}})$, and therefore the comparison theorem tells us that H_A^{geom} is the profinite completion of M_A^{geom}. This implies $M_A^{\mathrm{geom}} \subset \psi^{-1}(H_A^{\mathrm{geom}})$ and so M_A^{geom} is finite. It follows that H_A^{geom} is finite, being the profinite completion of M_A^{geom}. After a making a finite base change, we may assume H_A^{geom} is trivial. Then, it is a standard fact that A is isotrivial when its monodromy representation is trivial. For example, this follows from [Gro66b]. $\qquad\square$

4.3. Notation and Standing Assumptions. Before proceeding with the proof, we set some notation and assumptions, which will remain in place for the remainder of this section.

(a) As mentioned in Remark 1.1, the case where $g = 1$ is handled in [Zyw10b, Theorem 7.1], so we will restrict our consideration to the case where $g \geq 2$.

(b) Since we are assuming that $A \to U$ has big monodromy, it follows that $A \to U$ has big geometric monodromy, by Proposition 4.1. Define C to be the smallest integer bigger than 2, depending only on U, with the property that for all primes $\ell > C$ we have $H_A^{\mathrm{geom}}(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ and $H_A(\ell) = \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.

(c) Using [Zyw10b, Proposition 6.1] and the explanation given after the statement of [Zyw10b, Theorem 7.1], one readily checks that in Theorem 1.1, the asymptotic statement for K-valued points (i.e., points in $U(K)$) can be deduced immediately from the statement for *lattice points* (i.e., points in $U(K) \cap \mathcal{O}_K^r$). In what follows, we will work with K-valued points or lattice points depending on what is most convenient.

(d) Let $K^{\mathrm{cyc}} \subset \overline{K}$ denote the maximal cyclotomic extension of K, and let $K^{\mathrm{ab}} \subset \overline{K}$ denote the maximal abelian extension of K.

(e) In what follows, for a subgroup H of a topological group G, let $[H, H]$ denote the *closure* of the usual commutator subgroup.

4.4. Main Body of the Proof. We begin by reducing the proof of Theorem 1.1 to proving Proposition 4.2.

Proof of Theorem 1.1 assuming Proposition 4.2. As argued in [Zyw10b, Proof of Theorem 7.1], for any $u \in U(K)$ we have

$$[H_A : H_{A_u}] = [H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}) : \rho_{A_u}(\mathrm{Gal}(\overline{K}/K^{\mathrm{cyc}}))].$$

In the case that $K = \mathbb{Q}$, the Kronecker-Weber Theorem tells us that $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$, so we have

$$[H_A : H_{A_u}] = \delta_{\mathbb{Q}} \cdot [[H_A, H_A] : \rho_{A_u}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}))],$$

where $\delta_{\mathbb{Q}}$ is the index of $[H_A, H_A]$ in $H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$. Then Theorem 1.1 follows immediately from point (c) of Section 4.3 and the following proposition. $\qquad\square$

Proposition 4.2. *Let $B, n > 0$. We have the following asymptotic statements, where the implied constants depend only on U and n:*

(1) For every number field K,

$$\frac{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B, \rho_{A_u}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})) = [H_A, H_A]\}|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|} = 1 + O((\log B)^{-n}).$$

(2) Furthermore, if $K \neq \mathbb{Q}$,

$$\frac{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B, \rho_{A_u}(\mathrm{Gal}(\overline{K}/K^{\mathrm{cyc}})) = H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})\}|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|} = 1 + O((\log B)^{-n}).$$

Remark 4.1. Proposition 4.2 is a generalization of [Zyw10b, Proposition 7.9] from the case $g = 1$ to all dimensions. We shall prove it assuming Proposition 4.3 and Proposition 4.6. The basic idea behind the argument is to reduce the problem of studying the (global) monodromy groups to one of studying the mod-M' and mod-ℓ monodromy groups.

Proof assuming Proposition 4.3 and Proposition 4.6. Assuming point (1), the proof of point (2) is completely analogous to the proof of [Zyw10b, Proposition 7.9(ii)], which consists of two key steps. The first is the fact that $[H_A, H_A]$ is an open normal subgroup of $H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, which follows from Proposition 2.6. The second is [Zyw10b, Proposition 7.7], which is a variant of Hilbert's Irreducibility Theorem and does not depend in any way on the context of elliptic curves (with which [Zyw10b, Section 7] is concerned). It therefore suffices to prove point (1).

Since $\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}}) = [G_K, G_K]$, it follows by the continuity of ρ_{A_u} and the compactness of profinite groups that $\rho_{A_u}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})) = [H_{A_u}, H_{A_u}]$. Thus $\rho_{A_u}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}}))$ is a closed subgroup of $[H_A, H_A]$. Moreover, by Proposition 2.6, $[H_A, H_A]$ is an open subgroup of $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, so we may apply Proposition 2.5 with $G = [H_A, H_A]$ and $H = \rho_{A_u}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}}))$. In so doing, we obtain a positive integer M so that the only closed subgroup of $[H_A, H_A]$ whose mod-M reduction equals $[H_A, H_A](M) = [H_A(M), H_A(M)]$ and whose mod-ℓ reduction equals $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for every prime number $\ell \nmid M$ is $[H_A, H_A]$ itself. The same property is true when M is replaced by any multiple M' of M, and we choose a multiple M' which is divisible by all primes less than C, where C is defined as in point (b) of Section 4.3. The defining property of M' then implies that

$$\frac{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B, \rho_{A_u}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})) \neq [H_A, H_A]\}|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|} \leq$$

(4.1) $$\frac{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B, \rho_{A_u, M'}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})) \neq [H_A(M'), H_A(M')]\}|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|} +$$

(4.2) $$\frac{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B, \rho_{A_u, \ell}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})) \neq \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \text{ for some } \ell \nmid M'\}|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|}.$$

The rest of this section is devoted to finding upper bounds for (4.1) and (4.2). To bound (4.1), notice that we have

$$\rho_{A_u, M'}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})) \neq [H_A(M'), H_A(M')] \implies H_{A_u}(M') \neq H_A(M').$$

It then follows from Proposition 4.3 that (4.1) is bounded by $O((\log B)/B^{[K:\mathbb{Q}]/2})$. To bound (4.2), notice that for $\ell \geq 3$ we have

$$\rho_{A_u, \ell}(\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}})) \neq \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \implies H_{A_u}(\ell) \not\supseteq \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}),$$

because [LSTX17b, Proposition 1(a)] tells us that $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ has trivial abelianization for $\ell \geq 3$. Since $C \geq 3$ by definition, it follows from Proposition 4.6 that (4.2) is $O((\log B)^{-n})$, since $\ell \nmid M'$ implies that $\ell > C$. Combining the above estimates completes the proof of point (1). $\qquad\square$

It now remains to bound the terms (4.1) and (4.2).

4.5. **Bounding the Contribution of** (4.1). The next result is the means by which we bound (4.1); it is an immediate corollary of the Cohen-Serre version of Hilbert's Irreducibility Theorem (see [Zyw10b, Theorem 1.2]) since the set in the numerator of (4.3) is a "thin set."

Proposition 4.3. *For every integer $M' \geq 2$, we have*

$$(4.3) \qquad \frac{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B,\ H_{A_u}(M') \neq H_A(M')\}|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|} \ll \frac{\log B}{B^{[K:\mathbb{Q}]/2}},$$

where the implied constant depends only in U and M'.[4]

4.6. **Bounding the Contribution of** (4.2). To complete the proof of Theorem 1.1, it remains to bound (4.2). We do this in Proposition 4.6, which relies on a strong version of Hilbert's Irreducibility Theorem due to Wallace, namely [Wal14, Theorem 3.9]. Before we can state and apply Wallace's result, we must introduce the various conditions upon which it depends. The setup detailed in [Wal14, Section 3.2] applies in a more general context than the one described below, but we specialize our discussion for the sake of brevity.

4.6.1. *Setup and Statement of* [Wal14, Theorem 3.9]. We start by introducing some notation to help us count points $u \in U(K)$ whose associated monodromy groups H_{A_u} are not maximal. Let $B > 0$, and make the following two definitions:

$$E_\ell(B) := \{u \in U(K) : \mathrm{Ht}(u) \leq B,\ H_A^{\mathrm{geom}}(\ell) \not\subset H_u(\ell)\},\ \text{and}$$
$$E(B) := \bigcup_{\text{prime } \ell > C} E_\ell(B),$$

where C is defined as in point (b) of Section 4.3. The set $E_\ell(B)$ should be thought of as the set of exceptional points of height bounded by B for the ℓ-adic representation, and the set $E(B)$ should likewise be thought of as the set of points of height bounded by B that are exceptional for some $\ell > C$. Note in particular that for any $\ell > C$ we have $H_A(\ell)/H_A^{\mathrm{geom}}(\ell) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$; this condition is important for the proof of [Wal14, Theorem 3.9] to go through, so we impose the following restriction:

$$(4.4) \qquad \textit{For the rest of this section, we will maintain } \ell > C \textit{ as a standing assumption.}$$

For ease of notation, we redefine the set $S \subset \Sigma_K$ of "bad" primes, defined in Section 3.2, by adjoining to it all primes $\ell < C$.

Remark 4.2. Note that our definition of the exceptional set $E(B)$ differs slightly from that given in [Wal14, Theorem 1.1], where it is defined to be the union over *all* primes ℓ of the ℓ-adic exceptional sets $E_\ell(B)$. This difference is inconsequential, as we can always deal with a finite collection of primes using Proposition 4.3. Indeed, this is exactly why we replace M by a multiple M' divisible by all primes $\ell < C$ in the proof of Proposition 4.2.

---

[4]For functions f, g in the variable B, we say that $f(B) \ll g(B)$ if there exists a constant $c > 0$ such that $|f(B)| \leq c \cdot |g(B)|$ for all sufficiently large B.

Now that we have introduced the setup needed for stating [Wal14, Theorem 3.9], we declare the four criteria required for the theorem to be applied. For this, it will now be crucial to recall notation from the geometric setup detailed in Section 3.2.

Conditions 4.4. Recall from Section 3.2 that P_m denotes the set of primes of $\mathcal{O}_K$ dividing an integer m and that V_ℓ denotes the connected Galois étale cover of U giving rise to the monodromy group $H_A(\ell)$ for a prime ℓ. In order to apply [Wal14, Theorem 3.9], we need to verify the following geometric condition on the covers $V_\ell \to U$ as ℓ ranges through the primes greater than C:

(G) Let ζ_ℓ denote a primitive ℓ^{th} root of unity. Each connected component of the base-change $(V_\ell)_{K(\zeta_\ell)}$ is geometrically irreducible.

We also need the following three asymptotic conditions concerning the monodromy groups $H_A(\ell)$, $H_A^{\text{geom}}(\ell)$, and $H_{A,\mathfrak{p}}(\ell)$ for [Wal14, Theorem 3.9] to be applied:

(A1) There exist constants $\beta_1, \beta_2 > 0$ such that

$$|H_A(\ell)| \ll \ell^{\beta_1} \quad \text{and} \quad |\{\text{conjugacy classes of } H_A(\ell)\}| \ll \ell^{\beta_2},$$

where the implied constants depend only on U.

(A2) There exists a constant $\beta_3 > 0$ such that

$$\mathcal{T}_\ell := |\{\text{prime } \mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \in S \cup P_\ell \text{ or } H_{A,\mathfrak{p}}^{\text{geom}}(\ell) \not\simeq H_A^{\text{geom}}(\ell)\}| \ll \ell^{\beta_3},$$

where the implied constant depends only on $A \to U$.

(A3) For each $B > 0$, there exists a subset

$$F(B) \subset \{u \in U(K) : \text{Ht}(u) \leq B\}$$

and constants $c, \gamma > 0$ depending only on $A \to U$ such that

$$\lim_{B \to \infty} \frac{|F(B)|}{|\{u \in U(K) : \text{Ht}(u) \leq B\}|} = 1 \quad \text{and} \quad F(B) \cap E(B) \subset \bigcup_{\ell \leq c(\log B)^\gamma} E_\ell(B).$$

We are now in a position to state Wallace's main result:

Theorem 4.5 ([Wal14, Theorem 3.9]). *Suppose that condition (G) holds and that conditions (A1)–(A3) hold with the values $\beta_1, \beta_2, \beta_3, \gamma$.[5] Then we have the following bound on the proportion of exceptional points of height bounded by B:*
(4.5)
$$\frac{|E(B)|}{|\{u \in U(K) : \text{Ht}(u) \leq B\}|} \ll \frac{|\{u \in U(K) : \text{Ht}(u) \leq B\} \setminus F(B)|}{|\{u \in U(K) : \text{Ht}(u) \leq B\}|} + \frac{(\log B)^{(\beta_1 + \beta_2 + 2)\gamma + 1}}{B^{1/2}},$$
where the implied constant depends only on U.

4.6.2. *Bounding 4.2, Conditional on Verifying (G), (A2), and (A3).* We have not yet determined that Conditions 4.4 hold in our setting. We defer the verification of these conditions to Sections 4.7, 4.8, and 4.9. Nevertheless, assuming that these conditions hold, we obtain the following consequence:

Proposition 4.6. *Let $n > 0$. Then we have*
(4.6)
$$\frac{\left|\left\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B, \, H_{A_u}(\ell) \not\subset \text{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \text{ for some } \ell > C\right\}\right|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|} \ll (\log B)^{-n},$$

---

[5]The constant c from condition (A3) is absorbed into the implied constant in (4.5).

where the implied constant depends only on U and n.

Proof assuming Propositions 4.8, 4.10, and 4.12. Note that condition (A1) holds trivially in our setting, because

$$\max\{|H_A(\ell)|, |\{\text{conjugacy classes of } H_A(\ell)\}|\} \leq |\operatorname{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|,$$

and $|\operatorname{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})| = O(\ell^{\beta})$ for some positive constant β depending only on g because $\operatorname{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \subset \operatorname{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.

Condition (G) holds by Proposition 4.8, and condition (A2) holds by Proposition 4.10. Proposition 4.12 constructs $F(B)$ that not only satisfy condition (A3), but also have the property that

$$\frac{|\{u \in U(K) : \operatorname{Ht}(u) \leq B\} \setminus F(B)|}{|\{u \in U(K) : \operatorname{Ht}(u) \leq B\}|} \ll (\log B)^{-n}$$

for every $n > 0$. Upon applying the argument in point (c) of Section 4.3, which relates the left-hand-sides of (4.5) and (4.6), the proposition follows from Theorem 4.5.   □

The rest of this section is devoted to verifying the conditions necessary for the proof of Proposition 4.6.

4.7. Verifying Condition (G).
In this section, we will consider the base-change of the setting established in 3.2 from K to a finite extension $L \subset \overline{K}$ of K; in this setting, we obtain a family $A_L \to U_L$ and a (not necessarily connected) finite Galois étale cover $(V_\ell)_L \to U_L$. To verify condition (G), we employ the following lemma:

Lemma 4.7. *Let $L \subset \overline{K}$ be a finite extension of K. We have that $H_{A_L}(m) \simeq H_{A_L}^{\operatorname{geom}}(m)$ if and only if all connected components of $(V_m)_L$ are geometrically connected over L.*

Proof. Observe that $(V_m)_L$ and $(V_m)_{\overline{K}}$ are finite Galois étale covers of U_L and $U_{\overline{K}}$, which need not be connected.

Let $W \subset (V_m)_L$ be a connected component, and let $\widetilde{W} \subset (V_m)_{\overline{K}}$ be a connected component mapping to W. By construction, $W \to U_L$ is the connected Galois étale cover corresponding to the surjection $\pi_1(U_L) \twoheadrightarrow H_{A_L}(m)$. Likewise, $\widetilde{W} \to U_{\overline{K}}$ corresponds to $\pi_1(U_{\overline{K}}) \twoheadrightarrow H_A^{\operatorname{geom}}(m) = H_{A_L}^{\operatorname{geom}}(m)$. This implies that:

- The degree d_1 of $W \to U_L$ equals $|H_{A_L}(m)|$.
- The degree d_2 of $\widetilde{W} \to U_{\overline{K}}$ equals $|H_{A_L}^{\operatorname{geom}}(m)|$.

On the other hand, the maps $(V_m)_L \to U_L$ and $(V_m)_{\overline{K}} \to U_{\overline{K}}$ have equal degrees. Therefore $d_1 = d_2$ if and only if all connected components of $(V_m)_L$ are geometrically connected.   □

We are now in position to prove condition (G).

Proposition 4.8. *Condition (G) holds in the setting of Section 3.2.*

Proof. Let $L = K(\zeta_\ell)$, and recall the assumption (4.4). Since $(V_\ell)_L \to U_L$ is étale and U_L is smooth over L, it follows that $(V_\ell)_L$ is smooth over L. Therefore $(V_\ell)_L$ is geometrically irreducible over L if and only if it is geometrically connected over L. Now, by Lemma 4.7, it suffices to show that $H_{A_L}(\ell) = H_A^{\operatorname{geom}}(\ell)$. Since we always have $H_{A_L}(\ell) \supset H_A^{\operatorname{geom}}(\ell)$, it suffices to prove the reverse inclusion $H_{A_L}(\ell) \subset H_A^{\operatorname{geom}}(\ell) = \operatorname{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. Since χ_ℓ is trivial on $G_L = \pi_1(\operatorname{Spec} K(\zeta_\ell))$, it follows from Remark 3.2 that $H_{A_L}(\ell) \subset \operatorname{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.   □

4.8. **Verifying Condition (A2).** Before we carry out the verification of condition (A2) in Proposition 4.10, we need to introduce a modified version of the geometric setup developed in [Zyw10b, Subsection 5.2] and in the proof of [Zyw10b, Theorem 5.3].

4.8.1. *Geometric Setup from* [Zyw10b]. Fix the following notation: for a prime $\mathfrak{p} \subset \mathcal{O}_K$, let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$, let $K_\mathfrak{p}^{\mathrm{un}}$ be the maximal unramified extension of $K_\mathfrak{p}$, let $\mathcal{O}_\mathfrak{p}$ be the ring of integers of $K_\mathfrak{p}$, and let $\mathcal{O}_\mathfrak{p}^{\mathrm{un}}$ be the ring of integers of $K_\mathfrak{p}^{\mathrm{un}}$. For a ring R, define $\mathrm{Gr}_R(1,r)$ to be the Grassmannian of lines in $\mathbb{P}_R^r$ and let $\mathscr{L}_R \subset \mathbb{P}_R^r \times \mathrm{Gr}_R(1,r)$ denote the universal line over $\mathrm{Gr}_R(1,r)$. Let Z and $\mathcal{Z}$ be as defined in Section 3.2.

We now construct a closed subscheme $\mathcal{W}$ of the Grassmannian parameterizing all lines whose intersections with $\mathcal{Z}$ are not étale over the base. Define the projection $p : \mathscr{L}_{\mathcal{O}_K} \cap (\mathcal{Z} \times \mathrm{Gr}_{\mathcal{O}_K}(1,r)) \to \mathrm{Gr}_{\mathcal{O}_K}(1,r)$. Let $\mathcal{X}_1$ be the open subscheme of $\mathscr{L}_{\mathcal{O}_K} \cap (\mathcal{Z} \times \mathrm{Gr}_{\mathcal{O}_K}(1,r))$ on which p is étale with nonempty fibers. Define $\mathcal{W} := p(\mathscr{L}_{\mathcal{O}_K} \cap (\mathcal{Z} \times \mathrm{Gr}_{\mathcal{O}_K}(1,r)) \setminus \mathcal{X}_1)$ with reduced subscheme structure and define $\mathcal{X} := \mathrm{Gr}_{\mathcal{O}_K}(1,r) \setminus \mathcal{W}$. Note that $\mathcal{W}$ is closed because p is proper. Considering $\mathcal{W}$ and $\mathcal{X}$ as schemes over $\mathcal{O}_K$, let W and X denote their fibers over K.

Lemma 4.9. *The scheme $\mathcal{W}$, as defined above, is a proper closed subscheme of $\mathrm{Gr}_{\mathcal{O}_K}(1,r)$.*

Proof. It suffices to show that $\mathcal{X}$ is nonempty. In turn, it suffices to show X is nonempty. Since X is the set of points in $\mathrm{Gr}_K(1,r)$ over which p is étale, by generic flatness, we need only verify that there is an open subscheme of $\mathrm{Gr}_K(1,r)$ on which the fibers of p_K are étale. Since Z is reduced, hence generically smooth, and the fiber of p_K over $[L]$ is identified with $Z \cap L$, a Bertini theorem (specifically [Jou82, Theoreme I.6.10(2)] applied to the smooth locus of Z over K) implies that $Z \cap L$ is indeed étale over $\kappa([L])$ for $[L]$ general in $\mathrm{Gr}_K(1,r)$. $\square$

Remark 4.3. By Lemma 4.9, $\mathcal{W}$ is a proper closed subscheme of $\mathrm{Gr}_{\mathcal{O}_K}(1,r)$. Observe that for any line $[L] \in (\mathrm{Gr}_{\mathcal{O}_K}(1,r) \setminus \mathcal{W})(\mathbb{F}_\mathfrak{p})$, there exists a lift $[\mathcal{L}] \in (\mathrm{Gr}_{\mathcal{O}_K}(1,r) \setminus \mathcal{W})(\mathcal{O}_\mathfrak{p})$. The purpose of the above construction is to ensure that $\mathcal{L} \cap \mathcal{Z}_{\mathcal{O}_\mathfrak{p}}$ is étale over $\mathcal{O}_\mathfrak{p}$, which we use in the proof of Proposition 4.10.

4.8.2. *Applying the Setup to Check (A2).* In the following proposition, we use the Grothendieck Specialization Theorem to verify that condition (A2) holds in our situation:

Proposition 4.10. *For a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ let $\mathbf{N}(\mathfrak{p})$ denote its norm and define S' to be the finite set of primes over which the fiber of $\mathcal{W}$ is empty. Then,*

$$\mathcal{T}_\ell \leq |S' \cup P_\ell| + |\{\text{primes } \mathfrak{p} \subset \mathcal{O}_K : \gcd(\mathbf{N}(\mathfrak{p}), |\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|) \neq 1\}|.$$

In particular, we have that $\mathcal{T}_\ell$ is bounded by a fixed power of ℓ, so condition (A2) holds in the setting of Section 3.2.

Remark 4.4. In fact, it is true that $\mathcal{T}_\ell \ll \log \ell$. Apart from a finite number of primes depending only on the family $A \to U$, we need only throw out those primes whose norms are not coprime to $|\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|$. Since $|\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|$ grows polynomially in ℓ, the number of distinct primes dividing $|\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|$ is at most logarithmic in ℓ.

Proof of Proposition 4.10. Take a prime ideal $\mathfrak{p} \notin S' \cup P_\ell$ so that $\gcd(\mathbf{N}(\mathfrak{p}), |\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|) = 1$. It suffices to show $H_{A,\mathfrak{p}}^{\mathrm{geom}}(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) = H_A^{\mathrm{geom}}(\ell)$.

Choose $[\mathcal{L}] \in (\mathrm{Gr}_{\mathcal{O}_K}(1,r) \setminus \mathcal{W})(\mathcal{O}_{\mathfrak{p}})$, which exists by Remark 4.3. Furthermore, define $\mathcal{D} := \mathcal{L} \cap \mathcal{Z}_{\mathcal{O}_{\mathfrak{p}}}$ and $\mathcal{Y} := \mathcal{L} \setminus \mathcal{D}$. We have the commutative diagram

$$
\begin{array}{ccc}
\mathcal{Y}_{\overline{K}} & \longrightarrow & \mathcal{U}_{\overline{K}} \\
& \searrow & \searrow \\
& \mathcal{Y}_{\mathcal{O}_{\mathfrak{p}}^{\mathrm{un}}} \longrightarrow \mathcal{U}_{\mathcal{O}_{\mathfrak{p}}^{\mathrm{un}}} \longrightarrow \mathcal{U} & \\
& \nearrow & \nearrow \\
\mathcal{Y}_{\overline{\mathbb{F}}_{\mathfrak{p}}} & \longrightarrow & \mathcal{U}_{\overline{\mathbb{F}}_{\mathfrak{p}}}
\end{array}
$$

where all of the horizontal arrows are embeddings. Let $\pi_1^{(p)}$ denote the largest prime to p quotient of the fundamental group. Note that $\rho_{A,\ell}$ factors through $\pi_1^{(p)}(\mathcal{U})$ because we are assuming $\gcd(\mathbf{N}(\mathfrak{p}), |\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})|) = 1$. By applying the prime to $\mathbf{N}(\mathfrak{p})$ étale fundamental group functor to the above diagram, we obtain
(4.7)

$$
\begin{array}{ccccccccc}
\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{K}}) & \xrightarrow{\iota_{\overline{K}}} & & & \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{U}_{\overline{K}}) & & & & \\
\downarrow{\scriptstyle\phi} & {\scriptstyle\alpha_{\overline{K}}}\searrow & & & & {\scriptstyle\beta_{\overline{K}}}\searrow & & & \\
& & \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\mathcal{O}_{\mathfrak{p}}^{\mathrm{un}}}) & \xrightarrow{\iota_{\mathcal{O}_{\mathfrak{p}}^{\mathrm{un}}}} & \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{U}_{\mathcal{O}_{\mathfrak{p}}^{\mathrm{un}}}) & \xrightarrow{\beta_{\mathcal{O}_{\mathfrak{p}}^{\mathrm{un}}}} & \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{U}) & \xrightarrow{\rho_{A,\ell}} & \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \\
& {\scriptstyle\alpha_{\overline{\mathbb{F}}_{\mathfrak{p}}}}\nearrow & & & & & \nearrow & & \\
\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{\mathbb{F}}_{\mathfrak{p}}}) & \xrightarrow{\iota_{\overline{\mathbb{F}}_{\mathfrak{p}}}} & & & \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{U}_{\overline{\mathbb{F}}_{\mathfrak{p}}}) & {\scriptstyle\beta_{\overline{\mathbb{F}}_{\mathfrak{p}}}}\nearrow & & &
\end{array}
$$

By Remark 4.3, $\mathcal{D}$ is étale over $\mathcal{O}_{\mathfrak{p}}$. By the Grothendieck Specialization Theorem, [OV00, Théorème 4.4], there is a map $\phi \colon \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{K}}) \xrightarrow{\sim} \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{K}_{\mathfrak{p}}}) \to \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{\mathbb{F}}_{\mathfrak{p}}})$ which makes the triangle on the left in (4.7) commute and induces an isomorphism on the largest prime-to-$\mathbf{N}(\mathfrak{p})$ quotients of the source and target. Note that $\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{K}}) \xrightarrow{\sim} \pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{K}_{\mathfrak{p}}})$ is an isomorphism by [GR71b, Exposé XIII, Proposition 4.6]. Since the rest of the diagram (4.7) commutes, the entire diagram commutes.

Now, observe that we have

$$(\rho_{A,\ell} \circ \beta_{\overline{K}})(\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{U}_{\overline{K}})) = H_A^{\mathrm{geom}}(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$$

where the last step follows from the assumption 4.4. By [Zyw10b, Lemma 5.2], (since the scheme W used in [Zyw10b, Lemma 5.2] is contained in the scheme W we have constructed above) we have that

$$(\rho_{A,\ell} \circ \beta_{\overline{K}} \circ \iota_{\overline{K}})(\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{K}})) = H_A^{\mathrm{geom}}(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

Since ϕ is an isomorphism, we deduce that

$$
\begin{aligned}
(\rho_{A,\ell} \circ \beta_{\overline{\mathbb{F}}_{\mathfrak{p}}} \circ \iota_{\overline{\mathbb{F}}_{\mathfrak{p}}})(\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{\mathbb{F}}_{\mathfrak{p}}})) &= (\rho_{A,\ell} \circ \beta_{\overline{\mathbb{F}}_{\mathfrak{p}}} \circ \iota_{\overline{\mathbb{F}}_{\mathfrak{p}}} \circ \phi)(\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{K}})) \\
&= (\rho_{A,\ell} \circ \beta_{\overline{K}} \circ \iota_{\overline{K}})(\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{Y}_{\overline{K}})) \\
&= \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).
\end{aligned}
$$

Therefore, $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \subset (\rho_{A,\ell} \circ \beta_{\overline{\mathbb{F}}_{\mathfrak{p}}})(\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{U}_{\overline{\mathbb{F}}_{\mathfrak{p}}})) = H_{A,\mathfrak{p}}^{\mathrm{geom}}(\ell)$. Since $\ell \nmid \mathbf{N}(\mathfrak{p})$, we have that $\overline{\mathbb{F}}_{\mathfrak{p}}$ contains nontrivial ℓ^{th} roots of unity. Thus, the mod-ℓ cyclotomic character is trivial on $\pi_1^{(\mathbf{N}(\mathfrak{p}))}(\mathcal{U}_{\overline{\mathbb{F}}_{\mathfrak{p}}})$, and so $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \supset H_{A,\mathfrak{p}}^{\mathrm{geom}}(\ell)$. Hence, we have that

$$H_{A,\mathfrak{p}}^{\mathrm{geom}}(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) = H_A^{\mathrm{geom}}(\ell). \qquad \square$$

4.9. **Verifying Condition (A3).** It remains to check that condition (A3) is satisfied in our setting. As usual, before carrying out the argument, we must fix some notation. Let Σ_K denote the set of nonzero prime ideals of $\mathcal{O}_K$, and for a prime $\mathfrak{p} \in \Sigma_K$ of good reduction, let $\mathrm{Frob}_{\mathfrak{p}} \in G_K$ denote a corresponding Frobenius element.

Given a PPAV A/K, let $\mathrm{ch}_A(\mathrm{Frob}_{\mathfrak{p}})$ denote the characteristic polynomial of $\rho_A(\mathrm{Frob}_{\mathfrak{p}}) \in \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$, and observe that $\mathrm{ch}_A(\mathrm{Frob}_{\mathfrak{p}})$ has coefficients in $\mathbb{Z}$. Finally, let $h(A)$ denote the absolute logarithmic Faltings height of A, obtained by passing to any field extension over which A has semi-stable reduction.

4.9.1. *Applying Lombardo's Result.* The key input for our proof of this condition is the following theorem of Lombardo, which is an effective version of the Open Image Theorem:

Theorem 4.11 ([Lom15, Theorem 1.2] and Proposition A.2 in Appendix A). *Let A/K be a PPAV of dimension $g \geq 2$. Suppose that we have the following two conditions:*

(1) $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$.
(2) There exists a prime $\mathfrak{p} \in \Sigma_K$ at which A has good reduction and such that the splitting field of $\mathrm{ch}_A(\mathrm{Frob}_{\mathfrak{p}})$ has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$.

Then there are constants $c_1, c_2 > 0$ and γ_1, γ_2, depending only on g and K, for which the following statement is true: For every prime ℓ unramified in K and strictly larger than

$$\max\{c_1(\mathbf{N}(\mathfrak{p}))^{\gamma_1}, c_2(h(A))^{\gamma_2}\},$$

the ℓ-adic Galois representation surjects onto $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.

Remark 4.5. The group structure of $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ is defined by how S_g acts on $(\mathbb{Z}/2\mathbb{Z})^g$, namely by permuting the g factors. This group appears because it is the largest possible Galois group of a reciprocal polynomial, by which we mean a polynomial $P(T)$ satisfying $P(T) = P(1/T) \cdot T^{\deg P}$.

Now, the proof of condition (A3) will follow from Theorem 4.11 once we know that the two hypotheses of Theorem 4.11 hold for a density-1 subset of the K-valued points of the family. We shall first check condition (A3) under the assumption that these hypotheses hold most of the time. To this end, it will be convenient to introduce notation to help us count the points that fail to satisfy one of the hypotheses in Theorem 4.11. For a given family $A \to U$, define the following two sets:

$D_1(B) := \{u \in U(K) : \mathrm{Ht}(u) \leq B, \ A_u \text{ fails hypothesis (1)}\}$, and

$D_2(B) := \{u \in U(K) : \mathrm{Ht}(u) \leq B, \ A_u \text{ fails hypothesis (2) for all } \mathfrak{p} \text{ with } \mathbf{N}(\mathfrak{p}) \leq (\log B)^{n+1}\}$.

In the next proposition, we verify condition (A3), conditional upon the assumptions that sets $D_1(B)$ and $D_2(B)$ are sufficiently small (these assumptions are proven in Lemma 4.13 and Lemma 4.16 respectively):

Proposition 4.12. *Let $n > 0$. There are constants c, γ depending only on U such that the following holds: if we define*

$$F(B) := \{u \in U(K) : \mathrm{Ht}(u) \le B, \, H_{A_u}(\ell) \supset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \text{ for all } \ell > c(\log B)^\gamma\},$$

then we have

$$(4.8) \qquad \frac{|F(B)|}{|\{u \in U(K) : \mathrm{Ht}(u) \le B\}|} = 1 + O\left((\log B)^{-n}\right),$$

where the implied constant depends only on U and n.

Proof assuming Lemma 4.13, Lemma 4.16, and Lemma 4.22. Let c_1, c_2 and γ_1, γ_2 be as in Theorem 4.11. There exist constants c_2', γ_2', chosen appropriately in terms of the constants c_0, d_0 provided by Lemma 4.22, such that the following holds: for $u \in U(K)$ with $\mathrm{Ht}(u) > B_0$, where B_0 is a positive constant depending only on U, we have that

$$c_2(h(A_u))^{\gamma_2} \le c_2'(\log \mathrm{Ht}(u))^{\gamma_2'}.$$

The requirement that $\mathrm{Ht}(u)$ be sufficiently large is insignificant because

$$(4.9) \qquad \frac{|\{u \in U(K) : \mathrm{Ht}(u) \le B_0\}|}{|\{u \in U(K) : \mathrm{Ht}(u) \le B\}|} \ll \frac{1}{B^{[K:\mathbb{Q}](r+1)}},$$

and the right-hand-side of (4.9) is dominated by the right-hand-side of (4.8). If we take

$$c = \max(c_1, c_2') \quad \text{and} \quad \gamma = \max((n+1)\gamma_1, \gamma_2'),$$

Theorem 4.11 tells us that

$$\{u \in U(K) : \mathrm{Ht}(u) \le B\} \setminus F(B) \subset D_1(B) \cup D_2(B).$$

The desired result follows from Lemmas 4.13 and 4.16, from which we deduce that

$$\frac{|D_1(B) \cup D_2(B)|}{|\{u \in U(K) : \mathrm{Ht}(u) \le B\}|} \ll (\log B)^{-n}. \qquad \square$$

In what follows, we prove the results upon which the above proof of Proposition 4.12 depends. To begin with, we check that hypotheses (1) and (2) from Theorem 4.11 hold in our setting by bounding D_1 in Lemma 4.13 (thus verifying hypothesis (1)) and bounding D_2 in Lemma 4.16 (thus verifying hypothesis (2)).

4.9.2. *Verifying Hypothesis* (1). We check that hypothesis (1) holds in our setting via the following lemma:

Lemma 4.13. *We have that*

$$(4.10) \qquad \frac{|D_1(B)|}{|\{u \in U(K) : \mathrm{Ht}(u) \le B\}|} \ll \frac{\log B}{B^{[K:\mathbb{Q}]/2}},$$

where the implied constant depends only on U.

Proof. Choose $\ell > \max\{C, \ell_1(g)\}$, where C is defined in (4.4) and $\ell_1(g)$ is the constant, depending only on the dimension g, given in [EEHK09, Proposition 4]. By [EEHK09, Proposition 4], we have that $|D_1(B)|$ is bounded above by $\left|\{u \in U(K) : H_{A_u}(\ell) \supset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})\}\right|$. The lemma then follows from Proposition 4.3, where we are using point (c) of Section 4.3 to pass from lattice points to K-valued points. $\qquad \square$

4.9.3. *Verifying Hypothesis* (2). We complete the verification of hypothesis (2) in Lemma 4.16 by means of an argument involving the large sieve, which lets one bound a set in terms of its reduction modulo primes. The large sieve is stated as follows:

Theorem 4.14 (Large Sieve, [Zyw10a, Theorem 4.1]). *Let $\|-\|$ be a norm on $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_K^r$, and fix a subset $Y \subset \mathcal{O}_K^r$. Let $B \geq 1$ and $Q > 0$ be real numbers, and for every prime $\mathfrak{p} \in \Sigma_K$, let $0 \leq \omega_{\mathfrak{p}} < 1$ be a real number. Suppose that we have the following two conditions:*

(a) The image of Y in $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_K^r$ is contained in a ball of radius B.

(b) For every $\mathfrak{p} \in \Sigma_K$ with $\mathbf{N}(\mathfrak{p}) < Q$, we have $|Y_{\mathfrak{p}}| \leq (1 - \omega_{\mathfrak{p}}) \cdot \mathbf{N}(\mathfrak{p})^r$, where $Y_{\mathfrak{p}}$ is the image of Y under reduction modulo $\mathfrak{p}$.

Then we have that

$$|Y| \ll \frac{B^{[K:\mathbb{Q}]r} + Q^{2r}}{L(Q)}, \quad where \quad L(Q) := \sum_{\substack{\mathfrak{a} \subset \mathcal{O}_K \text{ squarefree} \\ \mathbf{N}(\mathfrak{a}) \leq Q}} \prod_{\text{prime } \mathfrak{p} | \mathfrak{a}} \frac{\omega_{\mathfrak{p}}}{1 - \omega_{\mathfrak{p}}},$$

and the implied constant depends only on K, r, and $\|-\|$.

We must now specialize the abstract setup in Theorem 4.14 to our setting. To do so, we define the various objects at play in the large sieve as follows:

Definition 4.15. Introduce the following notation:

- Let $\|-\|$ be the norm defined in Section 1.2.
- Let $B \geq 1$, take $Q := (\log B)^{n+1}$.
- Let m be the positive integer produced by Proposition 4.17, let ζ_m denote a primitive m^{th} root of unity, and let $\Sigma_K^m \subset \Sigma_K$ be the set of $\mathfrak{p} \in \Sigma_K$ which split completely in $K(\zeta_m)$. Now, with σ, τ as in Lemma 4.20, we may take $\omega_{\mathfrak{p}} = \sigma$ for all $\mathfrak{p} \in \Sigma_K^m$ with $\mathbf{N}(\mathfrak{p}) > \tau$ and $\omega_{\mathfrak{p}} = 0$ for all other $\mathfrak{p} \in \Sigma_K$.
- We take Y to be the following set:

$$Y := \{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B, \ A_u \text{ fails hypothesis (2) for all } \mathfrak{p} \text{ with } \mathbf{N}(\mathfrak{p}) \leq (\log B)^{n+1}\}.$$

As above, $Y_{\mathfrak{p}}$ denotes the mod-$\mathfrak{p}$ reduction of Y.

- Define $T_{\mathfrak{p}}$ by

$$T_{\mathfrak{p}} := \{x \in \mathcal{U}_{\mathbb{F}_{\mathfrak{p}}} : \text{splitting field of } \text{ch}_A(\text{Frob}_{\mathfrak{p}}) \text{ has Galois group } (\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g\}.$$

The motivation for defining $T_{\mathfrak{p}}$ is that its complement contains $Y_{\mathfrak{p}}$.

To ensure that the choices made in Definition 4.15 are suitable, we must prove Proposition 4.17 and Lemma 4.20, which when taken together assert that there exist a positive integer m and $\sigma, \tau > 0$ so that $|Y_{\mathfrak{p}}| \leq (1 - \sigma) \cdot \mathbf{N}(\mathfrak{p})^r$ for all $\mathfrak{p} \in \Sigma_K^m$. However, the proof of this result is rather laborious, and stating it now would serve to distract the reader from the primary thrust of the argument. We therefore defer the proof of Lemma 4.20 to Section 4.9.4, and conditional upon this, we now use the large sieve to check that hypothesis (2) holds in our setting.

Proposition 4.16. *For $n > 0$, we have that*

$$\frac{|D_2(B)|}{|\{u \in U(K) : \text{Ht}(u) \leq B\}|} \ll (\log B)^{-n}.$$

Proof assuming Proposition 4.17 and Lemma 4.20. Theorem 4.14 yields the estimate

$$|Y| \ll \frac{B^{[K:\mathbb{Q}]r} + (\log B)^{2n(n+1)}}{L((\log B)^{n+1})},$$

whose denominator is bounded below by

$$L((\log B)^n) > \sum_{\substack{\mathfrak{p} \in \Sigma_K^m \\ \tau < \mathbf{N}(\mathfrak{p}) < (\log B)^{n+1}}} \frac{\sigma}{1 - \sigma}$$

$$> \sigma \cdot |\{\mathfrak{p} \in \Sigma_K^m : \tau < \mathbf{N}(\mathfrak{p}) \le (\log B)^{n+1}\}|.$$

Applying the Chebotarev Density Theorem yields that

$$|\{\mathfrak{p} \in \Sigma_K^m : \tau < \mathbf{N}(\mathfrak{p}) \le (\log B)^{n+1}\}| \gg |\{\mathfrak{p} \in \Sigma_K : \tau < \mathbf{N}(\mathfrak{p}) \le (\log B)^{n+1}\}|.$$

Applying the Prime Number Theorem yields that

$$|\{\mathfrak{p} \in \Sigma_K : \tau < \mathbf{N}(\mathfrak{p}) \le (\log B)^{n+1}\}| \gg \frac{(\log B)^{n+1}}{\log((\log B)^{n+1})}.$$

Combining the above estimates, we deduce that

$$\frac{|Y|}{|\{u \in U(K) \cap \mathcal{O}_K^r : ||u|| \le B\}|} \ll \frac{B^{[K:\mathbb{Q}]r} + (\log B)^{2n(n+1)}}{\frac{(\log B)^{n+1}}{\log((\log B)^{n+1})}} \cdot \frac{1}{B^{[K:\mathbb{Q}]r}}$$

$$\ll \frac{\log((\log B)^{n+1})}{(\log B)^{n+1}} \ll (\log B)^{-n}.$$

Finally, employing point (c) of Section 4.3 to translate the above estimate from lattice points to K-valued points yields the desired result. $\qquad\square$

4.9.4. *Validating the Sieve Setup.* This section is devoted to proving Proposition 4.17 and Lemma 4.20, which together verify that the sieve setup introduced in Definition 4.15 satisfies the necessary conditions for applying the large sieve as we did in the proof of Proposition 4.16. We start by constructing the value of m that we use in our application of the large sieve:

Proposition 4.17. *There is a positive integer m and a subset $\mathcal{C} \subset \mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ invariant under conjugation in $\mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$, and hence in $\mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$, such that the following holds:*

(a) *We have $H_A(m) = \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ and $H_A^{\mathrm{geom}}(m) = \mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$.*
(b) *For any $\mathfrak{p} \notin S$ and any closed point $x \in \mathcal{U}_{\mathbb{F}_\mathfrak{p}}$, if $\rho_{A,m}(\mathrm{Frob}_x) \in \mathcal{C}$, then the splitting field of $\mathrm{ch}(\mathrm{Frob}_x)$ has Galois group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$.[6]*

Note that it is easy to construct many m satisfying (a) by the big monodromy hypothesis. The main point of this proposition is to show there is an m which also satisfies (b).

Proof. We construct the desired m as a product of four appropriate primes, depending on the family $A \to U$. By, for example, Hilbert irreducibility, (or more precisely [Ser97, §9.2, Proposition 1] in conjunction with [Ser97, §13.1, Theorem 3] applied to the extension $\mathbb{Q}(x_1, \ldots, x_g)[T]/(T^{2g} + \sum_{i=1}^{g-1}(-1)^i x_i(T^{2g-i} + T^i) + (-1)^g x_g T^g + 1)$ over $\mathbb{Q}(x_1, \ldots, x_g)$,) there exists a degree-$2g$ polynomial $P(T) \in \mathbb{Z}[T]$ satisfying $P(T) = P(1/T) \cdot T^{\deg P}$ with Galois

---

[6]For the definition of S, see the sentence immediately preceding Remark 4.2.

group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. It is easy to exhibit elements of $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ whose left-action on $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ is described by one of the following four cycle types:

$$
\begin{aligned}
& 2 + 1 + \cdots + 1, \\
& 4 + 1 + \cdots + 1, \\
& (2g - 2) + 1 + 1, \\
& 2g.
\end{aligned}
$$

(4.11)

We choose these cycle types because any subgroup of $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ containing an element with each of these cycle types is in fact all of $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ by [Kow06, Lemma 7.1]. For each such partition, the Chebotarev Density Theorem tells us that there are infinitely many primes ℓ such that $P(T)$ (mod ℓ) splits according to the chosen partition. For $\ell > C$ we have $\rho_{A,\ell}(\pi_1(U)) = \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ and $\rho_{A,\ell}(\pi_1(U_{\overline{K}})) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. So, for $i \in \{1, 2, 3, 4\}$ we can find $\ell_i > C$ so that $P(T)$ (mod ℓ_i) splits according to the ith partition above. By the Chinese remainder theorem, (a) holds.

To complete the proof, we construct $\mathcal{C}$ and verify (b). Since characteristic polynomials are conjugacy-invariant, the set

$$
\mathcal{C} := \{M' \in \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}) : \mathrm{ch}(M') \ (\mathrm{mod}\ \ell_i) \text{ splits as in (4.11) for all } i \in \{1, 2, 3, 4\}\}
$$

is a union of conjugacy classes of $\mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$. By [Riv08, Theorem A.1] there exists an $M \in \mathrm{Sp}_{2g}(\mathbb{Z})$ such that $\mathrm{ch}(M)(T) = P(T)$, which shows that $\mathcal{C}$ is nonempty. For this choice of $\mathcal{C}$, conclusion (2) follows from [Kow06, Lemma 7.1], which says that any subgroup of $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ that contains elements realizing all four cycle types in (4.11) must actually equal all of $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$. $\qquad\square$

The reason why we constructed m in Proposition 4.17 in the way that we did is that it allows us to apply the following theorem, which is a crucial tool for bounding the set of Frobenius elements with certain Galois groups modulo each prime.

Theorem 4.18 ([Eke90, Lemma 1.2]). *Let X be a scheme, and let $\pi \colon X \to \mathrm{Spec}\ \mathcal{O}_K$ be a morphism of finite type. Let $\phi \colon Y \to X$ be a connected finite Galois étale cover with Galois group G, and let $\rho \colon \pi_1(X) \to G$ denote the corresponding finite quotient. Suppose that $\pi \circ \phi$ has a geometrically irreducible generic fiber, and let $\mathcal{C}$ be a conjugacy-invariant subset of G. For every $\mathfrak{p} \in \Sigma_K$, we have*

$$
\frac{|\{x \in X(\mathbb{F}_{\mathfrak{p}}) : \rho(\mathrm{Frob}_x) \in \mathcal{C}\}|}{|X(\mathbb{F}_{\mathfrak{p}})|} = \frac{|\mathcal{C}|}{|G|} + O((\mathbf{N}(\mathfrak{p}))^{-1/2}),
$$

with implicit constants depending only on the family $Y \to X$. By Frob_x we mean the Frobenius element in $\pi_1(X)$ corresponding to $x \in X$.

We now apply Theorem 4.18 to the conjugacy-invariant set $\mathcal{C}$ from Proposition 4.17 in order to obtain a lower bound on $|T_{\mathfrak{p}}|$, the number of points $u \in U(K)$ with the splitting field of $\mathrm{ch}_{A_u}(\mathrm{Frob}_{\mathfrak{p}})$ having Galois group equal to $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$.

Proposition 4.19. *As $\mathfrak{p}$ ranges through the elements of Σ_K^m, where m is defined as in Proposition 4.17, we have that $|T_{\mathfrak{p}}| \gg (\mathbf{N}(\mathfrak{p}))^r$.*

Proof. Let $L := K(\zeta_m)$. As in Section 3.2, let $\mathcal{V}_m \to \mathcal{U}_{\mathcal{O}_{P_m}}$ be the connected Galois étale cover associated to the mod-m Galois representation $\rho \colon \pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$, and let

$\mathcal{X}$ be one of the connected components of $(\mathcal{V}_m)_L$. The map $\mathcal{X} \to (\mathcal{U}_{\mathcal{O}_{P_m}})_L$ is the connected Galois étale cover associated to the map

$$\rho' \colon \pi_1((\mathcal{U}_{\mathcal{O}_{P_m}})_L) \longrightarrow \pi_1(\mathcal{U}_{\mathcal{O}_{P_m}}) \xrightarrow{\ \rho\ } \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z});$$

note that the image of this composite map equals $\rho(\pi_1(\mathcal{U}_{\mathcal{O}_{P_m}})) \cap \mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ by Remark 3.2, since χ_m is trivial on $K(\zeta_m)$. By Proposition 4.17(a), we have $\rho(\pi_1(\mathcal{U}_{\mathcal{O}_{P_m}})) = \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$, so we conclude that $\rho'(\pi_1((\mathcal{U}_{\mathcal{O}_{P_m}})_L)) = \mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$.

We seek to apply Theorem 4.18 with

$$\mathcal{X} \to (\mathcal{U}_{\mathcal{O}_{P_m}})_L \to \mathrm{Spec}\ \mathcal{O}_L \quad \text{in place of} \quad Y \to X \to \mathrm{Spec}\ \mathcal{O}_K.$$

To do so, we must check that this composition has geometrically irreducible generic fiber, which follows from the second part of Proposition 4.17(a) in conjunction with Lemma 4.7.

Now let $\mathcal{C} \subset \mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ be as in Proposition 4.17(b). For any $\mathfrak{p} \in \Sigma_K^m \setminus S$ and $\mathfrak{p}' \in \Sigma_L$ lying over $\mathfrak{p}$, we have $(\mathcal{U}_L)_{\mathbb{F}_{\mathfrak{p}'}} \simeq \mathcal{U}_{\mathbb{F}_{\mathfrak{p}}}$, and so there is a bijection between

$$\{x \in \mathcal{U}_L(\mathbb{F}_{\mathfrak{p}'}) : \rho'(\mathrm{Frob}_x) \in \mathcal{C}\} \quad \text{and} \quad \{x \in \mathcal{U}(\mathbb{F}_{\mathfrak{p}}) : \rho(\mathrm{Frob}_x) \in \mathcal{C}\}.$$

By Proposition 4.17(b), $T_{\mathfrak{p}}$ contains the latter set, so we have

$$|T_{\mathfrak{p}}| \geq |\{x \in \mathcal{U}(\mathbb{F}_{\mathfrak{p}'}) : \rho(\mathrm{Frob}_x) \in \mathcal{C}\}| = |\{x \in \mathcal{U}_L(\mathbb{F}_{\mathfrak{p}'}) : \rho'(\mathrm{Frob}_x) \in \mathcal{C}\}|$$
$$= \left(\frac{|\mathcal{C}|}{|G|} + O((\mathbf{N}(\mathfrak{p}'))^{-1/2}) \right) \cdot |\mathcal{U}_L(\mathbb{F}_{\mathfrak{p}'})|,$$

where the last step above follows from Theorem 4.18. Now, we have the estimate

$$|\mathcal{U}_L(\mathbb{F}_{\mathfrak{p}'})| \gg (\mathbf{N}(\mathfrak{p}'))^r,$$

because the complement of $(\mathcal{U}_L)_{\mathbb{F}_{\mathfrak{p}'}}$ in $(\mathbb{P}_{\mathcal{O}_L}^r)_{\mathbb{F}_{\mathfrak{p}'}}$ has codimension at least 1, since $\mathfrak{p} \notin S$. Combining our results, and using that S is a finite set, we find that

$$|T_{\mathfrak{p}}| \geq \left(\frac{|\mathcal{C}|}{|G|} + O\left(\mathbf{N}(\mathfrak{p}')^{-1/2} \right) \right) \cdot |\mathcal{U}_L(\mathbb{F}_{\mathfrak{p}'})| \gg \mathbf{N}(\mathfrak{p}')^r = \mathbf{N}(\mathfrak{p})^r. \qquad \square$$

The following lemma completes our verification of the sieve setup by constructing the necessary constants σ, τ.

Lemma 4.20. *There are constants $\sigma, \tau > 0$ so that for all $\mathfrak{p} \in \Sigma_K^m$ with $\mathbf{N}(\mathfrak{p}) > \tau$, we have $|Y_{\mathfrak{p}}| \leq (1 - \sigma) \cdot \mathbf{N}(\mathfrak{p})^r$.*

Proof. By Proposition 4.19, there are constants $\sigma', \tau' > 0$ so that, for all $\mathfrak{p} \in \Sigma_K^m$ with $\mathbf{N}(\mathfrak{p}) > \tau'$, we have $|T_{\mathfrak{p}}| \geq \sigma' \cdot (\mathbf{N}(\mathfrak{p}))^r$. For such $\mathfrak{p}$, we have that

$$|Y_{\mathfrak{p}}| \leq (1 - \sigma') \cdot (\mathbf{N}(\mathfrak{p}))^r + O((\mathbf{N}(\mathfrak{p}))^{r-1}),$$

where the error term is on order of $\mathbf{N}(\mathfrak{p})$ smaller than the main term because $\mathcal{Z}$ has codimension at least 1 in $\mathbb{P}_{\mathcal{O}_K}^r$. By replacing σ' with a slightly smaller σ and τ' with a slightly larger τ, we may write

$$|Y_{\mathfrak{p}}| \leq (1 - \sigma) \cdot (\mathbf{N}(\mathfrak{p}))^r. \qquad \square$$

4.9.5. *Discussion of Heights.* In this section, we prove a result that describes the relationship between the absolute multiplicative height on projective space and the absolute logarithmic Faltings height. Let Ht be the height on $\mathbb{P}_K^r$ as defined in 1.2, and let h be the Faltings height. Let $\log$ Ht be the absolute logarithmic height on $\mathbb{P}^r(\overline{K})$, and note that $\log$ Ht naturally restricts to a logarithmic height function defined on the open subscheme $U \subset \mathbb{P}_K^r$.

Let $\mathscr{A}_g$ be the moduli stack of g-dimensional PPAVs, and let $p \colon \mathscr{U}_g \to \mathscr{A}_g$ be the universal family of abelian varieties. Let $\pi \colon \mathscr{A}_g \to A_g$ be its coarse moduli space, and let $j(A) \in A_g(K)$ be the closed point represented by A. As in [Fal86, Section 2], we choose $n \in \mathbb{N}$ such that the line bundle $\mathscr{L} = ((\pi \circ p)_* \omega_{\mathscr{U}_g/\mathscr{A}_g})^{\otimes n}$ is very ample, where $\omega_{\mathscr{U}_g/\mathscr{A}_g}$ is the canonical sheaf of $p \colon \mathscr{U}_g \to \mathscr{A}_g$. Fix an embedding $i \colon A_g \hookrightarrow \mathbb{P}^N$ with $i^* \mathscr{O}_{\mathbb{P}^N}(1) \simeq \mathscr{L}$. The modular height $\log$ Ht$(j(A))$ of A is then the restriction along i of the absolute logarithmic height (i.e., the absolute logarithmic height of $j(A)$ considered as a point of $\mathbb{P}^N(K)$). On the other hand, $\mathscr{O}_{\mathbb{P}^N}(1)$ is a metrized line bundle and restricts to give a metric on $\mathscr{L}$ [FWG+92, p. 36]; we denote by $\log$ Ht$_{\mathscr{L}}$ the corresponding height function on A_g.

We now relate the height on projective space and the Faltings height by piecing together results from the literature on heights:

Lemma 4.21. *Let g be a positive integer, K a number field, and let $n \in \mathbb{N}$ be as in the definition of the modular height. Then there exist constants α and β such that for every principally polarized abelian variety A over K, we have*

$$|n \cdot h(A) - \log \mathrm{Ht}(j(A))| \leq \alpha \cdot \log \max\{1, \log \mathrm{Ht}(j(A))\} + \beta.$$

Proof. By [Fal86, Proof of Lemma 3], there exist constants α_1 and β_1 such that for all abelian varieties A/K, we have

$$|n \cdot h(A) - \log \mathrm{Ht}_{\mathscr{L}}(j(A))| \leq \alpha_1 \cdot \log(\log \mathrm{Ht}_{\mathscr{L}}(j(A))) + \beta_1.$$

By [HS00, B.3.2(b)], there is a constant β_2 such that

$$|\log \mathrm{Ht}_{\mathscr{L}}(j(A)) - \log \mathrm{Ht}(j(A))| \leq \beta_2. \qquad \square$$

Lemma 4.22. *There exist constants c_0 and d_0 depending only on $A \to U$ such that*

$$h(A_u) \leq c_0 \log \mathrm{Ht}(u) + d_0$$

for all $u \in U(K)$.

Proof. By [Ser97, p. 19, Section 2.6, Theorem], $\mathrm{Ht}(j(A_u)) \ll \mathrm{Ht}(u)$ and $\mathrm{Ht}(u) \ll \mathrm{Ht}(j(A_u))$ for all $u \in U$. The result then follows from Lemma 4.21. $\qquad \square$

5. Applications of Theorem 1.1

The purpose of this section is to demonstrate that the main result, Theorem 1.1, can be applied to a number of interesting families of PPAVs, such as families containing a dense open substack of the locus of Jacobians of hyperelliptic curves, trigonal curves, or plane curves. In Section 5.1, we prove a general tool that is needed to guarantee big monodromy for the loci in our applications, and in Section 5.2, we examine each of these applications in detail.

5.1. **Finite-Index Criterion.** In this section we prove Proposition 5.2, which will be applied in the setting of Theorem 1.1 to determine that U has big monodromy when its image in the moduli stack of abelian varieties has big monodromy. We begin by recalling an elementary criterion giving surjectivity for the map on étale fundamental groups induced by a morphism of Deligne-Mumford stacks. By *Deligne-Mumford stack*, we mean a stack in the étale topology with representable diagonal (i.e., representable by algebraic spaces), which has an étale surjective morphism from a scheme. For a general reference on stacks, see [Ols16] or [LMB00]; also, see [Sta16] for a more comprehensive reference.

Lemma 5.1. *Suppose $f \colon X \to Y$ is a map of Deligne-Mumford stacks. The fiber product $U \times_Y X$ is connected for all finite connected étale maps $U \to Y$ if and only if the induced map $\pi_1(X) \to \pi_1(Y)$ is surjective. In particular, if X and Y are normal, integral, and Noetherian, and $f : X \to Y$ is a flat map with connected geometric generic fiber, then the induced map $\pi_1(X) \to \pi_1(Y)$ is surjective.*

Proof. The first part holds in greater generality as a statement about Galois categories; see [Sta16, Tag 0BN6]. As for the second part, we only need verify that a connected finite étale cover $U \to Y$ pulls back to a connected cover of X. Note that because X and Y are normal and integral, étale covers of X and Y are connected if and only if they are irreducible. Here, we are using that normal and connected implies irreducible and that normality is local in the étale topology over Noetherian stacks. To see why normality is local in the étale topology over a Deligne-Mumford stack, note first that normality is local in the étale topology over any base scheme by [Sta16, Tag 03E7]. Using this, one defines a Deligne-Mumford stack to be normal if any étale cover by a scheme is normal. From this definition, it follows that normality of a Deligne-Mumford stack is equivalent to normality of any étale cover.

Thus, we only need show that if $U \to Y$ is any irreducible finite étale cover, then so is $X \times_Y U \to X$. But this follows from the assumptions that f is flat and U is integral, which implies all generic points of $X \times_Y U$ map to the generic point of U. So, if $X \times_Y U$ were reducible, the geometric generic fiber over U would also be reducible, which contradicts the assumption that f has connected geometric generic fiber, since a geometric generic fiber of $X \times_Y U$ is also a geometric generic fiber of f. $\qquad\square$

Proposition 5.2. *Let k be an arbitrary field of characteristic 0. Suppose X is a scheme and Y is a Deligne-Mumford stack over k, both of which are normal, integral, separated, and finite type over k, and let $f \colon X \to Y$ be a dominant map. Then, the image of the induced map $\pi_1(X) \to \pi_1(Y)$ has finite index in $\pi_1(Y)$. If, in addition, the geometric generic fiber of f is connected, then the map $\pi_1(X) \to \pi_1(Y)$ is surjective.*

Proof. To begin, we reduce to the case in which f is smooth. By generic smoothness, we may replace X by a dense open $X' \subset X$ so that $f|_{X'}$ is smooth. Since, $\pi_1(X') \to \pi_1(X)$ is a surjection by Lemma 5.1, in order to prove the proposition, we may replace X by X'.

The last sentence of this Proposition follows from Lemma 5.1 (here we only needed that the map be f be flat, but we have already reduced to the case it is smooth). To conclude, we only need prove that the image of $\pi_1(X) \to \pi_1(Y)$ has finite index in $\pi_1(Y)$, without the assumption that the geometric generic fiber of f is connected. Since f is smooth and Y is Deligne-Mumford, we can find a scheme U and a dominant étale map $U \to X$ so that $U \to Y$ factors through $\mathbb{A}^N_Y$ where N is the dimension of the geometric generic fiber of f and $U \to \mathbb{A}^N_Y$ étale. So, after passing to a dense open substack of $W \subset \mathbb{A}^N_Y$ and a dense open

subscheme $U' \subset U$, we may assume that $U' \to W$ is a finite étale cover: To see why, take a smooth cover of $\mathbb{A}_Y^N$ by a scheme. The pullback to U is a separated algebraic space, so it has a dense open subspace that is a scheme by [Ols16, Theorem 6.4.1]. The finiteness claim then follows because the resulting étale morphism of schemes is locally quasi-finite, of finite type, and quasi-separated, hence generically finite on the target. Since $U' \to W$ is finite étale, $\pi_1(U') \to \pi_1(W)$ has finite index. Because the maps $\pi_1(W) \to \pi_1(\mathbb{A}_Y^N)$ and $\pi_1(\mathbb{A}_Y^N) \to \pi_1(Y)$ are surjective by Lemma 5.1, the composition $\pi_1(U') \to \pi_1(Y)$ has finite index in $\pi_1(Y)$, and hence so does $\pi_1(X) \to \pi_1(Y)$. $\qquad\square$

5.2. **Applications.** Let K be a number field with fixed algebraic closure $\overline{K}$, let $\mathcal{M}_g$ denote the moduli stack of curves of genus g over K, and let $\mathcal{A}_g$ denote the moduli stack of PPAVs of dimension g over K. We have a natural map $\tau_g \colon \mathcal{M}_g \to \mathcal{A}_g$ given by the Torelli map, which sends a curve to its Jacobian. Let $\mathcal{U}_g$ denote the universal family over $\mathcal{A}_g$. Note that if U is any scheme and $A \to U$ is a family of PPAVs, then there exist maps $A \to \mathcal{U}_g$ and $U \to \mathcal{A}_g$ so that A equals the fiber product $U \times_{\mathcal{A}_g} \mathcal{U}_g$.

We will also be interested in the locus of smooth hyperelliptic curves of genus g, $\mathcal{H}_g \subset \mathcal{M}_g$, and locus of trigonal curves of genus g, $\mathcal{T}^g \subset \mathcal{M}_g$. If a curve C is trigonal, there exists a unique nonnegative integer M, called the Maroni invariant, with the property that there is a canonical embedding into the Hirzebruch surface $\mathbb{F}_M := \mathbb{P}_{\mathbb{P}^1}(\mathcal{O}_{\mathbb{P}^1} \oplus \mathcal{O}_{\mathbb{P}^1}(M))$. As mentioned in [PV15], the Maroni invariant takes on all integer values between 0 and $\frac{g+2}{3}$ with the same parity as g. Let $\mathcal{T}^g(M) \subset \mathcal{M}_g$ denote the substack of trigonal curves of Maroni invariant M.

In order to more easily utilize Proposition 5.2 for the purpose of giving interesting examples of Theorem 1.1, we record the following easy consequence of Proposition 5.2:

Corollary 5.3. *Let $U \subset \mathbb{P}_K^r$ be an open subscheme, and let $A \to U$ be a family of g-dimensional PPAVs. Let $\phi \colon U \to \mathcal{A}_g$ be the map induced by the universal property of $\mathcal{A}_g$. Let V be the smallest locally closed substack of $\mathcal{A}_g$ through which U factors, and let $W \subset \mathcal{A}_g$ be a normal integral substack. Suppose further that $W \cap V$ is dense in W and that V is normal. Then, if W has big monodromy, so do V and U. Furthermore, if the geometric generic fiber of ϕ is irreducible, then the monodromy of V agrees with that of U. In particular, the conclusion of Theorem 1.1 holds for U.*

Proof. By Lemma 5.1, if W has big monodromy so does the dense open subset $W \cap V \subset W$. Therefore, V has big monodromy, because it contains $W \cap V$, which has big monodromy. The result then follows from Proposition 5.2, once we verify that both U and V are normal, irreducible, separated, and finite type over K, with V Deligne-Mumford. All of these conditions are immediate except possibly that V is generically smooth, which holds by generic smoothness on a smooth cover of V by a scheme. $\qquad\square$

Before stating the main theorem of this section, we pause to describe more precisely what we mean by "the locus of plane curves."

Remark 5.1. In Theorem 1.2(c) and Theorem 5.4(d), we refer to the "substack of Jacobians of plane curves of degree d," for $d \geq 3$, and we now make more precise what we mean by this locus. When $d = 3$, all 1-dimensional abelian varieties can be realized as the Jacobian of a degree 3 plane curve, so in this case we take the locus to be all of $\mathcal{M}_{1,1}$. For $d \geq 4$, we will define a locally closed substack of $\mathcal{M}_g$, where $g = \binom{d-1}{2}$, and the locus of Jacobians of plane curves of degree d will denote the image of this under the Torelli map. For $d \geq 4$, let $\pi_d \colon \mathcal{V}_d \to \mathbb{P}^{\binom{d+2}{2}-1}$ denote the universal family over the Hilbert scheme of plane curves of degree d, and let $U_d \subset \mathbb{P}^{\binom{d+2}{2}-1}$ denote the dense open subscheme over which π_d is smooth.

Since $\mathscr{V}_d|_{U_d} \subset U_d \times \mathbb{P}^2$, the action of PGL_3 on $\mathbb{P}^2$ induces an action on $\mathscr{V}_d|_{U_d}$ and hence on U_d. Then, we define the substack of Jacobians of plane curves of degree d to be the stack theoretic quotient $[U_d/\mathrm{PGL}_3]$.

Note that there is a natural map $[U_d/\mathrm{PGL}_3] \to \mathscr{M}_g$. It can be verified that this map is a locally closed immersion of stacks. Further, one can show $[U_d/\mathrm{PGL}_3]$ represents the functor associating to any base scheme T projective flat morphisms $f \colon C \to T$ where each geometric fiber is a proper smooth curve of genus $g := \binom{d-1}{2}$ with a degree d invertible sheaf on C which commutes with base change. In this sense, $[U_d/\mathrm{PGL}_3]$ may naturally be referred to as "the locus of plane curves of degree d" and it is evidently smooth, since U_d is smooth, being a dense open subscheme of projective space.

Let us now briefly sketch the proof of the two facts claimed above. First, one can first see that $[U_d/\mathrm{PGL}_3]$ represents the claimed functor by defining natural maps both ways and verifying they are mutually inverse. To show $[U_d/\mathrm{PGL}_3] \to \mathscr{M}_g$ is a locally closed immersion, one can factor $[U_d/\mathrm{PGL}_3] \to \mathscr{M}_g$ through the stack G_d^2 parameterizing g_d^2's on the universal curve over $\mathscr{M}_g$, via a natural generalization of the definition given in [ACG11, Chapter XXI, Definition 3.12]. One can check the map $[U_d/\mathrm{PGL}_3] \to G_d^2$ is an open immersion from the definitions. Finally, one can verify that the map $G_d^2 \to \mathscr{M}_g$ is a locally closed immersion, using that every smooth plane curve of degree at least 4 has a unique g_d^2, see [ACGH85, Appendix A, Exercises 17 and 18], and the valuative criterion for locally closed immersions [Moc14, Chapter 1, Corollary 2.13].

We are now in position to state and prove the main theorem of this section:

Theorem 5.4. *Suppose $A \to U$ is a rational family of principally polarized abelian varieties and define V to be the smallest locally closed substack of $\mathscr{A}_g$ through which U factors. The conclusion of Theorem 1.1 holds whenever V is normal and contains a dense open substack of one of the following loci:*

(a) *The locus $\tau_g(\mathscr{H}_g)$ for any $g \geq 1$. For every $g \geq 1$, there exists a U dominating $\tau_g(\mathscr{H}_g)$ because $\mathscr{H}_g$ is unirational.*

(b) *The locus $\tau_g(\mathscr{T}^g(M))$ of Jacobians of trigonal curves with Maroni invariant $M < \frac{g}{3} - 1$ for any $g \geq 5$. In this case, there exists U dominating $\tau_g(\mathscr{T}^g(M))$ because $\mathscr{T}^g(M)$ is unirational.*

(c) *The locus of trigonal curves $\mathscr{T}^g$ in any $g \geq 3$. We can take U to be any open subscheme of $\mathscr{T}^g$, as $\mathscr{T}^g$ is rational.*

(d) *The locus of Jacobians of degree-d plane curves for any $d \geq 3$. In this case, the open subscheme of the Hilbert scheme of degree-d plane curves parameterizing smooth curves is rational and dominates the locus of Jacobians of degree-d plane curves.*

(e) *The locus $\tau_g(\mathscr{M}_g)$ for any $g \geq 1$. In this case, when $1 \leq g \leq 14$, $\mathscr{M}_g$ is unirational, so there exists a U dominating $\mathscr{M}_g$. Moreover, when $3 \leq g \leq 6$, $\mathscr{M}_g$ is rational, and so we may take U to be any open subscheme of $\mathscr{M}_g$.*

(f) *The locus $\mathscr{A}_g$ for any $g \geq 1$. When $1 \leq g \leq 5$, $\mathscr{A}_g$ is unirational, so such a U exists.*

Proof. By Corollary 5.3, it suffices to check that each of the families enumerated above has a dense open substack which has big monodromy, is irreducible, and is normal, and to verify the rationality and unirationality claims made above. Irreducibility of these loci is well-known. Note that in the first five cases, if we denote the locus in question by $\tau_g(W) \subset \mathscr{A}_g$, it suffices to verify that $W \subset \mathscr{M}_g$ is smooth as a substack of $\mathscr{M}_g$, as we now explain. First, $\tau_g(W) \subset \mathscr{A}_g$ is generically smooth because it is reduced, since it is the image of W, which

is reduced. Taking a smooth dense open $Z' \subset \tau_g(W)$, we have that $\tau_g^{-1}(Z') \subset W$ is a dense open substack, hence it is also smooth and has big monodromy. This implies Z' also has big monodromy since the monodromy of a locus in $\mathscr{M}_g$ agrees with the monodromy of its image in $\mathscr{A}_g$ under τ_g, as both can be identified with the monodromy action on the first cohomology group. We now conclude the proof by verifying that each locus in $\mathscr{M}_g$ (in the first five cases) is normal, has big monodromy, and is rational or unirational when claimed. In fact, we just show the substack has big geometric monodromy, since this implies it has big monodromy by Proposition 4.1.

(a) The hyperelliptic locus, $\mathscr{H}_g$, has big geometric monodromy as was shown independently in [Mum07, Lemma 8.12] and [A'C79, Théorème 1]. The hyperelliptic locus $\mathscr{H}_g$ is smooth and unirational because it is the quotient of an open subscheme of $\mathbb{P}_K^{2g+2}$ by the smooth action of PGL_2.

(b) By [BL16, Theorem, p. 2], $\mathscr{T}^g(M)$ has big geometric monodromy when $M < \frac{g}{3} - 1$. Additionally, $\mathscr{T}^g(M)$ is smooth and unirational because it can be expressed as a quotient $[U/G]$ of a smooth rational scheme U by a smooth group scheme G. Here, G is the group of automorphisms of the Hirzebruch surface $\mathbb{F}_M$ and U is an open subscheme of the projectivization of the linear system of class $3e + \left(\frac{g+3M+2}{2}\right) f$ on $\mathbb{F}_M$, where f is the class of the fiber over $\mathbb{P}^1$ and e is the unique section with negative self-intersection (see [BL16, p. 8] for an explanation of this description of U). Note that in this application, we are implicitly translating between the topological monodromy representation of $\mathscr{M}_g$ described in [BL16, Theorem, p. 2] and the algebraic Galois representation in $\mathscr{A}_g$, but these two representations are compatible, essentially because both are given by the action of the fundamental group on the first cohomology group.

(c) In the case that $g \geq 5$, we have $\mathscr{T}^g(g \bmod 2)$ is birational to $\mathscr{T}^g$, so $\mathscr{T}^g$ has a smooth dense open with big geometric monodromy by the previous part. Next, $\mathscr{T}^g$ is rational for $g \geq 5$ by [Ma15, Theorem, p. 1]. The cases $g = 3, 4$ hold because for such g, $\mathscr{T}^g$ forms a dense open in $\mathscr{M}_g$, which is itself rational and smooth, as shown in the proof of part (e) below.

(d) By Remark 5.1, the locus of plane curves (as was also defined in Remark 5.1) in $\mathscr{M}_g$ is smooth. By [Bea86, Théorème 4], the locus of smooth degree-d plane curves in the Hilbert scheme has big geometric monodromy. It follows from Lemma 5.1 that the locus of plane curves has big monodromy. The locus of *smooth* degree-d plane curves in the Hilbert scheme is certainly rational, as it is an open subscheme of the Hilbert scheme of degree-d plane curves, which is itself isomorphic to $\mathbb{P}_K^{\binom{d+2}{2}-1}$.

(e) By [DM69, 5.12], the geometric monodromy of $\mathscr{M}_g$ is all of $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ for every $g \geq 1$. (Alternatively, the fact that $\mathscr{M}_g$ has big geometric monodromy follows immediately from the corresponding fact for any one of parts (a)–(d).) Next, $\mathscr{M}_g$ is smooth by [DM69, Theorem 5.2]. We have that $\mathscr{M}_g$ is unirational for $1 \leq g \leq 14$ by [Ver05]. Moreover, when $3 \leq g \leq 6$, we have that $\mathscr{M}_g$ is rational; see [CF07, p. 2] for comprehensive references.

(f) Note that $\mathscr{A}_g$ has geometric big monodromy because $\mathscr{A}_g$ contains $\mathscr{M}_g$ and $\mathscr{M}_g$ has monodromy $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, as argued in point (d). Further, $\mathscr{A}_g$ is smooth by [Oor71, Theorem 2.4.1]. We have that $\mathscr{A}_g$ is unirational for $1 \leq g \leq 5$ as shown in [Ver05, p. 1]. $\square$

Remark 5.2. In most of the cases enumerated in Theorem 5.4, we actually know that the geometric monodromy is not only big, but also equal to $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$. By Corollary 5.3, this occurs when U has irreducible geometric generic fiber over any of the following loci:

(a) The locus $\mathscr{T}^g(M)$ for any $M < \frac{g}{3} - 1$, by [BL16, Theorem, p. 2];
(b) The locus of plane curves of degree d with d even, by [Bea86, Theoreme 4(i)];
(c) The locus $\mathscr{M}_g$ for any g, by [DM69, 5.12];
(d) The locus $\mathscr{A}_g$ for any g, because $\mathscr{M}_g \subset \mathscr{A}_g$ and $\mathscr{M}_g$ has full monodromy by point (d).

Remark 5.3. If $A \to U$ is a family with $H_A^{\mathrm{geom}} = \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, then the group H_A can be determined as follows. The intersection $K \cap \mathbb{Q}^{\mathrm{cyc}}$ is of the form $\mathbb{Q}(\zeta_n)$ for some $n \geq 2$. Let $r_n : \widehat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ be the reduction map. Then

$$H_A = \ker(r_n \circ \mathrm{mult}) = \{M \in \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}) : \mathrm{mult}\, M \equiv 1 \pmod{n}\},$$

which follows from Remark 3.2. Thus, when the conclusion of the preceding remark holds, Theorem 1.1 tells us the following:

- If $K \neq \mathbb{Q}$, or if $K = \mathbb{Q}$ and $g \geq 3$, then most $u \in U(K)$ have $H_{A_u} = \ker(r_n \circ \mathrm{mult})$.
- If $K = \mathbb{Q}$ and $g \in \{1, 2\}$, then most $u \in U(K)$ are such that $[\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) : H_{A_u}] = 2$.

Remark 5.4. Theorem 5.4 (a) tells us that if U dominates $\mathscr{H}_g$, then the conclusion of Theorem 1.1 holds for U. In the case where U has irreducible geometric generic fiber, we can say explicitly what the monodromy group of the family is and what its commutator is. For example, let $\mathscr{Y}_{2g+2,K}$ denote the family of genus-g hyperelliptic curves over K with Weierstrass equation given by $y^2 = x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_0$. We show in [LSTX17a, Theorem 1.2] that most members of $\mathscr{Y}_{2g+2,K}$ have monodromy equal to $H_{\mathscr{Y}_{2g+2,K}}$ (which we explicitly compute) over $K \neq \mathbb{Q}$, and have index-2 monodromy when $K = \mathbb{Q}$. We neither prove nor state this result precisely here, but a complete statement and proof is given in [LSTX17a].

Appendix A. Explicit Surjectivity for Abelian Surfaces
By Davide Lombardo

Let K be a number field and A/K be an abelian surface such that $\mathrm{End}_{\overline{K}}(A) = \mathbb{Z}$. For every place w of K at which A has good reduction, let Frob_w be the corresponding Frobenius element of $\mathrm{Gal}\left(\overline{K}/K\right)$ and let $f_w(x)$ be the characteristic polynomial of Frob_w acting on $T_\ell A$, where ℓ is any prime different from the residual characteristic of w (as it is well known, this definition is well-posed). Let $F(w)$ be the splitting field over $\mathbb{Q}$ of $f_w(x)$. By Remark 4.5, the Galois group of $F(w)/\mathbb{Q}$ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2 \simeq D_4$, the dihedral group on 4 points.

To state our result we need the following function:

Definition A.1. Let $\alpha(g) = 2^{10}g^3$ and set $b(d,g,h) = \left((14g)^{64g^2}d\max{(h, \log d, 1)}^2\right)^{\alpha(g)}$.

We shall show the following result, which extends [Lom15, Theorem 1.2] to the case of abelian surfaces:

Proposition A.2. *Let v be a place of K, of good reduction for A, such that the Galois group of $f_v(x)$ is isomorphic to D_4. Let q_v be the order of the residue field at v. For all primes ℓ, let*

$$\rho_{\ell^\infty} : \mathrm{Gal}\left(\overline{K}/K\right) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{GL}_4(\mathbb{Z}_\ell)$$

be the natural ℓ-adic Galois representation attached to A/K. We have $\operatorname{Im}\rho_{\ell^\infty} = \operatorname{GSp}_4(\mathbb{Z}_\ell)$ for all primes ℓ that are unramified in K and strictly larger than

$$\max\{b(2[K:\mathbb{Q}],4,2h(A))^{1/4},(2q_v)^8\}.$$

From now on, let v be a place as in the statement of proposition A.2. Notice that $f_v(x)$ is irreducible by assumption, hence all its roots are simple. Moreover, $f_v(x)$ doesn't have any real roots, because (by the Weil conjectures) every root of $f_v(x)$ has absolute value $\sqrt{q_v}$, hence its only possible real roots are $\pm\sqrt{q_v}$. But these are algebraic numbers of degree at most 2 over $\mathbb{Q}$, while $f_v(x)$ is irreducible of degree 4, contradiction. In particular, the roots of $f_v(x)$ come in complex conjugate pairs, so we shall denote them by $\mu_1,\mu_2,\iota(\mu_1),\iota(\mu_2)$, where $\iota:\mathbb{C}\to\mathbb{C}$ is complex conjugation. We shall need the following lemma:

Lemma A.3. *Let x,y,z be three distinct eigenvalues of* Frob_v. *We have* $y^2 \neq xz$.

Proof. Suppose first that $z = \iota(x)$. Then $y^2 = x\iota(x) = q_v$, which implies that $y = \pm\sqrt{q_v}$ is a root of $f_v(x)$. As we have already seen, this is a contradiction. Hence, up to renaming the eigenvalues of Frob_v if necessary, we can assume $x = \mu_1, z = \mu_2$ and $y = \iota(\mu_1)$. Since $\operatorname{Gal}(F(v)/\mathbb{Q})$ is isomorphic to D_4 by assumption, there is a $\sigma \in \operatorname{Gal}(F(v)/\mathbb{Q})$ such that $\sigma(\mu_1) = \mu_1, \sigma(\iota(\mu_1)) = \iota(\mu_1), \sigma(\mu_2) = \iota(\mu_2)$ and $\sigma(\iota(\mu_2)) = \mu_2$. Applying σ to the equality $y^2 = xz$, that is, $\iota(\mu_1)^2 = \mu_1\mu_2$, we get $\iota(\mu_1)^2 = \mu_1\iota(\mu_2)$, whence $\iota(\mu_2) = \mu_2$. But this implies that μ_2 is real, which is once again a contradiction. $\square$

Proof of Proposition A.2. Let ℓ be a prime unramified in K and strictly larger than $b(2[K:\mathbb{Q}],4,2h(A))^{1/4}$. Let $\rho_\ell : \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut} A[\ell]$ be the natural Galois representation associated with the ℓ-torsion of A.

Much of the proof of [Lom16, Theorem 3.19] still applies in the current setting, and shows that one of the following holds:

(a) $\operatorname{Im}(\rho_{\ell^\infty}) = \operatorname{GSp}_4(\mathbb{Z}_\ell)$
(b) the image of ρ_ℓ is contained in a maximal subgroup of $\operatorname{GSp}_4(\mathbb{F}_\ell)$ of type (2) in the sense of Theorem 3.3 in [Lom16].

If we are in case (1) we are done, so assume we are in case (2). To conclude the proof, we shall show that $\ell \leq (2q_v)^8$. If ℓ is equal to the residual characteristic of v this inequality is obvious, so we can assume that $v \nmid \ell$. In this case, the characteristic polynomial of the action of Frob_v on $T_\ell A$ is $f_v(x)$. By [Lom16, Lemma 3.4], the eigenvalues of any $x \in \operatorname{Im}(\rho_\ell)$ can be written as $\lambda \cdot \lambda_1^3, \lambda \cdot \lambda_1^2\lambda_2, \lambda \cdot \lambda_1\lambda_2^2, \lambda \cdot \lambda_2^3$ for some $\lambda,\lambda_1,\lambda_2 \in \mathbb{F}_{\ell^2}^\times$. Taking $g := \rho_\ell(\operatorname{Frob}_v)$, we may assume the four eigenvalues $\nu_1,\dots,\nu_4$ of g satisfy $\nu_2^2 = \nu_1\nu_3$.

Let λ be a place of $F(v)$ of characteristic ℓ and identify λ with a maximal ideal of $\mathcal{O}_{F(v)}$. Since $f_v(x)$ splits completely in $F(v)$ by definition, its four roots $\mu_1,\mu_2,\iota(\mu_1),\iota(\mu_2)$ all belong to $\mathcal{O}_{F(v)}$. Upon reduction modulo λ, these four roots yield four elements of $\mathcal{O}_{F(v)}/\lambda$, which is a finite field of characteristic ℓ. Moreover, as $\{\mu_1,\mu_2,\iota(\mu_1),\iota(\mu_2)\}$ is a Galois-stable set, its image in $\overline{\mathbb{F}}_\ell$ independent of the choice embedding of $\mathcal{O}_{F(v)}/\lambda$ into $\overline{\mathbb{F}}_\ell$, hence well defined. Denote by $\overline{\mu_1},\overline{\mu_2},\overline{\iota(\mu_1)},\overline{\iota(\mu_2)}$ the images of $\mu_1,\mu_2,\iota(\mu_1),\iota(\mu_2)$ in $\overline{\mathbb{F}}_\ell$.

Now observe that the characteristic polynomial of g is the reduction modulo ℓ of $f_v(x)$, so its roots $\nu_1,\dots,\nu_4 \in \overline{\mathbb{F}}_\ell^\times$ must coincide with $\overline{\mu_1},\overline{\mu_2},\overline{\iota(\mu_1)},\overline{\iota(\mu_2)}$ in some order. Given that $\nu_2^2 = \nu_1\nu_3$, there are three (necessarily distinct) eigenvalues of Frob_v, call them x,y,z, that satisfy $y^2 - xz \equiv 0 \pmod{\lambda}$. By Lemma A.3, $N_{F(v)/\mathbb{Q}}(y^2 - xz)$ is a nonzero integer. Therefore, $N_{F(v)/\mathbb{Q}}(y^2 - xz)$ has positive valuation at λ, hence it is divisible by ℓ. In turn,

this gives

$$\ell \leq |N_{F(v)/\mathbb{Q}}(y^2 - xz)| = \prod_{\sigma \in \mathrm{Gal}(F(v)/\mathbb{Q})} |\sigma(y)^2 - \sigma(x)\sigma(z)| \leq (2q_v)^8,$$

where the inequality $|\sigma(y)^2 - \sigma(x)\sigma(z)| \leq 2q_v$ follows immediately from the triangle inequality and the Weil conjectures. □

Acknowledgments

References

[A'C79]   N. A'Campo. Tresses, monodromie et le groupe symplectique. *Comment. Math. Helv.*, 54(2):318–327, 1979.

[ACG11]   Enrico Arbarello, Maurizio Cornalba, and Phillip A. Griffiths. *Geometry of algebraic curves. Volume II*, volume 268 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer, Heidelberg, 2011. With a contribution by Joseph Daniel Harris.

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985.

[AdRAK+16] Sara Arias-de Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, and Núria Vila. Large Galois images for Jacobian varieties of genus 3 curves. *Acta Arith.*, 174(4):339–366, 2016.

[ALS16]   S. Anni, P. Lemos, and S. Siksek. Residual representations of semistable principally polarized abelian varieties. *Res. Number Theory*, 2:2:1, 2016.

[Bea86]   A. Beauville. Le groupe de monodromie des familles universelles d'hypersurfaces et d'intersections complètes. In *Complex analysis and algebraic geometry (Göttingen, 1985)*, volume 1194 of *Lecture Notes in Math.*, pages 8–18. Springer, Berlin, 1986.

[BL16]   M. Bolognesi and M. Lönne. Mapping class groups of trigonal loci. *Selecta Math. (N.S.)*, 22(1):417–445, 2016.

[Cad15]   Anna Cadoret. An open adelic image theorem for abelian schemes. *Int. Math. Res. Not. IMRN*, (20):10208–10242, 2015.

[CF07]   G. Casnati and C. Fontanari. On the rationality of moduli spaces of pointed curves. *J. Lond. Math. Soc. (2)*, 75(3):582–596, 2007.

[CGJ11]   A. C. Cojocaru, D. Grant, and N. Jones. One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations. *Proc. Lond. Math. Soc. (3)*, 103(4):654–675, 2011.

[CH05]   A. C. Cojocaru and C. Hall. Uniform results for Serre's theorem for elliptic curves. *Int. Math. Res. Not.*, (50):3065–3080, 2005.

[CM15]   Anna Cadoret and Ben Moonen. Integral and adelic aspects of the mumford-tate conjecture. *arXiv preprint arXiv:1508.06426*, 2015.

[CT12]   Anna Cadoret and Akio Tamagawa. A uniform open image theorem for ℓ-adic representations, I. *Duke Math. J.*, 161(13):2605–2634, 2012.

[CT13]   Anna Cadoret and Akio Tamagawa. A uniform open image theorem for ℓ-adic representations, II. *Duke Math. J.*, 162(12):2301–2344, 2013.

[Die02]   L. V. Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\text{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

[DM69]   P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.*, (36):75–109, 1969.

[Duk97]   W. Duke. Elliptic curves with no exceptional primes. *C. R. Acad. Sci. Paris Sér. I Math.*, 325(8):813–818, 1997.

[EEHK09]   J. S. Ellenberg, C. Elsholtz, C. Hall, and E. Kowalski. Non-simple abelian varieties in a family: geometric and analytic approaches. *Journal of the London Mathematical Society*, page jdp021, 2009.

[Eke90]   T. Ekedahl. An effective version of Hilbert's irreducibility theorem. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 241–249. Birkhäuser Boston, Boston, MA, 1990.

[Fal86]   G. Faltings. Finiteness theorems for abelian varieties over number fields. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 9–27. Springer, New York, 1986. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz.

[FWG+92]   G. Faltings, G. Wüstholz, F. Grunewald, Norbert Schappacher, and Ulrich Stuhler. *Rational points.* Aspects of Mathematics, E6. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1992. Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984, With an appendix by Wüstholz.

[GR71a]   A. Grothendieck and M. Raynaud. *Revêtements étales et groupe fondamental.* Springer-Verlag, Berlin-New York, 1971. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1).

[GR71b]   A. Grothendieck and M. Raynaud. *Revêtements étales et groupe fondamental.* Springer-Verlag, Berlin-New York, 1971. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1).

[Gra00]   D. Grant. A formula for the number of elliptic curves with exceptional primes. *Compositio Math.*, 122(2):151–164, 2000.

[Gre10]   A. Greicius. Elliptic curves with surjective adelic Galois representations. *Experiment. Math.*, 19(4):495–507, 2010.

[Gro66a]   A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. *Inst. Hautes Études Sci. Publ. Math.*, (28):255, 1966.

[Gro66b]   A. Grothendieck. Un théorème sur les homomorphismes de schémas abéliens. *Invent. Math.*, 2:59–78, 1966.

[Gro67]   A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[HS00]   M. Hindry and J. H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[Jon10]   N. Jones. Almost all elliptic curves are Serre curves. *Trans. Amer. Math. Soc.*, 362(3):1547–1570, 2010.

[Jou82]   Jean-Pierre Jouanolou. Theoremes de bertini et applications. 1982.

[Kaw03]   T. Kawamura. The effective surjectivity of mod l Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring. *Comment. Math. Helv.*, 78(3):486–493, 2003.

[Kow06]   E. Kowalski. The large sieve, monodromy and zeta functions of curves. *J. Reine Angew. Math.*, 601:29–69, 2006.

[LMB00]   G. Laumon and L. Moret-Bailly. *Champs algébriques*, volume 39 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2000.

[Lom15]   D. Lombardo. Explicit open image theorems for abelian varieties with trivial endomorphism ring. *arXiv:1508.01293v2*, August 2015.

[Lom16]   D. Lombardo. Explicit surjectivity of Galois representations for abelian surfaces and GL_2-varieties. *J. Algebra*, 460:26–59, 2016.

[LSTX17a]   A. Landesman, A. A. Swaminathan, J. Tao, and Y. Xu. Hyperelliptic curves with maximal galois action on the torsion points of their jacobians. *arXiv preprint arXiv:1705.08777v2*, 2017.

[LSTX17b]   Aaron Landesman, Ashvin A. Swaminathan, James Tao, and Yujie Xu. Lifting subgroups of symplectic groups over $\mathbb{Z}/\ell\mathbb{Z}$. *Res. Number Theory*, 3:Art. 14, 12, 2017.

[Ma15]   S. Ma. The rationality of the moduli spaces of trigonal curves. *Int. Math. Res. Not. IMRN*, (14):5456–5472, 2015.

[Moc14]   Shinichi Mochizuki. *Foundations of p-adic Teichmüller Theory*, volume 11. American Mathematical Soc., 2014.

[Mor01]   Dave Witte Morris. Introduction to arithmetic groups. *arXiv preprint math/0106063v6*, 2001.

[Mum07]   D. Mumford. *Tata lectures on theta. II*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.

[Ols16]   Martin Olsson. *Algebraic spaces and stacks*, volume 62 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2016.

[O'M78]   O. T. O'Meara. *Symplectic groups*, volume 16 of *Mathematical Surveys*. American Mathematical Society, Providence, R.I., 1978.

[Oor71]   F. Oort. Finite group schemes, local moduli for abelian varieties, and lifting problems. *Compositio Math.*, 23:265–296, 1971.

[OV00]   F. Orgogozo and I. Vidal. Le théorème de spécialisation du groupe fondamental. In *Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998)*, volume 187 of *Progr. Math.*, pages 169–184. Birkhäuser, Basel, 2000.

[PV15]   A. Patel and R. Vakil. On the Chow ring of the Hurwitz space of degree three covers of $\mathbf{P}^1$. *arXiv:1505.04323v1*, May 2015.

[Rib76]   K. A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[Riv08]   I. Rivin. Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms. *Duke Math. J.*, 142(2):353–379, 2008.

[Ser72]   J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser97]   J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Ser98]   J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Sta16]   The Stacks Project Authors. *Stacks Project*. http://stacks.math.columbia.edu, 2016.

[Ste61]   R. Steinberg. Automorphisms of classical Lie algebras. *Pacific J. Math.*, 11:1119–1129, 1961.

[Ver05]   A. Verra. The unirationality of the moduli spaces of curves of genus 14 or lower. *Compos. Math.*, 141(6):1425–1444, 2005.

[Wal14]   E. Wallace. Principally polarized abelian surfaces with surjective Galois representations on l-torsion. *J. Lond. Math. Soc. (2)*, 90(2):451–471, 2014.

[Zyw10a]   D. Zywina. Elliptic curves with maximal Galois action on their torsion points. *Bull. Lond. Math. Soc.*, 42(5):811–826, 2010.

[Zyw10b]   D. Zywina. Hilbert's irreducibility theorem and the larger sieve. *arXiv:1011.6465v1*, November 2010.

[Zyw15]   D. Zywina. An explicit Jacobian of dimension 3 with maximal Galois action. *arXiv:1508.07655v1*, August 2015.

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, STANFORD, CA 94305
E-mail address, Aaron Landesman: `aaronlandesman@stanford.edu`

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NJ 08544
E-mail address, Ashvin A. Swaminathan: `ashvins@math.princeton.edu`

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139
E-mail address, James Tao: `jamestao@mit.edu`

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138
E-mail address, Yujie Xu: `yujiex@math.harvard.edu`