ON ABELIAN VARIETIES WHOSE TORSION IS NOT SELF-DUAL

SARAH FREI, KATRINA HONIGS, AND JOHN VOIGHT

Abstract. We construct infinitely many abelian surfaces A defined over the rational numbers such that, for a prime $\ell \leqslant 7$, the ℓ-torsion subgroup of A is not isomorphic as a Galois module to the ℓ-torsion subgroup of its dual $A^\vee$. We do this by explicitly analyzing the action of the Galois group on the ℓ-adic Tate module and its reduction modulo ℓ. We offer a framework for these computations and illustrate its use in simpler examples before using it in the proof of our main result.

Contents

1. Introduction

1.1. **Setup.** Let K be a number field with algebraic closure K^{al}. Let A be an abelian variety over K of dimension $g := \dim A \geq 1$. For example, we may take $A = E$ an elliptic curve over K, the case $g = 1$. Many important arithmetic features of A are reflected in its torsion subgroups $A[n](K^{\mathrm{al}}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$ for $n \geq 1$. The equations that define the n-torsion subgroup define a variety $A[n]$ of dimension zero over K; and the finite set of points $A[n](K^{\mathrm{al}})$ is defined over its splitting field, a minimal finite Galois extension of K denoted $K(A[n])$. The Galois group $\mathrm{Gal}(K(A[n]) \,|\, K)$ acts on $A[n]$ preserving the group law, so each element acts via an element of $\mathrm{Aut}(A[n](K^{\mathrm{al}}))$, giving an injective homomorphism

$$\mathrm{Gal}(K(A[n]) \,|\, K) \hookrightarrow \mathrm{Aut}(A[n](K^{\mathrm{al}})) \simeq \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

It is convenient to lift this to the absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{al}} \,|\, K)$ to obtain a linear representation

$$\overline{\rho}_{A,n} \colon \mathrm{Gal}_K \to \mathrm{Aut}(A[n](K^{\mathrm{al}})) \simeq \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z}) \tag{1.1.1}$$

Date: October 28, 2024.

2020 *Mathematics Subject Classification.* Primary: 11G10, 11F80. Secondary: 14K15, 11G05.

Key words and phrases. Abelian varieties, non-principal polarizations, finite group schemes, Galois representations.

with $\ker \overline{\rho}_{A,n} = \mathrm{Gal}(K^{\mathrm{al}} \,|\, K(A[n]))$. Studying the Galois representation $\overline{\rho}_{A,n}$—for example, using techniques in number theory, group theory, and linear algebra—remains an essential technique for understanding A and is itself an interesting pursuit.

At the same time, attached to A is its dual abelian variety $A^\vee := \mathbf{Pic}^0_A$ parametrizing isomorphism classes of invertible line bundles on A. For $A = E$ an elliptic curve, there is a canonical isomorphism $E \cong \mathbf{Pic}^0_E$ [Sil09, Proposition III.3.4] (see also Example 2.4.3), so duals are predominantly a feature of abelian varieties of dimension $g \geq 2$. In some sense analogous to the tautological pairing between a vector space and its dual, there is a natural duality between the torsion subgroups $A[n]$ and $A^\vee[n]$, called the *(tautological) Weil pairing*

$$A[n] \times A^\vee[n] \to \mu_n. \tag{1.1.2}$$

The Weil pairing is perfect, so in particular it gives a canonical isomorphism

$$A^\vee[n] \cong \mathrm{Hom}(A[n], \mu_n) \tag{1.1.3}$$

that is compatible with the action of Gal_K. (For a quick review and further references, see section 2.3).

We recall that Gal_K acts on the variety μ_n, whose points $\mu_n(K^{\mathrm{al}}) = \langle \zeta_n \rangle$ are the nth roots of unity, by the mod n cyclotomic character

$$\varepsilon_n \colon \mathrm{Gal}_K \to \mathrm{Aut}(\mu_n(K^{\mathrm{al}})) \simeq (\mathbb{Z}/n\mathbb{Z})^\times, \tag{1.1.4}$$

uniquely defined by $\sigma(\zeta_n) = \zeta_n^{\varepsilon_n(\sigma)}$ for all $\sigma \in \mathrm{Gal}_K$. Therefore (1.1.3) yields a canonical isomorphism

$$\overline{\rho}_{A^\vee,n} \cong \overline{\rho}^{\,*}_{A,n} \otimes \varepsilon_n, \tag{1.1.5}$$

where * denotes the contragredient (dual) representation. Concretely put: if we are given a matrix for the action of $\sigma \in \mathrm{Gal}_K$ on $A[n](K^{\mathrm{al}})$ as in (1.1.1), then the matrix for the action of σ on $A^\vee[n](K^{\mathrm{al}})$ is its transpose inverse scaled by $\varepsilon_n(\sigma)$.

For most abelian varieties one encounters, there is an equivalence of linear representations $\overline{\rho}_{A,n} \simeq \overline{\rho}_{A^\vee,n}$—i.e., there is an isomorphism of splitting fields which induces a linear isomorphism on the n-torsion. Indeed, if A has a polarization $\lambda \colon A \to A^\vee$ over K whose degree is coprime to n—such as if A has a principal polarization over K, which holds when A is the Jacobian of a smooth, projective, geometrically integral curve over K (a so-called *nice* curve)—then the polarization induces an isomorphism $A[n] \simeq A^\vee[n]$.

In general, these two linear representations are quite challenging to distinguish. The number fields $K(A[n])$ and $K(A^\vee[n])$ are always *equal*, taken inside K^{al} (Lemma 5.2.2)! And for $n = \ell$ prime, the semi-simplifications of $\overline{\rho}_{A,\ell}$ and $\overline{\rho}_{A^\vee,\ell}$ are isomorphic (Lemma 5.2.1), so in particular we have the equality $\det(1 - \overline{\rho}_{A,n}(\sigma)T) = \det(1 - \overline{\rho}_{A^\vee,n}(\sigma)T) \in (\mathbb{Z}/n\mathbb{Z})[T]$ of characteristic polynomials for all $\sigma \in \mathrm{Gal}_K$.

1.2. Results.

Our main result shows that, in general, these representations need not be equivalent.

Theorem 1.2.1. *Let $n \in \mathbb{Z}_{>0}$ be divisible by a prime $\ell \leqslant 7$. Then there exist infinitely many pairwise geometrically non-isogenous abelian surfaces A over $\mathbb{Q}$ such that $\overline{\rho}_{A,n} \not\simeq \overline{\rho}_{A^\vee,n}$.*

Equivalently by (1.1.5), for a surface A in Theorem 1.2.1, the representation $\overline{\rho}_{A,n}$ is not self-dual up to twist by its similitude character, the cyclotomic character. (Also equivalent: $A[n] \not\simeq A^\vee[n]$ as group schemes over $\mathbb{Q}$.)

It is enough to prove the theorem for $n = \ell \leqslant 7$ prime. We construct the abelian surfaces in Theorem 1.2.1 explicitly, as follows. We choose elliptic curves E_1, E_2 and nontrivial $P \in E_1[\ell](\mathbb{Q})$, $Q \in E_2[\ell](\mathbb{Q})$ and glue E_1, E_2 along the diagonal subgroup $\langle(P, Q)\rangle$. The resulting abelian surfaces are not simple over $\mathbb{Q}$, and they have a $(1, \ell)$-polarization but not a principal polarization over $\mathbb{Q}$. In fact, infinitely many of these surfaces do not have a principal polarization over $\mathbb{Q}^{\mathrm{al}}$. We are able to prove the above theorem for odd values of ℓ by observing that although these abelian surfaces have a $\mathbb{Q}$-torsion point, their duals do not. In the $\ell = 2$ case, the dual abelian surface will have a $\mathbb{Q}$-torsion point, but the Galois actions are, nevertheless, not isomorphic.

The underlying parameter space for our construction is the product $Y_1(\ell)\times Y_1(\ell)$ of modular curves; for $\ell \leqslant 7$, this space is birational to $\mathbb{A}^2$. We may therefore modify the setup or ask for additional properties to be satisfied in Theorem 1.2.1. Accordingly, our results can be extended over any number field K with $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$.

Finally, we also go a bit further: forgetting the group structure, the linear representation $\overline{\rho}_{A,n}$ yields a permutation representation $\pi_{A,n} \colon \mathrm{Gal}_K \to \mathrm{Sym}(A[n]) \simeq S_{n^{2g}}$. If $\overline{\rho}_{A,n} \simeq \overline{\rho}_{A^\vee,n}$ then of course $\pi_{A,n} \simeq \pi_{A^\vee,n}$, but not necessarily conversely. In fact, the abelian surfaces among those exhibited in Theorem 1.2.1 satisfy the stronger property that $\pi_{A,n} \not\simeq \pi_{A^\vee,n}$ for $\ell \in \{3, 5, 7\}$.

Corollary 1.2.2. *Let $\ell \in \{3, 5, 7\}$. Then there exist infinitely many geometrically nonisogenous abelian surfaces A over $\mathbb{Q}$ such that $\pi_{A,\ell} \not\simeq \pi_{A^\vee,\ell}$. Moreover, the linear representations $\mathrm{Gal}_K \to \mathrm{GL}_{\ell^{2g}}(k)$ induced by the permutation representations $\pi_{A,\ell}$ and $\pi_{A^\vee,\ell}$ over any field k with $\mathrm{char}\, k = 0$ are not isomorphic.*

1.3. **Discussion.** In writing out the proof of Theorem 1.2.1, we found that it benefited from elaborating upon several topics and techniques that we could not find in the literature as accessibly or as completely as we needed for our application. In particular, the key matrix calculation became much more transparent once we had the appropriate commutative diagrams to guide us (as usual in linear algebra), so we make this the focus of section 3.

We hope this first paper will see followup work. In particular, it would be interesting to produce other constructions of abelian varieties satisfying Theorem 1.2.1. A first step in this direction would be to classify those subgroups $G \leqslant \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$ preserving a degenerate (but nonzero) alternating pairing up to scaling with the property that G is not isomorphic to its contragredient twisted by the similitude character. Attached to each G would be an associated moduli space of polarized abelian varieties of dimension g, and the rational points of this moduli space which do not lift to the moduli space attached to any proper subgroup $G' < G$ would similarly give candidate examples. We complete such a classification for $g = n = 2$ in Proposition 5.2.4. Exhibiting such abelian varieties systematically (and explicitly, if possible) presents an attractive challenge.

Finally, one impetus for exhibiting these abelian varieties came from studying the cohomology and derived categories of symplectic varieties of Kummer type: see Remark 5.1.3.

1.4. **Contents.** We begin by providing background on abelian varieties and relevant structures such as polarizations and duality in section 2; we also elaborate upon the Hilbert irreducibility theorem, a key tool in the proof of our main result. Before proceeding with our construction, in section 3 we explain (in a categorical context) how Galois actions on Tate modules change under isogenies and duals, and we work through some examples with our computational tools. We hope that this will serve as a useful framework for others interested in studying Galois images of torsion subgroups of abelian varieties. In section 4 we exhibit our family of abelian surfaces, describe its basic properties, and complete the proof of Theorem 1.2.1. In section 5, we give some further analysis, including a proof of Corollary 1.2.2, and conclude with some final remarks about related questions and future work.

Acknowledgements. The authors would like to thank Eran Assaf, Asher Auel, Nils Bruin, Johan de Jong, Aaron Landesman, Pablo Magni, Bjorn Poonen, Ari Shnidman, Alexei Skorobogatov, David Webb, and Ariel Weiss for helpful comments. Frei was supported by an AMS-Simons Travel grant. Honigs was supported by an NSERC Discovery grant. Voight was supported by a Simons Collaboration grant (550029).

2. Background on abelian varieties

In this section, we give a survey of the main ingredients in our proof of Theorem 1.2.1 and Corollary 1.2.2: isogenies and Tate modules (2.1), dual abelian varieties (2.2), polarizations (2.4), and the Weil pairing (2.3). A standard reference for abelian varieties is the book of Mumford [Mum70]; we also recommend Hindry–Silverman [HS00, Part A], the work of Milne [Mil86a, Mil08], and Birkenhake–Lange [BL04] for complex abelian varieties. Or to just get started with introduction via the perspective of elliptic curves, we suggest Silverman [Sil09]. There is a lot to be found in these works! So we endeavour in this section to give a motivated, working introduction.

2.1. **Isogenies and Tate modules.** Let k be a field with characteristic $\operatorname{char} k = p$, allowing $p = 0$. Let $k^{\text{sep}} \subseteq k^{\text{al}}$ be a separable and algebraic closure of k. Let A and A' be abelian varieties over k with common dimension $g := \dim A = \dim A'$. To avoid trivialities, we suppose that $g \geq 1$.

An isogeny $\varphi\colon A \to A'$ is a surjective homomorphism, or equivalently a homomorphism with finite kernel $\#(\ker\varphi)(k^{\text{al}}) < \infty$. (Some authors take the zero map to be an isogeny; we do not.) An isogeny is separable if the corresponding finite extension $k(A) \supseteq k(A')$ of function fields is separable, or equivalently $(\ker\varphi)(k^{\text{al}}) = (\ker\varphi)(k^{\text{sep}})$ and $[k(A) : k(A')] = \#(\ker\varphi)(k^{\text{sep}})$—analogous to the usual condition for a finite extension of fields to be Galois. (The reader may wish to focus on the case $k = \mathbb{Q}$ where all isogenies are separable; but the setup permits an arbitrary field.)

We pause to give a bit of motivation before proceeding further. Over the complex numbers $k = \mathbb{C}$, abelian varieties are complex tori, and isogenies can be understood using linear algebra. Indeed, we have an isomorphism $A(\mathbb{C}) \simeq V/\Lambda$ where $V \simeq \mathbb{C}^g$ is a complex vector space of dimension g and $\Lambda \subseteq V$ is a lattice of rank $2g$. (More precisely, we take $V = \operatorname{Hom}(\Omega^1(A), \mathbb{C})$ dual to the space $\Omega^1(A)$ of holomorphic 1-forms and $\Lambda = H_1(A, \mathbb{Z})$.) Then every isogeny of complex abelian varieties $V/\Lambda \to V'/\Lambda'$ is defined by a $\mathbb{C}$-linear isomorphism $V \to V'$ such that $\varphi(\Lambda) \subseteq \Lambda'$, and

$$\ker\varphi = \varphi^{-1}(\Lambda')/\Lambda \cong \Lambda'/\varphi(\Lambda). \tag{2.1.1}$$

This is such a convenient description! We seek to replicate it over an arbitrary field k, and Tate modules allow us to consider (separable) isogenies in an analogous way.

We can begin linearizing, as in the introduction, by working with a torsion subgroup $A[n]$—but instead of working with just one, to complete the analogy we package them together, as follows.

Let $\ell \neq p$ be prime. The ℓ-adic Tate module of A is the projective limit

$$T_\ell A := \varprojlim_j A[\ell^j](k^{\mathrm{sep}}) \simeq \mathbb{Z}_\ell^{2g}. \tag{2.1.2}$$

Concretely, an element of $T_\ell A$ is a sequence $P = (P_1, P_2, \dots)$ where $P_j \in A[\ell^j](k^{\mathrm{sep}})$ and $\ell P_j = P_{j-1}$ for all $j \geq 2$.

A homomorphism $\varphi\colon A \to A'$ induces a homomorphism $T_\ell\varphi\colon T_\ell A \to T_\ell A'$, and when φ is an isogeny, the finiteness of the kernel implies that $T_\ell\varphi$ is injective.

For complex abelian varieties (when $k = \mathbb{C}$), we recover in this way the ℓ-adic part of the description above. We have

$$A[\ell^j](\mathbb{C}) = (\ell^{-j}\Lambda)/\Lambda \cong \Lambda/\ell^j\Lambda$$

for all j, so $T_\ell A \cong \Lambda \otimes \mathbb{Z}_\ell$ is the ℓ-adic completion of Λ. An isogeny $\varphi\colon V_1/\Lambda_1 \to V_2/\Lambda_2$ induces a map of ℓ-adic Tate modules $T_\ell\varphi\colon \Lambda_1 \otimes \mathbb{Z}_\ell \to \Lambda_2 \otimes \mathbb{Z}_\ell$; and taking the ℓ-primary subgroups in (2.1.1) we see that

$$(\ker\varphi)(\mathbb{C})_\ell \cong (\Lambda_2 \otimes \mathbb{Z}_\ell)/(\varphi(\Lambda_1) \otimes \mathbb{Z}_\ell) \cong \operatorname{coker} T_\ell\varphi. \tag{2.1.3}$$

The following proposition shows that (2.1.3) extends in general.

Proposition 2.1.4. *Let $\varphi\colon A \to A'$ be an isogeny of abelian varieties with kernel H. Let $H[\ell^\infty]$ be the ℓ-primary (or ℓ-Sylow) subgroup of H. Then $H[\ell^\infty]$ is naturally isomorphic to the cokernel of $T_\ell\varphi\colon T_\ell A \to T_\ell A'$.*

Proof. Abbreviate $A_j := A[\ell^j](K^{\mathrm{al}})$. For $n, r \geq 1$, the sequence

$$0 \to A_n \to A_{n+r} \xrightarrow{\cdot\ell^n} A_r \to 0$$

is exact. The maps are compatible, so for all $r \geq 1$ and taking the limit over n, we claim that the sequence

$$0 \to T_\ell A \to \varprojlim_n A_{n+r} \to A_r \to 0$$

is exact. By left exactness of projective limits, it suffices to show the map to A_r is surjective. This map takes $(P_n)_n$ with $P_n \in A_{n+r}$ and maps to the common element $\ell P_1 = \ell^n P_n$ for all n. Hence, for any $Q = P_0 \in A_r$, a lift $(P_n)_n \in \varprojlim_n A_{n+r}$ is obtained by inductively choosing $P_n \in A_{n+r}$ satisfying $\ell P_n = P_{n-1}$ for $n \geq 1$.

Repeating the abbreviation with A' and H, we put the exact sequences together to get:

$$\begin{tikzcd} 0 \arrow[r] & T_\ell A \arrow[r] \arrow[d, "\varphi"] & \varprojlim_n A_{n+r} \arrow[r, "\cdot\ell^n"] \arrow[d, "\varphi"] & A_r \arrow[r] \arrow[d, "\varphi"] & 0 \\ 0 \arrow[r] & T_\ell A' \arrow[r] & \varprojlim_n A'_{n+r} \arrow[r, "\cdot\ell^n"] & A'_r \arrow[r] & 0 \end{tikzcd} \tag{2.1.5}$$

We now apply the snake lemma. The kernel of the middle vertical map is 0 since $\ker\varphi$ is finite, so we obtain the exact sequence

$$0 \to H_r \xrightarrow{\delta} T_\ell A'/\varphi(T_\ell A) \to \varprojlim_n A'_{n+r}/\varprojlim_n \varphi(A_{n+r}). \tag{2.1.6}$$

(To be explicit, the map δ is defined as follows: for $P = P_r \in H_r$, inductively choose $P'_n \in A_{n+r}$ for $n \geq 1$ such that $\ell P'_n = P'_{n-1}$ and take $\delta(P) = (\dots, \varphi(P'_r), \varphi(P'_{r+1}), \dots) \in T_\ell A'$.)

Now we take $r \geq 1$ to be such that $\ell^r = \#H_\infty$; then $H_r = H_\infty$. To finish, we need to check that the final map in (2.1.6) is the zero map. Indeed, the class of $(Q_n)_n \in T_\ell A' \leq \prod_n A'_n$ maps to the class of $(Q_n)_n \in \prod_n A'_{n+r}$, so we want to show for all $n \geq 1$ and all $Q_n \in A'_n$ that $Q_n = \varphi(P'_n)$ for some $P'_n \in A_{n+r}$. But $\deg \phi = \ell^r$ so there exists an isogeny $\psi\colon A' \to A$ such that $\ell^r = \varphi\psi$; therefore, if $P_n \in A_{n+r}$ is such that $\ell^r P_n = Q_n$ then $P'_n := \psi(P_n)$ has $\varphi(P'_n) = \ell^r P_n = Q_n$ and since $\ell^{n+r} P_n = \ell^n Q_n = O$ we have $\ell^{n+r} P'_n = \psi(\ell^{n+r} P_n) = O$ and so $P'_n \in A_{n+r}$ as desired.

Finally, the connecting isomorphism δ is natural, because the snake lemma is natural. □

Example 2.1.7. Consider the case $g = 1$, so $A = E$ is an elliptic curve. Choose a basis $P_1 = (P_{1,n})_n$, $P_2 = (P_{2,n})_n$ for $T_\ell E$. Consider the isogeny $\varphi\colon E \to E'$ with kernel $H = H_\ell = \langle P_{1,1} \rangle$. That is, E' is the quotient $E/\langle P_{1,1}\rangle$. Then it is straightforward to verify that $P'_1 := (\varphi(P_{1,n+1}))_n$ and $P'_2 := (\varphi(P_{2,n}))_n$ is a basis for $T_\ell E'$.

As in the proof of Proposition 2.1.4, we compute the isomorphism $\delta\colon H \xrightarrow{\sim} \operatorname{coker}(T_\ell\varphi)$, both groups isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. We lift $P_{1,1}$ to $(P_{1,2}, P_{1,3} \dots) \in T_\ell E$; so $\delta(P_{1,1})$ is the class of $(\varphi(P_{1,n+1}))_n = P'_1 \in T_\ell E'$ in $\operatorname{coker}(T_\ell\varphi)$.

2.2. **Duals.** Associated naturally to A is the dual abelian variety $A^\vee := \mathbf{Pic}^0_A$. More precisely, the relative Picard functor $\underline{\operatorname{Pic}}_A$, which associates to a k-scheme S the group $\operatorname{Pic}(A \times_k S)$, is represented by a group scheme $\mathbf{Pic}_A$ over k, and $\mathbf{Pic}^0_A$ is the connected component containing the identity (the structure sheaf $\mathscr{O}_A$) [Kle14, section 3]. The group $\operatorname{Pic}^0(A) = \mathbf{Pic}^0_A(k)$ consists of those line bundles $\mathscr{L}$ on A such that $t_P^*\mathscr{L}_{k^{\mathrm{al}}} \simeq \mathscr{L}_{k^{\mathrm{al}}}$ for all $P \in A(k^{\mathrm{al}})$.

Over the complex numbers $k = \mathbb{C}$, the dual admits a concrete description. For $A(\mathbb{C}) \simeq V/\Lambda$ where $V \simeq \mathbb{C}^g$, let

$$V^* := \operatorname{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C}) \tag{2.2.1}$$

be the $\mathbb{C}$-vector space of $\mathbb{C}$-*antilinear* functionals: that is, $f \in V^*$ means $f\colon V \to \mathbb{C}$ is an $\mathbb{R}$-linear map such that $f(ax) = \overline{a}x$ for all $x \in V$ and $a \in \mathbb{C}$. (Antilinear functionals come naturally out of Hermitian forms, where one component is $\mathbb{C}$-linear but the other is $\mathbb{C}$-antilinear.) The imaginary part of the evaluation map

$$\begin{aligned} V^* \times V &\to \mathbb{C} \\ (f, x) &\mapsto \operatorname{Im} f(x) \end{aligned} \tag{2.2.2}$$

defines a canonical, nondegenerate, $\mathbb{R}$-bilinear form. The dual of Λ under this pairing, namely

$$\Lambda^* := \{f \in V^* : \operatorname{Im} f(x) \subseteq \mathbb{Z}\} \subseteq V^* \tag{2.2.3}$$

is a lattice and

$$A^\vee(\mathbb{C}) \simeq V^*/\Lambda^*. \tag{2.2.4}$$

So in simple linear algebraic terms, the dual abelian variety is obtained from the dual lattice (with respect to (2.2.2)).

Example 2.2.5. Suppose $E = V/\Lambda$ with $V = \mathbb{C}$ and $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$, so $\omega_1 = \tau$, $\omega_2 = 1$ is a $\mathbb{Z}$-basis for Λ. Then $V^* = \mathbb{C}e$ where $e(x) = \overline{x}$, and it is straightforward to compute that a $\mathbb{Z}$-basis for Λ^* is $\omega_1^* = e/\operatorname{Im}(\overline{\tau})$, $\omega_2^* = -\tau e/\operatorname{Im}(\overline{\tau}) = \tau e/\operatorname{Im}(\tau)$.

Put a bit more abstractly, $A^\vee(\mathbb{C}) = \mathbf{Pic}^0_A(\mathbb{C})$ is the kernel of the map

$$\mathrm{Pic}(A) \simeq H^1(A, \mathscr{O}_A^\times) \to H^2(A, \mathbb{Z}), \tag{2.2.6}$$

the boundary map in the long exact sequence in cohomology induced by the exponential sequence

$$0 \to \mathbb{Z} \to \mathscr{O}_A \to \mathscr{O}_A^\times \to 1$$

(where $\mathbb{Z}$ is the constant sheaf) arising from $s \mapsto \exp(2\pi i s)$ for a section s of $\mathscr{O}_A$. For further details, see Mumford [Mum70, section II.9] or Swinnerton-Dyer [SD74, §8].

The universal line bundle $\mathscr{P}$ on $A \times A^\vee$ of the functor represented by $\mathbf{Pic}^0_A$ is called the Poincaré bundle: a point $Q \in A^\vee$ by definition gives a line bundle $\mathscr{L}_Q$ up to isomorphism, and $\mathscr{P}|_{A\times\{Q\}} \simeq \mathscr{L}_Q$. The bundle $\mathscr{P}$ furthermore gives rise to a natural isomorphism [Mum70, Corollary, p. 132]

$$\begin{aligned} i_A \colon A &\to (A^\vee)^\vee \\ P &\mapsto \mathscr{P}|_{\{P\}\times A^\vee}. \end{aligned} \tag{2.2.7}$$

A homomorphism $\varphi \colon A \to A'$ of abelian varieties induces a dual homomorphism

$$\varphi^\vee \colon (A')^\vee \to A^\vee$$

by pullback of line bundles, i.e. $\varphi^\vee := \varphi^* \colon \mathbf{Pic}^0_{A'} \to \mathbf{Pic}^0_A$. If φ is an isogeny, then so is $\varphi^\vee$. For an isogeny of complex abelian varieties $\varphi \colon V_1/\Lambda_1 \to V_2/\Lambda_2$ so $\varphi(\Lambda_1) \subseteq \Lambda_2$, the pullback

$$\begin{aligned} \varphi^\vee \colon V_2^*/\Lambda_2^* &\to V_1^*/\Lambda_1^* \\ f &\mapsto \varphi^*(f) = f \circ \varphi \end{aligned} \tag{2.2.8}$$

indeed gives $\varphi^\vee(\Lambda_2^*) \subseteq \Lambda_1^*$, and we now have $\ker \varphi^\vee = \Lambda_1^*/\varphi^\vee(\Lambda_2^*)$.

Example 2.2.9. For $\varphi \colon E \to E'$ an isogeny of elliptic curves, we recover the dual isogeny $\varphi^\vee \colon \mathbf{Pic}^0(E') \to \mathbf{Pic}^0(E)$ by restricting the pullback map $Q \mapsto \sum_{P\in\varphi^{-1}(Q)} Q$ [Sil09, §III.6] (taking classes), then applying the canonical isomorphism $E \cong \mathbf{Pic}^0(E)$ and the same with E'.

2.3. Weil pairing.

Recall that a finite-dimensional vector space and its dual admit a tautological perfect pairing. There is an analogous pairing as follows.

Theorem 2.3.1 (Tautological Weil pairing)**.** *Let $n \in \mathbb{Z}_{>0}$ be coprime to the characteristic of k. Then there is a canonical perfect, bilinear pairing*

$$\langle\cdot,\cdot\rangle_n \colon A[n] \times A^\vee[n] \to \mu_n, \tag{2.3.2}$$

compatible with the action of Gal_k.

We call (2.3.2) the tautological Weil pairing. This pairing is an expression of *Cartier duality* (for torsion in abelian varieties), and it is equivalently expressed by a canonical isomorphism

$$\beta_n \colon A^\vee[n] \xrightarrow{\sim} \mathrm{Hom}(A[n], \mu_n), \tag{2.3.3}$$

Proof of Theorem 2.3.1. For a detailed proof and properties of the pairing, see Oda [Oda69, Theorem 1.1]. See also Antieau–Auel [AA21, §2.2].

A definition of the pairing (2.3.2) follows along similar lines as in the case of elliptic curves [Sil09, §III.8]: see Mumford [Mum70, p. 184–185] or Hindry–Silverman [HS00, Exercise A.7.8]. Given $Q \in A^\vee[n](k^{\mathrm{al}})$ corresponding to $\mathscr{L} = \mathscr{L}_Q \simeq \mathscr{O}(D)$, we will construct a map $A[n](k^{\mathrm{al}}) \to \mu_n(k^{\mathrm{al}})$ as follows. By assumption, both $\mathscr{L}^{\otimes n}$ and $[n]^*\mathscr{L}$ are trivial, and therefore $nD = \operatorname{div}(f)$ and $[n]^*D = \operatorname{div}(g)$ for some $f = f_Q, g = g_Q \in k^{\mathrm{al}}(A)^\times$. Since

$$\operatorname{div}(f \circ [n]) = [n]^*(nD) = n([n]^*D) = n \operatorname{div}(g) = \operatorname{div}(g^n),$$

the functions $f \circ [n]$ and g^n differ by a scalar constant. Now for all $X \in A(k^{\mathrm{al}})$ and $P \in A[n](k^{\mathrm{al}})$, we have $(f \circ [n])(X + P) = (f \circ [n])(X)$, and therefore $g^n(X + P)/g^n(X) = 1$ and $g(X + P)/g(X)$ is constant, independent of X (but may depend on Q). Thus, we obtain a map

$$\begin{aligned} \beta_n \colon A[n](k^{\mathrm{al}}) &\to \mu_n \\ P &\mapsto \frac{g(X+P)}{g(X)} \end{aligned} \tag{2.3.4}$$

(for any choice of $X \in A(k^{\mathrm{al}})$ such that $g(X)$ and $g(X + P)$ are defined and nonzero), and

$$\langle P, Q\rangle_n = g_Q(P)/g_Q(X + P)$$

completing the definition of the pairing. □

For ℓ prime different from $\operatorname{char} k$, the pairing with $n = \ell^j$ is compatible with the multiplication-by-ℓ map, so together they yield a perfect bilinear pairing on ℓ-adic Tate modules:

$$\langle \cdot, \cdot \rangle \colon T_\ell A \times T_\ell A^\vee \to \mu_{\ell^\infty}(k^{\mathrm{al}}) \simeq \mathbb{Z}_\ell.$$

Given an isogeny $\varphi \colon A \to A'$ with $\ker \varphi \subseteq A[n]$, comparing the left- and right-kernels of the tautological Weil pairing yields a canonical perfect pairing

$$\ker \phi \times \ker \phi^\vee \to \mu_n. \tag{2.3.5}$$

Finally, it will be significant to the proceeding investigation of Galois actions that the Weil pairing is equivariant with respect to the action of $\mathrm{Gal}_k := \mathrm{Gal}(k^{\mathrm{sep}} \,|\, k)$, where Gal_k acts on μ_n by the mod n cyclotomic character ε_n (see Lemma 4.4.1): that is, for all $\sigma \in \mathrm{Gal}_k$ and all $P \in A(k^{\mathrm{al}})$ and $Q \in A^\vee(k^{\mathrm{al}})$, we have

$$\langle \sigma(P), \sigma(Q)\rangle = \langle P, Q\rangle^\sigma = \varepsilon_n(\langle P, Q\rangle). \tag{2.3.6}$$

2.4. **Polarizations.** If $\mathscr{L}$ is an ample line bundle on A, then the morphism

$$\begin{aligned} \varphi_{\mathscr{L}} \colon A &\to A^\vee \\ P &\mapsto \tau_P^*\mathscr{L} \otimes \mathscr{L}^{-1} \end{aligned} \tag{2.4.1}$$

is an isogeny, where $\tau_P \colon A \to A$ is the translation by P map, defined by $Q \mapsto Q + P$. (By contrast, note that if $\mathscr{L} \in \operatorname{Pic}^0(A)$, then (2.4.1) is the zero map.) This observation motivates the following definition.

Definition 2.4.2. An isogeny $\lambda \colon A \to A^\vee$ is a polarization if there is a finite separable field extension $K \supset k$ and an ample line bundle $\mathscr{L}$ on A_K so that $\lambda_K = \varphi_{\mathscr{L}}$.

A polarization λ is principal if it is an isomorphism, in which case we say that A is principally polarized by λ.

Polarizations can also be identified among isogenies over the ground field k: they are the isogenies $\lambda \colon A \to A^\vee$ where the line bundle $(\mathrm{id}, \lambda)^*\mathscr{P}$ on A is ample and λ is symmetric, meaning that $\lambda^\vee \circ i_A = \lambda$. Given such an isogeny $\lambda \colon A \to A^\vee$, the line bundle $\mathscr{L}$ as in

Definition 2.4.2 can be constructed, after a possible finite base change, as a bundle satisfying the relation $[2]^*\mathscr{L} \simeq ((\mathrm{id}, \lambda)^*\mathscr{P})^2$ [Mum70, Theorem 2, p. 188].

Over the complex numbers, the existence of a polarization distinguishes abelian varieties among complex tori. Indeed, an ample line bundle on $A(\mathbb{C}) = V/\Lambda$ is specified by a positive definite Hermitian form $H\colon V \times V \to \mathbb{C}$ such that $E := \operatorname{Im} H$ has $E(\Lambda, \Lambda) \subseteq \mathbb{Z}$ (more generally, see the Appell–Humbert theorem for a linear-algebraic description of line bundles on A). The restriction $E|_\Lambda\colon \Lambda \times \Lambda \to \mathbb{Z}$ is alternating, and so there exists a $\mathbb{Z}$-basis of Λ in which the Gram matrix is

$$[E] = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}$$

where $D = \operatorname{diag}(d_1, \ldots, d_g)$ is diagonal with $d_i \geq 1$. Then $\ker \lambda \simeq (\mathbb{Z}/d_1\mathbb{Z})^2 \oplus \cdots \oplus (\mathbb{Z}/d_g\mathbb{Z})^2$, and so λ is principal if and only if $d_1 = \cdots = d_g = 1$.

Example 2.4.3. Elliptic curves are always principally polarized. We follow (2.4.1). For $\mathscr{L} = \mathscr{O}(D)$,

$$\tau_P^*\mathscr{L} \otimes \mathscr{L}^{-1} \simeq \mathscr{O}(\tau_{-P}(D)) \otimes \mathscr{O}(-D) \simeq \mathscr{O}(\tau_{-P}(D) - D). \tag{2.4.4}$$

Now let $D = [O]$ be the origin (divisor of degree 1); then $\tau_{-P}([O]) - [O] = [-P] - [O] \sim [O] - [P]$, since $[P] + [-P] \sim 2[O]$. Plugging back in,

$$\tau_P^*\mathscr{L} \otimes \mathscr{L}^{-1} \simeq \mathscr{O}([O] - [P]). \tag{2.4.5}$$

Unfortunately, this is the *negative* of the natural isomorphism $\kappa\colon E \xrightarrow{\sim} E^\vee$ given by $P \mapsto [P] - [O]$ [Sil09, §III.6], and does not define a polarization—the sign is caused by moving between line bundles and divisors.

Example 2.4.6. If C is a smooth, projective, geometrically integral curve (a so-called *nice* curve) of genus g over k with $C(k) \neq \emptyset$, then its Jacobian $J := \mathbf{Pic}^0(X)$ is principally polarized by the theta divisor $\Theta \subset J$, the translate under the isomorphism $J \cong \mathbf{Pic}_C^{g-1}$ of the image of the natural morphism $\operatorname{Sym}^{g-1} C \to \mathbf{Pic}_C^{g-1}$. More generally, see Milne [Mil86b, section 1].

There is a second natural morphism $J \to J^\vee$, which is the inverse of the pullback morphism $j^*\colon J^\vee \to J$ induced by the inclusion $j\colon C \hookrightarrow J$. Again, there is a negative sign relating the two: $\varphi_{\mathscr{O}(\Theta)} = -(j^*)^{-1}$ [Mil86b, Lemma 6.9].

Now let $\lambda\colon A \to A^\vee$ be a polarization. Then we can plug it into the tautological Weil pairing, giving a (possibly degenerate) bilinear pairing on $A[n]$:

$$\begin{aligned} \langle \cdot, \cdot \rangle_{n,\lambda}\colon A[n] \times A[n] &\to \mu_n \\ (P, Q) &\mapsto \langle P, \lambda(Q) \rangle_n \end{aligned} \tag{2.4.7}$$

Taking λ the principal polarization in Example 2.4.3, we recover the usual formula for the Weil pairing [Sil09, section III.8] (noting how the sign is compensated for).

3. Approach to Galois action computations

Our results depend on analyzing the Galois action on torsion subgroups of certain abelian surfaces that are isogenous to products of elliptic curves. We are able to characterize the Galois action on the elliptic curves, which is comparatively well-understood, and then use the fact that isogenous abelian varieties have conjugate Galois representations to analyze the abelian surfaces in question. In this section, we explain what we mean by this, first in categorical terms and then in terms of matrices, suitable for computation. (We found it very helpful, as is often the case in linear algebra, to have both the commutative diagrams and the explicit matrices.)

In section 3.1, we begin by showing an example of how to conjugate the Galois action of an elliptic curve to find the action on the torsion of an isogenous curve. In sections 3.2 and 3.3, we develop a formal categorical framework for our methods, and show that the choices of basis necessary for our computations are equivalent to choosing a functor we will call a *computation functor*. The remaining sections are devoted to showing examples of how these choices can be made. Section 3.4 examines common presentations of isogenies, and section 3.5 addresses polarizations and dual isogenies. The reader may wish to skip ahead to the next section and flip back to this section as needed.

Throughout, let k be a field with characteristic $p \geq 0$.

3.1. **A guiding example.** We begin with a simple example computing the Galois action on the ℓ-torsion of an elliptic curve that is isogenous to a curve whose Galois structure is known. This example is instructive in revealing what concerns must be addressed in a general approach.

Let E be an elliptic curve over k and let $\ell \neq p$ be a prime number. Let $\varphi \colon E \to E'$ be a cyclic isogeny with the choice of basis $P_1, P_2 \in T_\ell E$ as in Example 2.1.7. We suppose that the point $P_{1,1} \in E[\ell](k)$ generating the kernel is a k-rational point, so the isogeny φ is defined over k as well. Let $\sigma \in \mathrm{Gal}_k$. Then $\sigma P_{1,1} = P_{1,1}$ and $\sigma P_{2,1} = b_1 P_{1,1} + d_1 P_{2,1}$ for some $b_1, d_1 \in \mathbb{F}_\ell$ with $d_1 \neq 0$, so the action of σ on $E[\ell]$ in this basis is given by

$$\begin{pmatrix} 1 & b_1 \\ 0 & d_1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_\ell).$$

(We are taking the column convention; the row convention is also used, see [RSZB+22, Remark 2.1].)

We now compute the action of σ on a basis for $E'[\ell]$ consisting of images of points under φ. In Example 2.1.7 we use the basis $P_1' := \{\varphi(P_{1,n+1})\}_n$, $P_2' := \{\varphi(P_{2,n})\}$ for $T_\ell E'$, so we may take our basis for $E'[\ell]$ to be $P_{1,1}' = \varphi(P_{1,2})$ and $P_{2,1}' = \varphi(P_{2,1})$. Note that it is not possible to choose points in $E[\ell]$ whose images under φ are a basis for $E'[\ell]$; we must choose at least one of the points in E to be ℓ^2-torsion. To determine the action of σ on $P_{1,1}'$, we need to know the action of σ on $P_{1,2}$. The action of σ on $E[\ell^2]$ is given by $\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})$, where

$$\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \equiv \begin{pmatrix} 1 & b_1 \\ 0 & d_1 \end{pmatrix} \pmod{\ell}.$$

If we write $P_{2,2}' := \varphi(P_{2,2})$, then we have

$$\begin{aligned} \sigma P_{1,1}' &= \varphi(\sigma P_{1,2}) = \varphi(a_2 P_{1,2} + c_2 P_{2,2}) = 1P_{1,1}' + c_2 P_{2,2}', \\ \sigma P_{2,1}' &= \varphi(\sigma P_{2,1}) = \varphi(b_1 P_{1,1} + d_1 P_{2,1}) = d_1 P_{2,1}'. \end{aligned} \tag{3.1.1}$$

We know that $c_2 = \ell c'$ for some $c' \in \mathbb{F}_\ell$, and $c_2 P_{2,2}' = c' P_{2,1}'$. The action of σ on $E'[\ell]$ is thus given by

$$\begin{pmatrix} 1 & 0 \\ c' & d_1 \end{pmatrix}.$$

It is interesting to see how the matrix giving the action of σ on $E'[\ell]$ differs from the one giving the action on $E[\ell]$: it is lower rather than upper triangular. Both b_1 and b_2 do not appear, but c_2 does have an effect. Although it is possible to find a point of $E'[\ell]$ fixed by σ, the point one might solve for has dependence on c' and d_1, which will vary as σ does, meaning that $E'[\ell]$ need not have any k-points. We will see similar changes to Galois actions of isogenous abelian surfaces in the proof of Theorem 1.2.1.

Now that we see how that goes, we reinterpret the above by thinking of it as obtained from a *change of basis* on the ℓ-adic modules, so we can find the action on the image basis by conjugating the action as follows:

$$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\begin{pmatrix} 1/\ell & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_2 & \ell b_2 \\ c_2/\ell & d_2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ c' & d_1 \end{pmatrix} \pmod{\ell}. \tag{3.1.2}$$

We have arrived at the same answer, but we have not yet explained where the conjugating matrix came from, nor have we defined the setting for this conjugation. We justify this calculation in the next section.

3.2. **From isogenies to Tate modules.** Let A_0 be a (fixed) abelian variety over k of dimension g. Let $\varphi\colon A_0 \to A$ be an isogeny. Given the action of the Galois group on $T_\ell A_0$, we may determine the action on $T_\ell A$ by identifying it with a sublattice of $V_\ell A_0 := T_\ell A_0 \otimes \mathbb{Q}_\ell$. This approach also facilitates comparing the Galois actions on more than one quotient of A_0.

In this section, we describe this as a functor from isogenies to sublattices. Since our goal is to give a framework for computing the Galois action on torsion points of any order prime to $p = \operatorname{char} k$, we simultaneously keep track of all ℓ-adic Tate modules where $\ell \neq p$ as follows. Let

$$\widehat{\mathbb{Z}}' := \prod_{\ell \neq p} \mathbb{Z}_\ell \tag{3.2.1}$$

be the prime-to-p profinite completion of $\mathbb{Z}$. We define the (prime-to-p) adelic Tate module of A by

$$\widehat{T}'A := \varprojlim_{\substack{n \\ p\nmid n}} A[n](k^{\mathrm{sep}}) \simeq \prod_{\ell \neq p} T_\ell A. \tag{3.2.2}$$

Then $\widehat{T}'A$ is a free $\widehat{\mathbb{Z}}'$-module of rank $2g$. Let $\widehat{V}'A := \widehat{T}'A \otimes_{\mathbb{Z}} \mathbb{Q}$ be the (prime-to-p) adelic Tate representation of A.

Remark 3.2.3. When $p \neq 0$, we could also augment the adelic Tate module with a component at p using the Dieudonné module. (Our application is in characteristic 0.)

In order to introduce the category that keeps track of isogenies $\varphi\colon A_0 \to A$, we will use the following general categorical construction. Given a category and a particular choice of object, we may form a new category where we restrict our attention to morphisms into (resp. out of) that object, called a slice (resp. coslice) category.

Example 3.2.4. Let CRing be the category of commutative rings under ring homomorphisms, and let R be an object of CRing, i.e., a commutative ring. Then the objects and morphisms of the coslice category of CRing under R, denoted CRing^R, are R-algebras and R-algebra homomorphisms.

A natural way to form the category we are interested in is to first consider a category whose objects are abelian varieties and whose morphisms are isogenies, and then take the coslice category for A_0.

Let $\mathcal{I} = \mathsf{AbVar}'_k$ be the category whose objects are abelian varieties over k and whose morphisms are isogenies (over k) with degree prime to p. The objects of the coslice category of $\mathcal{I}$ under A_0, denoted $\mathcal{I}^{A_0}$, are isogenies whose domain is A_0; the morphisms of this coslice category are commuting triangles of isogenies:

$$\begin{tikzcd} & A_0 \arrow[dl, "(\varphi)"'] \arrow[dr, "(\psi)"] & \\ A \arrow[rr, "f"'] & & B. \end{tikzcd} \tag{3.2.5}$$

Since the objects and morphisms of $\mathcal{I}^{A_0}$ are both given by isogenies, we use parentheses to distinguish objects.

Remark 3.2.6. In a coslice category, the identity morphism on the fixed object is an initial object of the coslice category.

Next we define the category of sublattices, where we will compute Galois actions.

Let $\mathcal{T}_{A_0}$ be the category whose objects are $\widehat{\mathbb{Z}}'$-lattices of rank $2g$ contained in $\widehat{V}'A_0$ and whose morphisms are injective maps of lattices in $\widehat{V}'A_0$:

$$\begin{tikzcd} T \arrow[rr, hook] \arrow[dr, hook] & & T' \arrow[dl, hook'] \\ & \widehat{V}'A_0 & \end{tikzcd} \tag{3.2.7}$$

We consider only injections of lattices in $\mathcal{T}_{A_0}$ since, as discussed in section 2.1, isogenies induce injective maps between Tate modules. We now define the functor Ψ, which shows how Tate modules of isogenous quotients of A_0 are identified with sublattices of $\widehat{V}'A_0$.

For any $(\varphi)\colon A_0 \to A \in \operatorname{Ob}\mathcal{I}^{A_0}$, we have the injective $\widehat{\mathbb{Z}}'$-linear map $\widehat{T}'\varphi\colon \widehat{T}'A_0 \hookrightarrow \widehat{T}'A$ and the isomorphism $\widehat{V}'\varphi\colon \widehat{V}'A_0 \xrightarrow{\sim} \widehat{V}'A$. We define the sublattice of $\widehat{V}'A_0$ associated with $\widehat{T}'A$ via φ to be $\Psi(\varphi) := (\widehat{V}'\varphi)^{-1}(\widehat{T}'A)$, which is the image of $\widehat{T}'A$ in $\widehat{V}'A_0$ under the dotted arrow in the following commutative diagram:

$$\begin{tikzcd} \widehat{T}'A_0 \arrow[r, hook, "\widehat{T}'\varphi"] \arrow[d, hook, "\otimes\mathbb{Q}"'] & \widehat{T}'A \arrow[d, hook, "\otimes\mathbb{Q}"] \arrow[dl, dashed] \\ \widehat{V}'A_0 \arrow[r, "\sim", "\widehat{V}'\varphi"'] & \widehat{V}'A. \end{tikzcd} \tag{3.2.8}$$

We write the ℓ-adic part of $\Psi(\varphi)$ as $\Psi_\ell(\varphi)$.

For any morphism f in $\mathcal{I}^{A_0}$ as in (3.2.5), we may form the commutative diagram (3.2.9). $\Psi(\varphi)$ and $\Psi(\psi)$ are the images of $\widehat{T}'A$ and $\widehat{T}'B$ under the dotted arrows, and we define $\Psi f\colon \Psi(\varphi) \to \Psi(\psi)$ to be the map given by the image of $\widehat{T}'f$ in $\widehat{V}'A_0$ via those dotted arrows.

$$\begin{tikzcd}
\widehat{T}'A_0 \arrow[r, hook, "\widehat{T}'\varphi"] \arrow[d, hook, "\otimes\mathbb{Q}"] & \widehat{T}'A \arrow[r, hook, "\widehat{T}'f"] \arrow[d, hook, "\otimes\mathbb{Q}"] \arrow[dl, hook, dashed] & \widehat{T}'B \arrow[d, hook, "\otimes\mathbb{Q}"] \arrow[dll, hook, dashed] \\
\widehat{V}'A_0 \arrow[r, "\sim", "\widehat{V}'\varphi"'] & \widehat{V}'A \arrow[r, "\sim", "\widehat{V}'f"'] & \widehat{V}'B
\end{tikzcd} \tag{3.2.9}$$

The functoriality of Ψ is a consequence of the functoriality of $\widehat{T}'$ and $\widehat{V}'$ acting on $\mathcal{I}$. Since (id_{A_0}) is initial in $\mathcal{I}^{A_0}$, each submodule of $\widehat{V}'A_0$ in the image of Ψ is an overlattice of $\widehat{T}'A_0 = \Psi(\mathrm{id}_{A_0})$, via the injection $\Psi\varphi$.

Remark 3.2.10. The categories in this section were chosen for their convenience in providing a useful setting for Galois actions. However, one might ask about the properties of the functor Ψ, which is closely related to the functors $\widehat{T}'$ and $\widehat{V}'$. Since $\widehat{T}'$ is a faithful functor, so is Ψ. However, Ψ is not full in general; lattice morphisms that are not invariant under Gal_k cannot be in its image. If we restrict morphisms in $\mathcal{T}_{A_0}$ to Galois equivariant ones, then fullness of Ψ is equivalent to the Tate conjecture. The essential image of Ψ consists of the sublattices of $\widehat{V}'A_0$ that originate from an isogeny. The interested reader may wish to compare our setting with [Lan13, §1.3.5.2], where the author gives an *equivalence* of categories relating isogenies $A_0 \to A$ to subgroups of $\widehat{V}'A_0$, working over an algebraically closed field.

3.3. **From Tate modules to group representations.** In this section we will define functors, which we call computation functors, that map from isogenies to the category we will use to keep track of the Galois action on the adelic Tate module. These functors factor through the functor Ψ defined in the previous section, so we may think of them as attaching the Galois representations of the lattices given by Ψ. After defining this formalism, we will reexamine the example from section 3.1 from this new point of view.

The categorical setting for our computations is as follows. We abbreviate $G := \mathrm{Gal}_k$.

Definition 3.3.1. Fix $W := \prod_{\ell \neq p} W_\ell$, a free $\widehat{\mathbb{Z}}'$-module of rank $2g$. The objects in the category RepMat_G are $\widehat{\mathbb{Z}}'$-representations $\rho := \prod_{\ell \neq p} \rho_\ell$ where $\rho_\ell \colon G \to \prod_{\ell \neq p} \mathrm{Aut}_{\mathbb{Z}_\ell}(W_\ell)$. A morphism $\gamma \colon \rho \to \rho'$ in RepMat_G consists of, for each $\ell \neq p$, a $\mathbb{Z}_\ell$-linear map $\gamma_\ell \colon W_\ell \to W_\ell$ that is G-equivariant, satisfying $\gamma_\ell \circ \rho_{\ell,\sigma} = \rho'_{\ell,\sigma} \circ \gamma_\ell$ for any $\sigma \in G$. Composition of morphisms is given by composition of $\mathbb{Z}_\ell$-module maps for each ℓ.

A computation functor $F \colon \mathcal{I}^{A_0} \to \mathrm{RepMat}_G$ assigns each isogenous quotient $A_0 \to A$ to a Galois representation of $\widehat{T}'A$ in the following manner:

Definition 3.3.2. For each object $(\varphi) \colon A_0 \to A$ in $\mathcal{I}^{A_0}$, choose an isomorphism $\Psi(\varphi) \simeq W$.

The Galois action on $\widehat{V}'A_0$ restricts to a map $G \to \prod_{\ell \neq p} \mathrm{Aut}_{\mathbb{Z}_\ell}(\Psi(\varphi))$ via the containment $\Psi(\varphi) \subseteq \widehat{V}'A_0$. Then we obtain the object $F(\varphi) \in \mathrm{RepMat}_G$ by conjugating the maps in $\mathrm{Aut}_{\mathbb{Z}_\ell}(\Psi(\varphi))$ with the isomorphism $\Psi(\varphi) \simeq W$.

For any morphism $f \colon (\varphi) \to (\psi)$ (see (3.2.5)), given $F(\varphi)$ and $F(\psi)$, Ff is determined by the map Ψf between the lattices $\Psi(\varphi)$ and $\Psi(\psi)$. We define it to be the composition

$$Ff \colon W \simeq \Psi(\varphi) \overset{\Psi f}{\hookrightarrow} \Psi(\psi) \simeq W, \tag{3.3.3}$$

which satisfies $Ff_\ell \circ F(\varphi)_{\ell,\sigma} = F(\psi)_{\ell,\sigma} \circ Ff_\ell$ for any $\ell \neq p$ and $\sigma \in G$. That is, Ff is an intertwiner mapping between the representations $F(\varphi)$ and $F(\psi)$.

The definition of F ensures that it is a functor, and it naturally factors through Ψ.

Remark 3.3.4. In our definition of a computation functor F, Ff is determined by $F(\varphi)$ and $F(\psi)$. Similarly, $F(\varphi)$ and Ff, which implicitly contains a choice of isomorphism $\Psi(A) \simeq W$, determine $F(\psi)$, which is the conjugation of $F(\varphi)$ by Ff; although the $\mathbb{Z}_\ell$-module maps comprising Ff may not be invertible as $\mathbb{Z}_\ell$ module maps, they may still be inverted as $\mathbb{Q}_\ell$-module maps, allowing us to compute:

$$F(\psi)_\sigma = Ff \circ F(\varphi)_\sigma \circ Ff^{-1}. \tag{3.3.5}$$

Since (id_{A_0}) is initial in $\mathcal{I}^{A_0}$, for any object $(\varphi) \in \mathcal{I}^{A_0}$, we may obtain the Galois representation $F(\varphi)$ by conjugating $F(\mathrm{id}_{A_0})$, which is the Galois representation of $\widehat{T}' A_0$, with $F\varphi$.

Our overall goal is to compute Galois actions on isogenous abelian varieties, which are conjugate to one another. Making the choices of basis necessary to perform these matrix computations is equivalent to choosing a computation functor. Since we are usually interested in a few specific isogenous abelian varieties, we often need only consider how we might choose a computation functor acting on a finite diagram in $\mathcal{I}^{A_0}$. In the remainder of section 3, we will consider choosing computation functors in different situations.

Example 3.3.6. We will now revisit Example 2.1.7 by considering it in terms of choosing (part of) a computation functor $F\colon \mathcal{I}^E \to \mathrm{RepMat}_G$. We restrict our attention to ℓ-adic rather than adelic Tate modules since φ acts identically at other primes, and consider the Galois representations acting on $W_\ell := \mathbb{Z}_\ell^{\oplus 2}$.

We identify $T_\ell E$ with W_ℓ via the choice of basis vectors $P_1, P_2 \in T_\ell E$. Let $\sigma \in G$. Its action on $T_\ell E$, i.e. $F(\mathrm{id}_E)_\sigma$, is given by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) \text{ where } a, b, c, d \in \mathbb{Z}_\ell,\ a_1 = 1 \text{ and } c_1 = 0.$$

We identify $T_\ell E'$ with W_ℓ via the choice of basis vectors $Q_1, Q_2 \in T_\ell E'$. Given this choice of isomorphism and recalling that $T_\ell\varphi(P_1) = \ell Q_1$and $T_\ell\varphi(P_2) = Q_2$, the transformation

$$\begin{aligned} F\varphi\colon W_\ell \simeq T_\ell E &\hookrightarrow T_\ell E' \simeq W_\ell \\ e_1 \mapsto P_1 &\mapsto T_\ell\varphi(P_1) = \ell Q_1 \mapsto \ell e_1 \\ e_2 \mapsto P_2 &\mapsto T_\ell\varphi(P_2) = Q_2 \mapsto e_2 \end{aligned}$$

is given by the matrix $\left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Finally, we may determine $F(\varphi)$ by the following change of basis computation, where we are inverting $F\varphi$ by considering it as a map over $\mathbb{Q}_\ell$:

$$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{1}{\ell} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \ell b \\ \frac{1}{\ell} c & d \end{pmatrix}.$$

Despite the presence of the fraction $\frac{1}{\ell}$ in the action we computed, this outcome is still an element of $\mathrm{GL}_2(\mathbb{Z}_\ell)$: since $c_1 = 0$, $\frac{1}{\ell} c = \{c_{n+1}\}_n$ is an element of $\mathbb{Z}_\ell$. If we truncate this action to find the element of $\mathrm{GL}(\mathbb{F}_\ell)$ giving the action of σ on $E'[\ell]$, we recover the action calculated in Example 2.1.7.

3.4. **Producing change of basis matrices.** In the previous section, we defined computation functors, whose data includes choices of basis necessary for our computations of Galois actions. In this section, we will discuss practical methods for choosing those bases in two common situations, and apply them to some example isogenies between elliptic curves.

Let $\varphi\colon A_0 \to A$ be an isogeny. We want to choose a computation functor acting on φ. In particular, we need a choice of basis for $\Psi(\varphi)$ for each $\ell \neq p$ as well as the action of φ relative to that basis. Fix W a free $\widehat{\mathbb{Z}}'$-module of dimension $2g$. We want a map as in (3.3.3):

$$F\varphi\colon W \simeq \widehat{T}'A_0 \overset{\Psi\varphi}{\hookrightarrow} \Psi(\varphi) \simeq W. \tag{3.4.1}$$

We consider the following two common situations:

(1) Isogenies $\varphi\colon A_0 \to A_0$.
(2) Isogenies which are given $\ker\varphi$.

Case (1)*: Endomorphisms.* In this situation, we may choose the bases for the Tate modules of both the domain and codomain of our isogeny the same way. Then, given a choice of basis for $\widehat{T}'A_0$, we observe that $F\varphi$ factors through $\widehat{T}'A_0$ as follows:

$$\begin{tikzcd}
F\varphi\colon W \simeq \widehat{T}'A_0 \arrow[rr, hook, "\Psi\varphi"] \arrow[dr, hook, "\widehat{T}'\varphi"'] & & \Psi(\varphi) \simeq W. \\
& \widehat{T}'A_0 \arrow[ur, dashed, "\simeq"'] &
\end{tikzcd} \tag{3.4.2}$$

We may choose $\Psi(\varphi) \simeq W$ so that the isomorphism $W \simeq \widehat{T}'A_0$ on the left and the composition $\widehat{T}'A_0 \dashrightarrow \Psi(\varphi) \simeq W$ are both the identifications given by our choice of basis.

Consequently, in this situation the matrix giving (3.4.1) is simply the same as the matrix giving the map $\widehat{T}'\varphi\colon \widehat{T}'A_0 \to \widehat{T}'A_0$ with this choice of basis. We can already see this observation in action in Example 3.3.6 if we consider φ as a map $E \to E$. A multiplication map is shown in the following example.

Example 3.4.3. Let E/k be an elliptic curve and $\ell \neq p$ a prime. Fix a basis for $T_\ell E$. Consider the multiplication map $[\ell]\colon E \to E$. The matrix for $T_\ell[\ell]\colon T_\ell E \to T_\ell E$ is the following:

$$\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}.$$

If φ is a homothety, as in the above example, the base change of a representation is exactly the same since conjugating by such a matrix has no effect.

Case (2)*: Kernels.* The kernel of an isogeny identifies it up to isomorphism. In diagram (3.2.9), if f is an isomorphism between $\varphi\colon A_0 \to A$ and $\psi\colon A_0 \to B$, then $\widehat{V}'f^{-1}(\widehat{T}'B) = \widehat{T}'A$ and so $\Psi(\varphi) = \Psi(\psi)$. Given $H := \ker(\varphi)(k^{\mathrm{sep}})$, we first examine $\Psi(\varphi)$ and then give a recipe for choosing $F\varphi\colon F(\mathrm{id}_{A_0}) \to F(\varphi)$.

Lemma 3.4.4. *The following statements hold.*

(a) *If $H \subseteq A_{0,k^{\mathrm{sep}}}[m]$, then $\Psi(\varphi) \subseteq \frac{1}{m}\widehat{T}'A_0 \subseteq \widehat{V}'A_0$.*
(b) *Moreover, $\Psi(\varphi)$ is the unique sublattice of $\frac{1}{m}\widehat{T}'A_0$ where $m(\Psi(\varphi)/\widehat{T}'A_0)$ is canonically identified with H.*

Proof. (a) We may construct an isogeny $f\colon A \to A_0$ so that $f \circ \varphi = [m]$. We see from (3.2.9) in the case where $\psi = [m]$ that $\Psi([m])$ is an overlattice of $\Psi(\varphi)$ inside $\widehat{V}'A_0$. Furthermore, if we consider the diagram (3.2.8) in the case $\varphi = [m]$, $\Psi([m]) = \frac{1}{m}\widehat{T}'A_0 \subseteq \widehat{V}'A_0$.

(b) It suffices to prove the result on the ℓ-primary sublattice for each $\ell \mid \#H$. Let ℓ be a prime with ℓ^n the highest power dividing m, and $H_\ell := H \cap A_0[\ell^n]$.

We have $T_\ell A_0 \subseteq \Psi_\ell(\varphi) \subseteq \frac{1}{\ell^n}T_\ell A_0$, and isomorphisms

$$\Big(\frac{1}{\ell^n}T_\ell A_0\Big)/T_\ell A_0 \xrightarrow{\cdot \ell^n} T_\ell A_0/\ell^n T_\ell A_0 \xrightarrow{\sim} A_0[\ell^n],$$

where the second map is the canonical isomorphism given by projection $T_\ell A_0 \to A_0[\ell^n]$, which factors through the quotient $T_\ell A_0/\ell^n T_\ell A_0$. Thus, we will write this as $[x] \mapsto x_n$, where $x = \{x_m\}_m \in T_\ell A_0$.

We also have $\Psi_\ell(\varphi)/T_\ell A_0 \leqslant \left(\frac{1}{\ell^n}T_\ell A_0\right)/T_\ell A_0$, so

$$\ell^n(\Psi_\ell(\varphi)/T_\ell A_0) = \ell^n\Psi_\ell(\varphi)/\ell^n T_\ell A_0 \leqslant T_\ell A_0/\ell^n T_\ell A_0,$$

and we claim that the canonical isomorphism above restricts to an isomorphism

$$\ell^n\Psi_\ell(\varphi)/\ell^n T_\ell A_0 \xrightarrow{\sim} H_\ell.$$

First, we will demonstrate that the image of the restriction is contained in H_ℓ by showing that for any $x \in \ell^n\Psi_\ell(\varphi)$, $x_n \in \ker\varphi$, i.e. $\varphi(x_n) = 0$. Since $T_\ell\varphi(x) = \{\varphi(x_m)\}_m$, we have that $\varphi(x_n) = T_\ell\varphi(x)_n$. Also, we can write $x = \ell^n y$ for some $y \in (V_\ell\varphi)^{-1}(T_\ell A)$, since $x \in \ell^n\Psi_\ell(\varphi)$. Now,

$$T_\ell\varphi(x) = T_\ell\varphi(\ell^n y) = \ell^n V_\ell\varphi(y).$$

Since $V_\ell\varphi(y) \in T_\ell A$, this means $T_\ell\varphi(x) \in \ell^n T_\ell A$. This implies $T_\ell\varphi(x)_n = \varphi(x_n) = 0$, as desired.

Next, we show that the image of the restriction is all of H_ℓ. Let $y \in H_\ell$, and choose a lift $\tilde{y} = \{\tilde{y}_m\}_m \in T_\ell A_0$, so $\tilde{y}_n = y$. If we write

$$\tilde{y} = \ell^n\Big(\frac{1}{\ell^n}\tilde{y}\Big)$$

with $\frac{1}{\ell^n}\tilde{y} \in \frac{1}{\ell^n}T_\ell A_0 \subseteq V_\ell A_0$, we must show that $\frac{1}{\ell^n}\tilde{y} \in \Psi_\ell(\varphi)$. Using the fact that $\varphi(\tilde{y}_n) = \varphi(y) = 0$ and $\ell\tilde{y}_{m+1} = \tilde{y}_m$, we check that

$$(V_\ell\varphi)\Big(\frac{1}{\ell^n}\tilde{y}\Big) = \frac{1}{\ell^n}(T_\ell\varphi)(\tilde{y}) = \frac{1}{\ell^n}(\varphi(\tilde{y}_m))_m = \frac{1}{\ell^n}\cdot\ell^n\{\varphi(\tilde{y}_{n+1}), \varphi(\tilde{y}_{n+2}), \ldots\} \in T_\ell A.$$

Therefore, $\frac{1}{\ell^n}\tilde{y} \in \Psi_\ell(\varphi)$, as desired.

Thus, we have canonically identified $\ell^n(\Psi_\ell(\varphi)/T_\ell A_0) \cong H_\ell$, hence $m(\Psi(\varphi)/\widehat{T}'A_0) \cong H$. □

Remark 3.4.5. Recall from Proposition 2.1.4 that for an isogeny $\varphi\colon A_0 \to A$ of abelian varieties with kernel H, there is an isomorphism between H and the cokernel of $\widehat{T}'\varphi\colon \widehat{T}'A_0 \to \widehat{T}'A$. The isomorphism in Lemma 3.4.4(b) can also be deduced from this perspective.

Construction 3.4.6. We now show a general method for choosing a basis for $\Psi(\varphi)_\ell$, given $H := \ker\varphi$. First we choose a minimal generating set for H_ℓ, lift this generating set to elements of $\Psi_\ell(\varphi)$, and then complete it to a basis. The results in Lemma 3.4.4 give some guidance on how we can make those choices.

Let $P_1, \dots P_{2g}$ be a basis for $T_\ell A_0$, and let $P_{i,j}$ denote the restriction of P_i to its ℓ^j-torsion part. Then it is possible to write a minimal generating set for $H_\ell := H \cap A_0[\ell^n]$ as a $\mathbb{Z}/\ell^n\mathbb{Z}$-module in terms of linear combinations of $P_{1,n}, \dots, P_{2g,n}$ with coefficients in $\{0, 1, \dots, \ell^n - 1\}$. If $a_1 P_{1,n} + \dots + a_{2g} P_{2g,n}$ is one of the generators for H_ℓ, then for any choice of lifts $\tilde{a}_i \in \mathbb{Z}_\ell$ of a_i, we have the following lift to $\Psi_\ell(\varphi)$:

$$\frac{\tilde{a}_1}{\ell^n} P_1 + \dots + \frac{\tilde{a}_{2g}}{\ell^n} P_{2g} \in \frac{1}{\ell^n} T_\ell A_0. \tag{3.4.7}$$

The element (3.4.7) is in $\Psi_\ell(\varphi)$ by Lemma 3.4.4(b): it is contained in $\frac{1}{\ell^n} T_\ell A_0$ and if we consider the element $\ell^n(\frac{\tilde{a}_1}{\ell^n} P_1 + \dots + \frac{\tilde{a}_{2g}}{\ell^n} P_{2g} + T_\ell A_0) \in \ell^n(\Psi_\ell(\varphi)/T_\ell A_0)$, we recover $a_1 P_{1,n} + \dots + a_{2g} P_{2g,n}$.

Since the generating set for H is minimal, a lift of the generating set to $\Psi(\varphi)$ must be linearly independent. To find a basis for $\Psi_\ell(\varphi)$, we begin by choosing a lift of each element of H to $\Psi_\ell(\varphi)$. It is possible to choose the remaining basis vectors to be linear combinations of $P_1, \dots, P_{2g}$ with coefficients in $\{0, 1, \dots, \ell^n - 1\}$.

Moreover, if we wish to choose the action of a computation functor $F \colon \mathcal{I}^{A_0} \to \mathrm{RepMat}_G$ on $\varphi \colon (\mathrm{id}_{A_0}) \to (\varphi)$ in terms of the basis $P_1, \dots, P_{2g}$ of $\Psi(\mathrm{id}_{A_0})$, then the coefficients of $P_1, \dots, P_{2g}$ in a basis of $\Psi(\varphi)$ give the columns of the change of basis matrix corresponding to $F\varphi_\ell^{-1}$.

We now show the basis selection of $\Psi(\varphi)$ in Example 3.3.6 in terms of this construction.

Example 3.4.8. Let $\varphi \colon E \to E'$ be the isogeny of elliptic curves given by Example 2.1.7 where P_1, P_2 is a basis for $T_\ell E$ and $\ker(\varphi) = \langle P_{1,1} \rangle$.

The exponent of $\ker \varphi$ is ℓ and $\{P_{1,1}\}$ is a minimal generating set. We may lift the coefficient 1 of $P_{1,1}$ to $1 \in \mathbb{Z}_\ell$, which gives us $\frac{1}{\ell} P_1 \in \Psi_\ell(\varphi)$. However, $\frac{1}{\ell} P_1$ on its own is not a basis for $\Psi_\ell(\varphi)$. A natural choice for a second basis element is P_2, giving the following matrix, which is the inverse of the $F\varphi_\ell$ we chose in Example 3.3.6:

$$\begin{pmatrix} \frac{1}{\ell} & 0 \\ 0 & 1 \end{pmatrix}.$$

In fact any combination $c_1 P_1 + c_2 P_2$ with $c_1, c_2 \in \{0, 1, \dots, \ell - 1\}$ that is linearly independent from $\frac{1}{\ell} P_1$ will work as a choice of second basis vector.

3.5. **Change of basis matrices for polarizations and duals.** In this section, we look at how to choose a computation functor acting on isogenies that are polarizations or are dual to isogenies where we have already chosen how the functor acts. We first recall some facts about constructing polarizations, discuss generally how to apply our computational methods, and then show an example of a pushforward of the principal polarization on an elliptic curve.

Given a polarization $\lambda_0 \colon A_0 \to A_0^\vee$ associated with an ample line bundle L (cf. Definition 2.4.2), we may construct other polarizations.

Definition 3.5.1. Let $f\colon A \to A_0$ be an isogeny. The pullback of λ_0 by f is the composition $f^*\lambda_0 := f^\vee \circ \lambda_0 \circ f$ shown below. It is a polarization associated with the line bundle f^*L.

$$\begin{tikzcd}
A \arrow[r, "f^*\lambda_0"] \arrow[d, "f"'] & A^\vee \\
A_0 \arrow[r, "\lambda_0"] & A_0^\vee \arrow[u, "f^\vee"']
\end{tikzcd}$$

Definition 3.5.2. Let $g\colon A_0 \to A$ be an isogeny so that $\ker(g)$ is isotropic under the pairing given by λ_0, and let d be the minimum value so that $\ker(g) \subseteq \ker(d\lambda_0)$. The pushforward of λ_0 by g is the map $g_*\lambda_0$ filling in the following diagram, which is a polarization [Mum70, Corollary, p. 231].

(3.5.3)
$$\begin{tikzcd}
A_0 \arrow[r, "d\lambda_0"] \arrow[d, "g"'] & A_0^\vee \\
A \arrow[r, "g_*\lambda_0"] & A^\vee \arrow[u, "g^\vee"']
\end{tikzcd}$$

The value of d in the definition of the pushforward of a polarization divides the exponent e_g of g since $A_0[e_g] \subseteq \ker(e_g\lambda_0)$.

Definition 3.5.4. For a polarization λ_0 whose degree is coprime to p, we say it has type $D := (d_1, \dots, d_g)$, where the $d_i \in \mathbb{N}$ are the unique values such that $d_i \mid d_{i+1}$ and there is a group isomorphism $\ker(\lambda_0) \simeq (\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_g\mathbb{Z})^2$.

Given the type D of a polarization λ_0 on a complex variety A_0, we may choose a symplectic basis for its underlying torus and the dual basis for $A_0^\vee$ so that the following matrix gives $\widehat{V}'\lambda_0\colon \widehat{V}'A_0 \to \widehat{V}'A_0^\vee$, where D denotes the diagonal matrix with entries given by the type [BL04, §3.1]:

(3.5.5)
$$\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}.$$

This matrix also gives the Weil pairing on $\widehat{T}'A_0$ associated with the polarization.

Working over k, if we are given the type of a polarization, we may choose the action of a computation functor $F\colon \mathcal{I}^{A_0} \to \mathrm{RepMat}_G$ on $\lambda_0\colon (\mathrm{id}_{A_0}) \to (\lambda_0)$ analogously, as shown in the next example.

Example 3.5.6. Let $\lambda_0\colon A_0 \to A_0^\vee$ be a polarization with type $(d_1, \dots, d_g)$ and let $\ell \neq p$ a prime. Let $D_\ell := (\ell^{n_1}, \dots, \ell^{n_g})$, where ℓ^{n_i} is the highest power of ℓ dividing d_i. We may choose a (symplectic) basis for $T_\ell A_0$ and the dual basis for $T_\ell A_0^\vee$ so that $F\lambda_{0,\ell}$ is given by the matrix

$$\begin{pmatrix} 0 & D_\ell \\ -D_\ell & 0 \end{pmatrix}.$$

If λ_0 is a principal polarization on an elliptic curve, then for any $\ell \neq p$, we may choose the matrix for $F\lambda_{0,\ell}$ to be

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

If λ_0 is a $(1,3)$-polarization on an abelian surface (we will see $(1,\ell)$-polarizations in section 4.1), we may choose $F\lambda_{0,3}$ so it is given by the following matrix:

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \\ -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \end{pmatrix}.$$

Next, let $f\colon A \to B$ and suppose we have Ff and wish to next choose how the computation functor F acts on the dual isogeny $f^\vee\colon B^\vee \to A^\vee$.

We may identify $\widehat{V}'A^\vee, \widehat{V}'B^\vee$ with the dual vector spaces of $\widehat{V}'A, \widehat{V}'B$ at each ℓ; the dual of a basis for $\widehat{T}'A \subset \widehat{V}'A$ gives a basis for $\widehat{T}'A^\vee$. With these choices, for any ℓ, the matrix giving $Ff_\ell^\vee$ is the transpose of that for Ff_ℓ. In the following example, we compute the pullback and pushforward of a principal polarization on an elliptic curve.

Example 3.5.7. Let $\varphi\colon E \to E'$ be the cyclic isogeny introduced in Example 2.1.7. Assume that the basis P_1, P_2 for $T_\ell E$ is symplectic, so that, given the principal polarization $\lambda_0\colon E \to E^\vee$, we may choose $F\lambda_0$ so that $F\lambda_{0,\ell} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, as shown in Example 3.5.6.

To compute the pullback of λ_0 by φ, we use the equality $F(\varphi^*\lambda_0) = F\varphi^\vee \circ F\lambda_0 \circ F\varphi$ from Definition 3.5.1, and so $F(\varphi^*\lambda_0)_\ell$ is given by the following matrix:

$$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \ell \\ -\ell & 0 \end{pmatrix}.$$

We see that the pullback $\varphi^*\lambda_0$ is the ℓ-th power of the principal polarization on E.

Now, we may compute the pushforward of λ_0 by φ since the kernel of φ is isotropic under the pairing given by λ_0. As ℓ is the smallest value so that $\ker(\varphi) \subseteq \ker(\ell\lambda_0)$, we have the following equality from Definition 3.5.2: $F(\ell\lambda_0) = F\varphi^\vee \circ F(\varphi_*\lambda_0) \circ F\varphi$. Thus, $F(\varphi_*\lambda_0)_\ell$ is given by the following matrix:

$$\left(\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}^T\right)^{-1} \begin{pmatrix} 0 & \ell \\ -\ell & 0 \end{pmatrix} \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{\ell} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \ell \\ -\ell & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\ell} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thus, the pushforward $\varphi_*\lambda_0$ is a principal polarization on the elliptic curve E'.

4. Constructions and computations

In this section, we prove Theorem 1.2.1. We begin with the construction of the abelian surfaces A in the theorem. We then use the technical tools developed in section 3 to compute the Galois action on $A[\ell]$ and on $A^\vee[\ell]$ by comparing $T_\ell A$ and $T_\ell A^\vee$ inside $V_\ell A_0$ for A_0 a third abelian surface isogenous to both A and $A^\vee$. We also confirm that the result agrees with the twisted contragredient action discussed in the introduction (see (1.1.5)). Finally, we give the proof of our main theorem.

4.1. **Construction of the abelian surfaces.** Let k be a field with absolute Galois group $\mathrm{Gal}_k := \mathrm{Gal}(k^{\mathrm{sep}} \,|\, k)$ and let $\ell \neq \operatorname{char} k$ be prime. Recalling the introduction, a necessary but not sufficient condition for $A[\ell] \not\simeq A^\vee[\ell]$ is that every polarization on A has degree divisible by ℓ. We produce abelian surfaces satisfying this condition by gluing together two (non-isogenous) elliptic curves along a subgroup of order ℓ. There are many references for this construction. For example it is described on MathOverflow [CP10], implicitly suggested as an exercise [Gor02, Exercise 6.35], and even recently exhibited [BS23, Theorem 2.5]. We present a brief account, for completeness. We do not give the most general construction but address in section 4.7 how it can be generalized.

Construction 4.1.1. Let E_1 and E_2 be elliptic curves over k and let $P \in E_1[\ell](k)$ and $Q \in E_2[\ell](k)$ be k-rational ℓ-torsion points. Let

$$G := \langle (P, Q) \rangle \leqslant E_1 \times E_2 \quad \text{and} \quad A := (E_1 \times E_2)/G,$$

with the quotient map $q \colon E_1 \times E_2 \to A$.

In section 4.6, we will use Construction 4.1.1 in the proof of Theorem 1.2.1.

Lemma 4.1.2. *With setup as in Construction 4.1.1, the following statements hold.*

(a) *A is an abelian surface over k with a $(1, \ell)$-polarization over k.*
(b) *For a field extension $k' \supseteq k$, if there is no isogeny $E_1 \to E_2$ over k', then any polarization on A over k' has degree divisible by ℓ.*

Proof. Part (a) follows since G is defined over k, and A obtains a $(1, \ell)$-polarization λ from the pushforward under q (cf. definition 3.5.2) of the principal product polarization λ_0 on $E_1 \times E_2$.

Next, part (b). Without loss of generality, we may replace k by k'. Let $\lambda \colon A \to A^\vee$ be a polarization (over k) of degree d^2. Consider the pullback $q^*\lambda$, a polarization on $E_1 \times E_2$. The composition $\phi := \lambda_0^{-1} \circ q^*\lambda \in \operatorname{End}(E_1 \times E_2)$ is an endomorphism of degree $(\ell d)^2$, fixed under the Rosati involution. Since E_1 and E_2 are not isogenous, we have

$$\operatorname{End}(E_1 \times E_2) \simeq \operatorname{End}(E_1) \times \operatorname{End}(E_2).$$

The ring of Rosati-fixed endomorphisms of an elliptic curve is $\mathbb{Z}$ (if the elliptic curve has complex multiplication, the Rosati involution acts by complex conjugation), so $\phi = (d_1, d_2)$ with $d_1, d_2 \in \mathbb{Z}_{>0}$ satisfying $d_1 d_2 = \ell d$. Since ϕ factors through q, we have the containment $\ker q \subseteq \ker \phi = E_1[d_1] \times E_2[d_2]$.

Now suppose that $\ell \nmid d$. Without loss of generality, $\ell \mid d_1$ and $\ell \nmid d_2$, which implies that, under projection onto the E_2 factor, $\ker q$ projects to the trivial subgroup in $E_2[d_2]$. But this is a contradiction, since by construction $\ker q$ projects to a nontrivial subgroup under projection to both E_1 and E_2. □

Over number fields, we can exhibit infinitely many generic instances of Construction 4.1.1 as follows. We begin with the elliptic curves.

Lemma 4.1.3. *Let $\ell \leqslant 7$ be prime and let K be a number field. There exist infinitely many elliptic curves E over K with $P \in E[\ell](K)$.*

Proof. Recall that the modular curve $Y_1(\ell)$ parametrizes isomorphism classes of pairs (E, P) where E is an elliptic curve and $P \in E[\ell](K)$, and that $Y_1(\ell) \subseteq X_1(\ell)$ is an open subscheme. Then the statement follows from the fact that we have $X_1(\ell) \simeq \mathbb{P}^1$ for these values of ℓ, classically known. More precisely, there are infinitely many j-invariants in K with $j \neq 0, 1728$ such that any elliptic curve E over K with $j(E) = j$ has an ℓ-torsion point $P \in E[\ell](K)$. □

4.2. **Background on Hilbert irreducibility.** We pause to give a very quick review of the Hilbert irreducibility theorem: we will give references, but for the purposes of our argument we can treat it as a black box.

Let K be a number field and let

$$f_t(x) = f(t_1, ..., t_n; x) \in K(t_1, ..., t_n)[x]$$

be an irreducible polynomial of degree d. The coefficients of $f_t(x)$ are simultaneously defined on a nonempty open subset $U \subseteq \mathbb{A}^n_K$ (avoiding denominators).

Theorem 4.2.1 (The Hilbert irreducibility theorem (HIT))**.** *There are infinitely many points $a = (a_1, \ldots, a_n) \in U(K)$ such that the specialization $f_a(x) = f(a_1, ..., a_n; x) \in K[x]$ is irreducible of degree d.*

Proof. See Serre [Ser97, sections 9.2, 9.6] or [Ser92, Chapter 3], or Lang [Lang83, Chapter 9]. □

In fact, the set of points $(a_1, ..., a_n) \in U(K) \subseteq K^n$ such that $f_a(x)$ is irreducible has density 1, when ordered by height. More precisely, a subset $S \subseteq K^n$ is thin if

$$A \subseteq V(K) \cup \bigcup_{i=1}^{r} \phi_i(W_i(K))$$

where $V \subsetneq \mathbb{A}^n_K$ is a proper subvariety, and $\phi_i \colon W_i \to \mathbb{A}^n$ is a dominant rational map with $\dim(W_i) = n$ and $\deg(\phi_i) \geq 2$ for all $i = 1, \ldots, r$. The conclusion of Theorem 4.2.1 holds for $a \in U(K)$ away from a thin set; and precise understanding of the thin set of exceptions gives a way to quantify the error term in counting good specializations by height.

Example 4.2.2. Consider $f_t(x) = x^3 - x + t$. Then $f_a(x)$ is irreducible for $a \in \mathbb{Q}$ if and only if $a \neq b^3 - b$ for $b \in \mathbb{Q}$ (a thin set of type II, arising from the map $\mathbb{A}^1 \to \mathbb{A}^1$ by $b \mapsto b^3 - b$).

Remark 4.2.3. More generally, the fields K such that $\mathbb{A}^1(K)$ is not thin (and therefore $V(K)$ is not thin for every irreducible quasi-projective variety over K) are called Hilbertian fields.

The classical application of Corollary 4.2.4 is to the study of Galois groups, so much so that often it is this corollary that is referred to as HIT. Recall that $f_t(x)$ has a *generic* Galois group $G \leq S_d$ over the field $K(t_1, \ldots, t_n)$, obtained by the permutation action on the roots of $f_t(x)$ in an algebraic closure of $K(t) = K(t_1, \ldots, t_n)$.

Corollary 4.2.4. *Suppose that $f_t(x)$ has Galois group $G \leq S_d$ over $K(t)$. Then for all $a \in U(K)$ outside of a thin set, the specialization $f_a(x) \in K[x]$ has Galois group $G \leq S_d$ over K.*

Proof. The set of points where the Galois group is smaller is defined by polynomial conditions, and so lies in a thin set: see e.g. Serre [Ser92, Proposition 3.3.5]. For further treatment, see also Serre [Ser97, Chapter 10], Saltman [Sal82], or more recently Wittenberg [Wit24, section 1]. □

Corollary 4.2.4 can be understood geometrically, as follows. Let $X \to U$ be a generically finite étale morphism with X irreducible; concretely, X is described by the equation $f(t_1, \ldots, t_n; x) = 0$ in $U \times \mathbb{A}^1$. (The converse holds by the primitive element theorem.) Then the Hilbert irreducibility theorem says that for points $u \in U(K)$ outside of a thin set, the fiber X_u is irreducible over K. For the corollary, without loss of generality we suppose that

$X \to U$ is generically Galois with $G := \mathrm{Gal}(K(X) \,|\, K(U))$ the Galois group over the generic point. Then outside of a thin set in $U(K)$, the fiber $X_u \to \operatorname{Spec} K$ is also a G-Galois cover.

It is from this final perspective that we will apply the Hilbert irreducibility theorem: we will construct infinitely many abelian surfaces from elliptic curves with certain specified Galois image, and we will do so by specialization after computing the generic Galois group over a universal family. For more general results, see recent work of Zywina [Zyw23], who studies families of abelian varieties with large Galois image in an effective manner.

We will need to apply Corollary 4.2.4 under multiple specializations: we will want not just that there are infinitely many G-extensions, but for these to be as disjoint as possible. It is of course enough to do this pairwise, so we consider the fiber product

$$X \times_k X \to U \times_k U.$$

Concretely, this corresponds to the polynomial $f_t(x) f_u(x) \in K(t_1, \dots, t_n, u_1, \dots, u_n)[x]$ introducing new transcendentally independent elements. In particular, the generic Galois group is naturally a subgroup of $G \times G$.

Proposition 4.2.5. *Let $X \to U$ be a Galois cover with generic Galois group G. Let $L \supseteq K$ be the algebraic closure of K in $K(X)$; let*

$$G_0 := \mathrm{Gal}(L \,|\, K) \simeq \mathrm{Gal}(L(U) \,|\, K(U)),$$

and let $\pi \colon G \to G_0$ be the restriction map. Then $\mathrm{Gal}(K(X \times X) \,|\, K(U \times U))$ is equal to

$$G \times_{G_0, \pi} G := \{(\sigma_1, \sigma_2) : \pi(\sigma_1) = \pi(\sigma_2)\}.$$

Proof. We obtain a diagram of covers

$$\begin{tikzcd} & X \times X \arrow[dl] \arrow[dr] & \\ X \times U \arrow[dr] & & U \times X \arrow[dl] \\ & U \times U & \end{tikzcd}$$

where the bottom vertical maps are G-extensions. The corresponding field diagram has a compositum on top. Let $K' := K(X \times U) \cap K(U \times X)$. By the fundamental theorem of Galois theory, we have

$$\mathrm{Gal}(K(X \times X) \,|\, K(U \times U)) = \{(\sigma_1, \sigma_2) \in G \times G : (\sigma_1)|_{K'} = (\sigma_2)|_{K'}\} \leqslant G \times G.$$

So we need to prove that $K' = L(U \times U)$.

We recall that if k is an algebraically closed field, and A and B are k-algebras that are domains, then $A \otimes_k B$ is a domain (see e.g. Milne [Mil12, Proposition 4.15]). In fact, it is enough for k to be algebraically closed in A and B. Since X is irreducible, we conclude that $L(X \times X) \supseteq L(U \times U)$ is the compositum of two linearly disjoint extensions isomorphic to $L(X) \supseteq L(U)$; therefore $K' \subseteq L(U \times U)$. But of course $K' \supseteq L$ so $K' = L(U \times U)$. □

4.3. **Computation of the Galois action on A.** Let A be an abelian surface over $\mathbb{Q}$ as in Construction 4.1.1 with (E_1, P) and (E_2, Q) satisfying $P \in E_1[\ell](\mathbb{Q})$ and $Q \in E_2[\ell](\mathbb{Q})$. To understand the action of the Galois group on $A[\ell]$, we use the image of the Galois action on $T_\ell(E_1 \times E_2)$, along with a choice of basis for $\Psi(q) \subset V_\ell(E_1 \times E_2)$, as explained in Remark 3.3.4.

Here and in subsequent sections we use the computational ideas outlined in section 3. In our example of interest, the isogenies all have degrees which are powers of ℓ, so we need only consider the ℓ-adic portion of the Tate modules in question. In particular, we will be interested in the mod ℓ representation, which we obtain by reducing modulo ℓ the Tate module.

Lemma 4.3.1. *Let $\ell \leqslant 7$ be prime. Then the following statements hold.*

(a) *For (E,P) such that $[(E,P)] \in Y_1(\ell)(\mathbb{Q}) \subset \mathbb{P}^1$, the image of the ℓ-adic Galois representation*

$$\rho_{E,\ell} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell(E)(\mathbb{Q}^{\mathrm{al}})) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is contained in

$$\left\{ \begin{pmatrix} a & b \\ \ell c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_\ell) : a, d \in \mathbb{Z}_\ell^\times, a \equiv 1 \bmod \ell \right\} \leqslant \mathrm{GL}_2(\mathbb{Z}_\ell) \tag{4.3.2}$$

in any basis P_1, P_2 for $T_\ell(E)$ such that $P_1 \bmod \ell = P$. In particular,

$$\bar{\rho}_{E,\ell} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell](\mathbb{Q}^{\mathrm{al}})) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

has image contained in

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{F}_\ell) : d \in \mathbb{F}_\ell^\times \right\} \leqslant \mathrm{GL}_2(\mathbb{F}_\ell).$$

(b) *Outside of a thin set in $Y_1(\ell)(\mathbb{Q})$, the image $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is the entire subgroup in* (4.3.2).

Since $\mathbb{Q}$ is Hilbertian, when $[E_t] \in Y_1(\ell)(\mathbb{Q}) \subseteq \mathbb{P}^1$ are ordered by the height of $t \in \mathbb{P}^1$, the conclusion of Lemma 4.3.1(b) holds for a density 1 subset.

Proof. Part (a) follows by a direct calculation.

Part (b) follows from Hilbert irreducibility, Corollary 4.2.4. Recall that we summarized this result in section 4.2, but we can make the application precise in this case as follows: if the image of the Galois representation is $H \leqslant \mathrm{GL}_2(\mathbb{Z}_\ell)$, a group smaller than the one given, then there exists a (possibly branched) cover $Y_H \to Y_1(\ell)$ of degree ≥ 2 where Y_H is the associated modular curve (see Deligne–Rapoport [DR73, IV-3.1] or Rouse–Zureick-Brown [RZB15, section 2]) such that $[(E,P)] \in Y_1(\ell)(\mathbb{Q})$ lifts to $Y_H(\mathbb{Q})$. There are finitely many minimal such $H \leqslant \mathrm{GL}_2(\mathbb{Z}_\ell)$, so the errant curve lies in a thin set of $Y_1(\ell)(\mathbb{Q})$. □

Choose a basis $\{P_1, P_2, Q_1, Q_2\}$ for $T_\ell(E_1 \times E_2) \simeq \mathbb{Z}_\ell^4$ as in Lemma 4.3.1, specifically:

- $P_1 \bmod \ell = P \in E_1[\ell](\mathbb{Q})$,
- $Q_1 \bmod \ell = Q \in E_2[\ell](\mathbb{Q})$,
- $\{P_1, P_2\}$ is a symplectic basis for $T_\ell E_1$, and
- $\{Q_1, Q_2\}$ is a symplectic basis for $T_\ell E_2$.

Then the Galois action on $(E_1 \times E_2)[\ell](\mathbb{Q}^{\mathrm{al}})$ has image contained in the subgroup

$$\left\{ \begin{pmatrix} 1 & b_1 & 0 & 0 \\ 0 & d_1 & 0 & 0 \\ 0 & 0 & 1 & b_2 \\ 0 & 0 & 0 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : a_1, d_1, a_2, d_2 \in \mathbb{F}_\ell^\times \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell). \tag{4.3.3}$$

In fact, there is a further condition on elements in the image of $\bar{\rho}_{E_1 \times E_2, \ell}$, determined by the Galois equivariance of the Weil pairing. We summarize this in the following lemma.

Lemma 4.3.4. *For any elliptic curve E over $\mathbb{Q}$ and points $P, Q \in E[\ell](\mathbb{Q}^{\mathrm{al}})$, the cyclotomic character $\varepsilon_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{Z}_\ell^\times$ satisfies $\langle \bar\rho_{E,\ell}(\sigma)P, \bar\rho_{E,\ell}(\sigma)Q\rangle = \varepsilon_\ell(\sigma)\cdot\langle P, Q\rangle$, for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, where $\langle\cdot,\cdot\rangle$ is the Weil pairing. Moreover, this implies that if $\bar\rho_{E,\ell}(\sigma) = M \in \mathrm{GL}_2(\mathbb{F}_\ell)$, then $\varepsilon_\ell(\sigma) = \det M$.*

Proof. The first claim follows directly from the Galois equivariance of the Weil pairing [Sil09, section III.8]. For the second statement, let $\{P_1, P_2\}$ be a symplectic basis for $E[\ell](\mathbb{Q}^{\mathrm{al}})$, so that, as in Example 3.5.6, the Gram matrix for the Weil pairing is

$$B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then for points $P = a_1P_1 + a_2P_2$ and $Q = b_1P_2 + b_2P_2$ in $E[\ell](\mathbb{Q}^{\mathrm{al}})$, we have

$$\langle \bar\rho_{E,\ell}(\sigma)P, \bar\rho_{E,\ell}(\sigma)Q\rangle = \begin{pmatrix} a_1 & a_2 \end{pmatrix} M^T B M \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \det M \cdot \begin{pmatrix} a_1 & a_2 \end{pmatrix} B \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \det M \cdot \langle P, Q\rangle.$$

Thus, $\varepsilon_\ell(\sigma) = \det M$. □

Consequently, for our elliptic curves E_1 and E_2, $\det \bar\rho_{E_1,\ell}(\sigma) = \det \bar\rho_{E_2,\ell}(\sigma)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, so $d_1 = d_2$. Lemma 4.3.4 also holds for any ℓ^n-torsion points (or more generally on $T_\ell(E)$), and this implies that $\rho_{E_1\times E_2,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is contained in

$$G_\ell := \left\{ \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ \ell c_1 & d_1 & 0 & 0 \\ 0 & 0 & a_2 & b_2 \\ 0 & 0 & \ell c_2 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{l} a_1, d_1, a_2, d_2 \in \mathbb{Z}_\ell^\times, \\ a_1 \equiv a_2 \equiv 1 \bmod \ell, \text{ and} \\ a_1d_1 - \ell b_1c_1 = a_2d_2 - \ell b_2c_2 \end{array} \right\} \leqslant \mathrm{GL}_4(\mathbb{Z}_\ell). \tag{4.3.5}$$

We now show that there are infinitely many pairs where the image in fact surjects onto this group.

Proposition 4.3.6. *Let $\ell \leqslant 7$ be prime. There are infinitely many pairs E_1, E_2 of elliptic curves satisfying the following:*

- (a) *The image of $\rho_{E_1\times E_2,\ell}$ is the subgroup (4.3.5); in particular, there exist points $P \in E_1[\ell](\mathbb{Q})$ and $Q \in E_2[\ell](\mathbb{Q})$ of order ℓ; and*
- (b) *E_1 is not geometrically isogenous to E_2.*

Moreover, the products $E_1 \times E_2$ fall into infinitely many distinct geometric isogeny classes.

Proof. First, for $\ell = 5, 7$, there exists a universal elliptic surface $\pi_\ell \colon E_{\mathrm{univ},1}(\ell) \to Y_1(\ell)$ over $Y_1(\ell)$, equipped with (a zero section and) a section P_{univ} of order ℓ defined over $\mathbb{Q}$. For $\ell = 2$, a similar statement holds over the open subset of $Y_1(\ell)$ removing the points above $j = 0$ and $j = 1728$ (universal for elliptic curves over a base S such that j is invertible on S). For $\ell = 3$, the same is true after removing the points above $j = 0$.

To prove (a), analogous to Lemma 4.3.1(b), we now apply HIT (Corollary 4.2.4), taking the cover $(E_{\mathrm{univ},1} \times E_{\mathrm{univ},1})[\ell]$ over $Y_1(\ell) \times Y_1(\ell)$. We claim that over the generic point, the ℓ-adic Galois representation $\rho_{A_E,\ell} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{Z}_\ell)$ has image given by (4.3.5). For this, we apply Proposition 4.2.5, so we need to verify that the only constant subextension of $\mathbb{Q}(E_{\mathrm{univ},1}[\ell^\infty])$ over $\mathbb{Q}(E_{\mathrm{univ},1}) \simeq \mathbb{Q}(t)$ is $\mathbb{Q}(\zeta_\ell)$. This is indeed a constant subfield since the Galois closure contains the values $\mathbb{Q}(\zeta_\ell)$ of the Weil pairing. To show it is no larger, for each $\ell \leqslant 7$, we find two elliptic curves E_1 and E_2 over $\mathbb{Q}$ each with rational ℓ-torsion points and such that $\mathbb{Q}(E_1[\ell]) \cap \mathbb{Q}(E_2[\ell]) = \mathbb{Q}(\zeta_\ell)$. Or more conceptually, the Galois group over

$\mathbb{Q}$ is the same as that over $\mathbb{C}$, where it becomes the monodromy group; and then we note that the monodromy group of $Y(\ell)$ over $Y_1(\ell)$ is $\Gamma(\ell)/\Gamma_1(\ell) \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \simeq \mathbb{F}_\ell$, so the constant extension can be no larger by consideration of degree.

For part (b), let $E_1 \times E_2$ have large image as in (a), and suppose that E_1 is isogenous to E_2 over a number field K. Then this isogeny shows that the ℓ-adic representation $\rho_{E_{1,K},\ell}$ is conjugate to $\rho_{E_{2,K},\ell}$ (over K). Concretely, restricting the Galois representation to K, we conclude that $\rho_{(E_1\times E_2)_K,\ell}(\mathrm{Gal}_K)$ lies in a subgroup abstractly isomorphic to $\rho_{E_{1,K},\ell}(\mathrm{Gal}_K)$, a contradiction as this is a proper subgroup of G_ℓ.

The final statement follows quite a bit more generally, see Cantoral-Farfán–Lombardo–Voight [FLV23+, Proposition 6.6.1]: even for fixed E_1, the curves E_2 fall into infinitely many distinct geometric isogeny classes. We also give a simpler proof in this special case. Recall (Tate's algorithm) that E has bad potentially multiplicative reduction at p if and only if $\mathrm{ord}_p(j(E)) < 0$ has negative valuation. Let t be a parameter on $Y_1(\ell)$. We conclude in the style of Euclid: for any finite set $\{(E_i', P_i')\}_i \subset Y_1(\ell)(\mathbb{Q})$ corresponding to $t_i \in \mathbb{Q}$, we can find p such that $\mathrm{ord}_p(j(E_i')) \geq 0$ and there exists $t^* \in \mathbb{Q}$ giving $(E^*, P^*) \in Y_1(\ell)(\mathbb{Q})$ such that $\mathrm{ord}_p(j(E_{t^*})) < 0$. Indeed, this is determined by congruence conditions on the numerator and denominator, and the resulting set has positive density so intersects the density 1 subset. If (E^*, P^*) has $j(E^*) = j(t^*)$ then E^* cannot be geometrically isogenous to any E_i', since each E_i' has potentially good reduction whereas E^* has bad potentially multiplicative reduction. □

For convenience, we rewrite the elements in G_ℓ (defined in (4.3.5)) as

$$\begin{pmatrix} 1+x_1\ell & b_1+y_1\ell & 0 & 0 \\ w_1\ell & d+z_1\ell & 0 & 0 \\ 0 & 0 & 1+x_2\ell & b_2+y_2\ell \\ 0 & 0 & w_2\ell & d+z_2\ell \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \tag{4.3.7}$$

where:

- $d \in \{1, \dots, \ell-1\}$,
- $b_1, b_2 \in \{0, \dots, \ell-1\}$, and
- $w_i, x_i, y_i, z_i \in \mathbb{Z}_\ell$

still subject to the condition (Lemma 4.3.4) that

$$\det A_1 = \det A_2. \tag{4.3.8}$$

Now, we follow the recipe given in Construction 3.4.6 to write down the change of coordinates matrix for $\Psi_\ell(q) \subseteq V_\ell(E_1 \times E_2)$. Recall that $A = (E_1 \times E_2)/\langle (P, Q)\rangle$. Then the change of coordinates matrix $M_{q,\ell}$ (i.e. Fq_ℓ^{-1} for some computation functor $F\colon \mathcal{I}^{A_0} \to \mathrm{RepMat}_G$ where $A_0 := E_1 \times E_2$) is given by

$$M_{q,\ell} = \begin{pmatrix} 1 & 0 & 1/\ell & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.3.9}$$

As explained in section 3.3 (cf. Remark 3.3.4), to understand the Galois action on $A[\ell](\mathbb{Q}^{\mathrm{al}})$, we conjugate the elements (4.3.7) above by this change of coordinates matrix (i.e. we compute

$M_{q,\ell}^{-1} G_\ell M_{q,\ell}$, since $M_{q,\ell} = F q_\ell^{-1}$), which gives

$$\begin{pmatrix} 1 + x_1\ell & b_1 + y_1\ell & x_1 - x_2 & -b_2 - y_2\ell \\ w_1\ell & d + z_1\ell & w_1 & 0 \\ 0 & 0 & 1 + x_2\ell & b_2\ell + y_2\ell^2 \\ 0 & 0 & w_2 & d + z_2\ell \end{pmatrix} \tag{4.3.10}$$

with the same conditions on the variables. To get the image of $\bar{\rho}_{A,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{F}_\ell)$, we reduce this subgroup modulo ℓ, as given in the following proposition.

Proposition 4.3.11. *The image of $\bar{\rho}_{A,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{F}_\ell)$ is given by the subgroup*

$$\left\{ \begin{pmatrix} 1 & b_1 & x_1 - x_2 & -b_2 \\ 0 & d & w_1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & w_2 & d \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : \begin{matrix} d \in \mathbb{F}_\ell^\times \\ b_i, w_i, x_i \in \mathbb{F}_\ell \end{matrix} \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell).$$

Proof. We need to check that the determinant condition (4.3.8) being satisfied does not constrain our choices of variables above: it requires that

$$d + (dx_1 + z_1 - b_1w_1)\ell + (x_1z_1 - w_1y_1)\ell^2 = d + (dx_2 + z_2 - b_2w_2)\ell + (x_2z_2 - w_2y_2)\ell^2.$$

We may deduce that

$$z_1 - z_2 = b_1w_1 - b_2w_2 - dx_1 + dx_2 \in \mathbb{F}_\ell, \tag{4.3.12}$$

so for every $d \in \mathbb{F}_\ell^\times$ and $b_1, b_2, w_1, w_2, x_1, x_2 \in \mathbb{F}_\ell$, we can solve for z_1 with $z_2 = 0$ to obtain a solution to the determinant equation. □

4.4. **Computation of the Galois action on $A^\vee$ via the contragredient.** Next, we would like to compare this to the Galois action on $A^\vee[\ell](\mathbb{Q}^{\mathrm{al}})$. To do so, we make use of the following, as indicated in the introduction.

Lemma 4.4.1. *Given the representation $\bar{\rho}_{A,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell A)$, there is an isomorphism $\rho_{A^\vee,\ell} \cong \rho_{A,\ell}^* \otimes \varepsilon_\ell$, where $\rho_{A,\ell}^*$ is the dual or contragredient representation and ε_ℓ is the cyclotomic representation. In particular, there is an isomorphism $\bar{\rho}_{A^\vee,\ell^n} \cong \bar{\rho}_{A,\ell^n}^* \otimes \varepsilon_\ell$ for all $n \in \mathbb{Z}_{\geq 1}$.*

Proof. The tautological pairing $T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1)$ given by taking the inverse limit over n of the Weil pairing $A[\ell^n] \times A^\vee[\ell^n] \to \mu_{\ell^n}$ is described in section 2.3. This is a perfect bilinear pairing, hence non-degenerate, and so the result follows. □

By Lemma 4.3.4, the cyclotomic character is given by multiplication by d. Thus, when we take the inverse transpose of matrices as in Proposition 4.3.11 and scale by this factor, we get the following.

Proposition 4.4.2. *The image of $\bar{\rho}_{A^\vee,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{F}_\ell)$ is given by the subgroup*

$$\left\{ \begin{pmatrix} d & 0 & 0 & 0 \\ -b_1 & 1 & 0 & 0 \\ z_1 - z_2 & -w_1 & d & -w_2 \\ b_2 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : \begin{matrix} d \in \mathbb{F}_\ell^\times \\ b_i, w_i, x_i \in \mathbb{F}_\ell \end{matrix} \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell),$$

where $z_1 - z_2 = b_1w_1 - b_2w_2 - dx_1 + dx_2 \in \mathbb{F}_\ell$.

Proof. This proposition follows from the explanation above, but for the $(3,1)$-entry which is

$$b_1w_1 - b_2w_2 - dx_1 + dx_2 = z_1 - z_2$$

by the determinant condition (4.3.12). □

4.5. **Computation of the Galois action on $A^\vee$ via isogenies.** We give an alternate computation of the Galois action on $A^\vee[\ell](\mathbb{Q}^{\mathrm{al}})$ using the framework developed in section 3, which avoids directly using the contragredient representation. To do this, we will use the isogeny between A and $A^\vee$ given by the $(1,\ell)$-polarization λ on A of Lemma 4.1.2 to relate their Galois representations. We hope that this demonstrates the usefulness of the categorical formalism introduced in section 3.

We first observe that the polarization λ on A is the pushforward of the principal polarization λ_0 on $E_1 \times E_2$ by the quotient isogeny q (cf. Definition 3.5.2), as shown in the following commutative diagram:

(4.5.1)
$$\begin{tikzcd}
E_1 \times E_2 \arrow[r, "\ell\lambda_0"] \arrow[d, "q"] & (E_1 \times E_2)^\vee \\
A \arrow[r, "\lambda"] & A^\vee. \arrow[u, "q^\vee"']
\end{tikzcd}$$

This commutative diagram allows us to directly compare the actions of the Galois group on $T_\ell A$ and $T_\ell A^\vee$ as sublattices of $V_\ell(E_1 \times E_2)$. In terms of the framework developed in section 3, we wish to choose a computation functor $F\colon \mathcal{I}^{E_1\times E_2} \to \mathrm{RepMat}_G$ acting on the above diagram considered inside $\mathcal{I}^{E_1\times E_2}$. We have already chosen Fq_ℓ via (4.3.9) and, consequently, $F(q)_\ell$ (4.3.10), which is the Galois action on $T_\ell A$. We will now choose $F\lambda_\ell$, and conjugate $F(q)_\ell$ with it to determine $F(\lambda \circ q)_\ell$ (cf. Remark 3.3.4), which is the Galois action on $T_\ell A^\vee$. Choosing $F\lambda_\ell$ will also allow us to computationally verify that the pushforward of λ_0 by q is a $(1,\ell)$-polarization.

Since we have already chosen Fq_ℓ and $F(q)_\ell$, we may take dual bases as in section 3.5. This method leads us to choose $Fq_\ell^\vee$ to be the transpose of the matrix giving Fq_ℓ, and to choose the following matrix for $F\ell\lambda_{0,\ell}$:

$$F\ell\lambda_{0,\ell} = \begin{pmatrix} 0 & \ell & 0 & 0 \\ -\ell & 0 & 0 & 0 \\ 0 & 0 & 0 & \ell \\ 0 & 0 & -\ell & 0 \end{pmatrix}.$$

Then by (4.5.1) we have $F\ell\lambda_{0,\ell} = Fq_\ell^\vee \circ F\lambda_\ell \circ Fq_\ell$, which we rearrange to $F\lambda_\ell = (Fq_\ell^\vee)^{-1} \circ F\ell\lambda_{0,\ell} \circ Fq_\ell^{-1}$, which is:

$$F\lambda_\ell = \begin{pmatrix} 1 & 0 & 1/\ell & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^T \begin{pmatrix} 0 & \ell & 0 & 0 \\ -\ell & 0 & 0 & 0 \\ 0 & 0 & 0 & \ell \\ 0 & 0 & -\ell & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1/\ell & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \ell & 0 & 0 \\ -\ell & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

The cokernel of this matrix, which we recall from Proposition 2.1.4 is isomorphic to the kernel of λ, has ℓ^2 elements, confirming that the type of λ is $(1,\ell)$. To find $F(\lambda \circ q)_\ell$, we conjugate elements of $F(q)_\ell$ by $F\lambda_\ell$. This gives the subgroup

$$\left\{ F\lambda_\ell \begin{pmatrix} 1+x_1\ell & b_1+y_1\ell & x_1-x_2 & -b_2-y_2\ell \\ w_1\ell & d+z_1\ell & w_1 & 0 \\ 0 & 0 & 1+x_2\ell & b_2\ell+y_2\ell^2 \\ 0 & 0 & w_2 & d+z_2\ell \end{pmatrix} F\lambda_\ell^{-1} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{l} d \in \mathbb{F}_\ell^\times, \\ b_i \in \mathbb{F}_\ell, \\ w_i, x_i, y_i, z_i \in \mathbb{Z}_\ell \end{array} \right\}$$

$$= \left\{ \begin{pmatrix} d+z_1\ell & -w_1\ell & 0 & 0 \\ -b_1-y_1\ell & 1+x_1\ell & 0 & 0 \\ z_1-z_2 & -w_1 & d+z_2\ell & -w_2 \\ b_2+y_2\ell & 0 & -b_2\ell-y_2\ell^2 & 1+x_2\ell \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{l} d \in \mathbb{F}_\ell^\times, \\ b_i \in \mathbb{F}_\ell, \\ w_i, x_i, y_i, z_i \in \mathbb{Z}_\ell \end{array} \right\}$$

in $\mathrm{GL}_4(\mathbb{Z}_\ell)$. This subgroup reduces mod ℓ to the subgroup

$$\left\{ \begin{pmatrix} d & 0 & 0 & 0 \\ -b_1 & 1 & 0 & 0 \\ z_1-z_2 & -w_1 & d & -w_2 \\ b_2 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : \begin{array}{l} d \in \mathbb{F}_\ell^\times \\ b_i, w_i, z_i \in \mathbb{F}_\ell \end{array} \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell),$$

which agrees with that calculated in Section 4.4, as it should.

4.6. **Proof of the main result.** We now prove Theorem 1.2.1, which we restate for convenience.

Theorem 4.6.1. *Let $\ell \leqslant 7$ be prime. Then there exist infinitely many pairwise geometrically non-isogenous abelian surfaces A over $\mathbb{Q}$ such that $A[\ell] \not\cong A^\vee[\ell]$ as group schemes over $\mathbb{Q}$.*

Proof. Let A be an abelian surface over $\mathbb{Q}$ as in Construction 4.1.1, with the pair E_1, E_2 coming from the infinite set in Proposition 4.3.6.

Let $\sigma \in \mathrm{Gal}_\mathbb{Q}$. Then Proposition 4.3.11 gives

$$\bar{\rho}_{A,\ell}(\sigma) = \begin{pmatrix} 1 & b_1 & x_1-x_2 & -b_2 \\ 0 & d & w_1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & w_2 & d \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_\ell)$$

for some $d \in \mathbb{F}_\ell^\times$ and $b_1, b_2, x_1, x_2, w_1, w_2 \in \mathbb{F}_\ell$. Similarly, Proposition 4.4.2 gives

$$\bar{\rho}_{A^\vee,\ell}(\sigma) = \begin{pmatrix} d & 0 & 0 & 0 \\ -b_1 & 1 & 0 & 0 \\ z_1-z_2 & -w_1 & d & -w_2 \\ b_2 & 0 & 0 & 1 \end{pmatrix}$$

where

$$z_1 - z_2 = b_1w_1 - b_2w_2 - dx_1 + dx_2 \in \mathbb{F}_\ell.$$

Now, for $\ell = 2$, we check computationally that there is no $M \in \mathrm{GL}_4(\mathbb{F}_2)$ for which $M\bar{\rho}_{A,2}(\sigma)M^{-1} = \bar{\rho}_{A^\vee,2}(\sigma)$ for all $\sigma \in \mathrm{Gal}_\mathbb{Q}$; see the Magma [BCP97] code [FHV23]. Hence, these representations are not isomorphic and $A[2]$ is not isomorphic to $A^\vee[2]$ over $\mathbb{Q}$.

It remains to show that the same is true for $\ell \in \{3, 5, 7\}$. We claim that this can be seen directly from the images of the representations $\bar{\rho}_{A,\ell}$ and $\bar{\rho}_{A^\vee,\ell}$. Indeed, $A[\ell](\mathbb{Q}) \neq \emptyset$, since the first basis element is fixed by $\mathrm{Gal}_\mathbb{Q}$. However, one can check that there is no vector in $\mathbb{F}_\ell^4$ which is fixed by $\bar{\rho}_{A^\vee,\ell}(\sigma)$ for all $\sigma \in \mathrm{Gal}_\mathbb{Q}$, so $A^\vee[\ell](\mathbb{Q}) = \emptyset$. (Each matrix $\bar{\rho}_{A^\vee,\ell}(\sigma)$ has fixed vectors, but the coordinates depend on the matrix entries, whose values are unconstrained, as shown in Proposition 4.4.2.) Note that this argument fails for $\ell = 2$, since both A and $A^\vee$ have a rational 2-torsion point (given on $A^\vee$ by the third basis element). $\square$

4.7. **Generalizing the construction.** It is possible to generalize Construction 4.1.1 to produce more examples of abelian surfaces satisfying Theorem 1.2.1. Here, we give the construction and outline the ways in which the results of sections 4.1–4.6 need to be adapted to arrive at the result.

Instead of starting with E_1 and E_2 elliptic curves over k each with a k-rational ℓ-torsion point, we assume more generally that there are cyclic subgroups $C_1 \leqslant E_1[\ell]$ and $C_2 \leqslant E_2[\ell]$ such that $c\colon C_1 \xrightarrow{\sim} C_2$ are isomorphic as Gal_k-modules. Then, we let

$$G := \langle (P, c(P)) : P \in C_1 \rangle \leqslant E_1 \times E_2 \quad \text{and} \quad A := (E_1 \times E_2)/G.$$

When $\ell = 2$ or when the Galois action on $C_1 \simeq C_2$ is trivial, we recover Construction 4.1.1.

For $3 \leqslant \ell \leqslant 7$ a prime, there are again infinitely many elliptic curves E over $\mathbb{Q}$ with a cyclic subgroup $C \leqslant E[\ell](\mathbb{Q}^{\mathrm{al}})$ stable under $\mathrm{Gal}_{\mathbb{Q}}$ — they are parametrized by the modular curve $Y_0(\ell)$, which is birational to $\mathbb{P}^1$. Moreover, for such a pair (E, C), there exist infinitely many pairs (E', C') such that $C \simeq C'$ as Gal_K-modules. This can be seen by constructing a moduli space for the desired pairs (E', C') as a twist of $Y_1(\ell)$. This same strategy is employed in the construction of families of elliptic curves with a fixed mod N representation (see e.g. Silverberg [Sil97]).This moduli space, $Y_C(\ell)$, has a universal family $E_{\mathrm{univ},C}(\ell)$ over it (or at least over an open subset).

By sourcing our elliptic curves from $Y_0(\ell)$ instead of $Y_1(\ell)$, the images of the ℓ-adic and mod ℓ Galois representations will change. There is no longer a condition on a mod ℓ in (4.3.2), and similarly for the mod ℓ representation (that is, the 1 in the top left entry can be any $a \in \mathbb{F}_\ell^\times$). The same modification must be made in (4.3.3) and (4.3.5). Then the proof of Proposition 4.3.6 goes through the same, replacing $E_{\mathrm{univ},1}(\ell)$ with the universal family $E_{\mathrm{univ},C}(\ell)$ over $Y_C(\ell)$. Thus there are again infinitely many pairwise geometrically non-isogenous such abelian surfaces constructed as above with maximal Galois image.

Finally, the images of $\bar\rho_{A,\ell}$ and $\bar\rho_{A^\vee,\ell}$ can be calculated using the same techniques as in sections 4.3-4.5. It will no longer be the case that $A[\ell](\mathbb{Q}) \neq \emptyset$; rather, both $A[\ell](\mathbb{Q}^{\mathrm{al}})$ and $A^\vee[\ell](\mathbb{Q}^{\mathrm{al}})$ have a unique Galois-stable line. One can argue that the Galois actions on these lines do not agree, and so $A[\ell]$ and $A^\vee[\ell]$ cannot be isomorphic group schemes over $\mathbb{Q}$.

5. Further analysis and discussion

With Theorem 1.2.1 now proven, we conclude with an application and some final remarks. In section 5.1, we examine the associated permutation representations, proving Corollary 1.2.2 and giving an application to derived equivalences of Kummer fourfolds. In section 5.2, we examine the context of our results, including considering further properties the Galois actions on $A[n]$ and $A^\vee[n]$ must or need not share, with an eye toward how our results may be extended in the future.

5.1. **Associated permutation representations.** When studying the representations associated to $A[\ell](k^{\mathrm{sep}})$ and $A^\vee[\ell](k^{\mathrm{sep}})$, it is natural to ask about their corresponding permutation representations and the induced linear representations over a field F. We will give a geometric motivation for such an exploration below.

Following the notation in the introduction, for an abelian surface A, let $\pi_{A,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Sym}(A[\ell]) \simeq S_{\ell^4}$ be the permutation representation associated to $\bar{\rho}_{A,\ell}$. The following result shows that the associated permutation and linear representations of abelian surfaces A constructed as in Construction 4.1.1 are also non-isomorphic, which proves Corollary 1.2.2.

Proposition 5.1.1. *Let A be an abelian surface constructed as in Construction 4.1.1, coming from a pair E_1, E_2 as in Proposition 4.3.6.*

Then for $\ell \in \{3, 5, 7\}$, the permutation representations $\pi_{A,\ell}$ and $\pi_{A^\vee,\ell}$ are not isomorphic. Moreover, the induced linear representations over any field F with $\mathrm{char}\, F = 0$ are not isomorphic.

Proof. We can see this computationally in multiple ways; see the Magma code provided [FHV23]. For the permutation representations, we can check that the permutation characters are not isomorphic. For the induced linear representations, we compute the multiplicities of the trivial representation in the induced linear representations; we find that the multiplicities are different (for $\ell = 5$ and 7, the computations are quite time-consuming!). We check this over $\mathbb{Q}$, but the result holds over any field not of characteristic 2 or 3 by Maschke's theorem. Since the induced linear representations are not isomorphic, this also shows that the permutation representations cannot be isomorphic. □

Remark 5.1.2. We should expect that, in general, information is lost when passing from the representation $\bar{\rho}_{A,\ell}$ to the permutation representation $\pi_{A,\ell}$, in the sense that $\pi_{A,\ell}$ and $\pi_{A^\vee,\ell}$ can become isomorphic, despite $\bar{\rho}_{A,\ell}$ and $\bar{\rho}_{A^\vee,\ell}$ being non-isomorphic. This is simply because there are more elements to conjugate by in S_{ℓ^4}. The following two examples demonstrate this phenomenon:

(1) For $\ell = 2$, we have $\pi_{A,2} \simeq \pi_{A^\vee,2}$ for any A as in Proposition 5.1.1. We check in Magma that the subgroups from Propositions 4.3.11 and 4.4.2 are conjugate subgroups in S_{2^4} [FHV23].

(2) In section 4.7, we saw that there was a more general construction of abelian surfaces satisfying Theorem 1.2.1, using elliptic curves from $Y_0(\ell)$ instead of $Y_1(\ell)$. In fact, for A constructed in this more general way with $\ell = 3$ (in particular, with a non-trivial Galois action on $C_1 \simeq C_2$), we again have that $\pi_{A,3}$ and $\pi_{A^\vee,3}$ are isomorphic. This is verified computationally [FHV23].

Thus, Proposition 5.1.1 stands in contrast to these results.

Remark 5.1.3. The linear representation induced by the permutation representation associated to the 3-torsion of an abelian surface A over K is contained in the ℓ-adic étale cohomology of the generalized Kummer fourfold $K_2(A)$ [FH23, Theorem 1.1] (see also Hassett–Tschinkel [HT13, Proposition 4.1]). As a result [FH23, Corollary 1.2], the fourfolds $K_2(A)$ and $K_2(A^\vee)$ are not derived equivalent *over* K if the induced linear representations associated to $A[3]$ and $A^\vee[3]$ are not isomorphic. Using the ideas of [H19, §2.1] on twisted derived equivalence and cohomology, this result extends immediately to prove that under this condition, $K_2(A)$ and $K_2(A^\vee)$ cannot be twisted derived equivalent, either. In particular, Corollary 1.2.2 (Proposition 5.1.1) implies that there are infinitely many abelian surfaces A defined over $\mathbb{Q}$ where $K_2(A)$ and $K_2(A^\vee)$ are not (twisted) derived equivalent over $\mathbb{Q}$; it would be interesting to determine if they have such a relationship over $K(A[3], A^\vee[3]) = K(A[3])$, by Lemma 5.2.2 below.

Also in the direction of derived equivalence, recall that, as seen in the proof of Theorem 4.6.1, the abelian surfaces in Theorem 1.2.1 are such that $A[3](\mathbb{Q}) \neq \emptyset$ and $A^\vee[3](\mathbb{Q}) = \emptyset$. Since A and $A^\vee$ are derived equivalent [Muk81], this shows that the Mordell–Weil group is not a derived invariant. Note that the first dimension in which this could happen is for surfaces, since derived equivalent elliptic curves are isomorphic [AKW17, Theorem 1.1].

5.2. **Final remarks.** In closing, we look at the larger context of our results. Although we have shown that the Galois action on the torsion groups of an abelian surface and its dual can be different, it is interesting to consider whether other weaker relationships hold. Then, we speculate on further constructions of abelian surfaces or abelian varieties which would satisfy the conclusion of Theorem 1.2.1.

First, we pause to prove the statement about semisimplifications made in the introduction.

Lemma 5.2.1. *Let A be an abelian variety over a number field K and let ℓ be prime. Then the semisimplifications of the mod ℓ Galois representations attached to A and $A^\vee$ are equivalent.*

Proof. Let $\lambda\colon A \to A^\vee$ be a polarization. Then for all nonzero prime ideals $\mathfrak{p}$ in the ring of integers of K that are of good reduction for A, we obtain an isogeny $\lambda_\mathfrak{p}\colon A_{\mathbb{F}_\mathfrak{p}} \to A^\vee_{\mathbb{F}_\mathfrak{p}}$ over the residue field $\mathbb{F}_\mathfrak{p}$ between the reductions of A and $A^\vee$ modulo $\mathfrak{p}$. Hence $\overline{\rho}_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ and $\overline{\rho}_{A^\vee,\ell}(\mathrm{Frob}_\mathfrak{p})$ have the same characteristic polynomials for a dense set of Frobenius elements $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}_K$. Already the traces determine the semisimplifications up to isomorphism, by the Brauer–Nesbitt theorem. □

The next result shows that, while the images of $\overline{\rho}_{A,n}$ and $\overline{\rho}_{A^\vee,n}$ can differ, the kernels (and hence their fixed fields) always *agree*!

Lemma 5.2.2. *For all $n \in \mathbb{Z}_{\geq 1}$, we have $K(A[n]) = K(A^\vee[n]) \subset K^{\mathrm{al}}$.*

Proof. We show that $\ker \overline{\rho}_{A,n} = \ker \overline{\rho}_{A^\vee,n} \leqslant \mathrm{Gal}(K^{\mathrm{al}} \,|\, K)$. Let $\sigma \in \mathrm{Gal}(K^{\mathrm{al}} \,|\, K)$. Then $\rho_{A^\vee,n}(\sigma) = \rho_{A,n}(\sigma)^* \varepsilon_n(\sigma) = 1$ if and only if $\rho_{A,n}(\sigma) = \varepsilon_n(\sigma)$. But A has a primitive polarization λ over K, so there exist $P, Q \in A[n](K^{\mathrm{al}})$ with Weil pairing $\langle P, Q\rangle_\lambda = \zeta_n$. By Galois equivariance of the pairing, we have

$$\langle \sigma(P), \sigma(Q)\rangle_\lambda = \zeta_n^{\varepsilon_n(\sigma)},$$

so if $\rho_{A,n}(\sigma) = \varepsilon_n(\sigma)$ we get

$$\langle \varepsilon_n(\sigma)P, \varepsilon_n(\sigma)Q\rangle_\lambda = \zeta_n^{\varepsilon_n(\sigma)},$$

which yields $\varepsilon_n(\sigma) = 1$, and of course conversely. Thus $\rho_{A,n}(\sigma) = \varepsilon_n(\sigma)$ if and only if $\rho_{A,n}(\sigma) = 1$, proving the claim. □

Remark 5.2.3. The subgroups $H := \mathrm{img}\, \overline{\rho}_{A,\ell}$ and $H' := \mathrm{img}\, \overline{\rho}_{A^\vee,\ell}$ are subgroups of the subgroup $G \leqslant \mathrm{GL}_4(\mathbb{F}_\ell)$ of matrices preserving a rank 2 alternating form. (See also Proposition 5.2.4.) Recall that two subgroups $H, H' \leqslant G$ are Gassmann equivalent if $\#(H \cap C) = \#(H' \cap C)$ for all conjugacy classes C in G. We calculate that for $\ell = 2$, in fact the images are not Gassmann equivalent.

It is interesting to consider which subgroups of $\mathrm{GL}_4(\mathbb{F}_\ell)$ could be the image of $\overline{\rho}_{A,\ell}$ if $\overline{\rho}_{A,\ell}$ and $\overline{\rho}_{A^\vee,\ell}$ are not equivalent. In the following result, we enumerate such possible Galois images in the case of $\ell = 2$.

Proposition 5.2.4. *The following statements hold.*

(a) *The subgroup $G \leqslant \mathrm{GL}_4(\mathbb{F}_2)$ of elements preserving (up to scaling) the unique rank* 2 *degenerate symplectic form is a solvable group of order* 576 *and exponent* 12 *isomorphic to $C_2^4 \rtimes S_3^2$ as a group.*

(b) *Of the* 128 *conjugacy classes of subgroups $H \leqslant G$, there are* 52 *for which the natural inclusion $H \hookrightarrow G \leqslant \mathrm{GL}_4(\mathbb{F}_2)$ is not equivalent to its (twisted) contragredient.*

Proof. This follows from a direct calculation with matrix groups, which was performed in Magma; see the code [FHV23]. □

The list of groups from Proposition 5.2.4(b) is already quite interesting: the smallest group has size 4, the largest has index 2 in G!

We conclude with a few final comments on constructing abelian surfaces.

First, Bruin [Bru17] has exhibited algorithms to work with finite flat group schemes; using these methods, we could exhibit specific instances of our construction (including the Galois action). In the same vein, although our abelian surfaces are not principally polarized, so cannot arise as Jacobians of genus 2 curves, they may still be obtained as the Prym variety attached to a cover of curves. It would be interesting to see this explicitly, for example in the case $\ell = 2$ [HSS21].

Second, abelian varieties with real multiplication over fields with nontrivial narrow class group also give potential examples of abelian varieties without principal polarizations which could be used as input into our method. The underlying parameter space is now a Hilbert modular variety which may be disconnected—only one component generically corresponds to those with a principal polarization.

Third, given that our construction is limited to $\ell \leqslant 7$, one may wonder when it is even possible to construct explicit families of abelian varieties of dimension g with a polarization of degree $d > 1$. For fixed dimension g over a fixed number field K, the possible degrees d are conjecturally bounded: see Rémond [Rém18, Théorème 1.1(1)], which deduces this finiteness from Coleman's conjecture on endomorphism algebras using Zarhin's trick.

References

[AA21] Benjamin Antieau and Asher Auel, *Explicit descent on elliptic curves and splitting Brauer classes*, preprint, 2021, `arXiv:2106.04291`. 2.3

[AKW17] Benjamin Antieau, Daniel Krashen, and Matthew Ward, *Derived categories of torsors for abelian schemes*, Adv. Math. **306** (2017), 1–23. 5.1.3

[BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd. ed., Grundlehren der Mathematischen Wissenschaften, vol. 302, Springer-Verlag, Berlin, 2004. 2, 3.5

[BS23] Pawel Borówka and Anatoli Shatsila, *Hyperelliptic genus 3 curves with involutions and a Prym map*, 2023, preprint, `arXiv:2308.07038`. 4.1

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (3–4), 1997, 235–265. 4.6

[Bru17] Peter Bruin, *Dual pairs of algebras and finite commutative group schemes*, 2017, preprint, `arXiv:1709.09847`. 5.2

[CP10] Brian Conrad and Bjorn Poonen, *Non-principally polarized complex abelian varieties*, 2010, `https://mathoverflow.net/q/17014`. 4.1

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1973, Lecture Notes in Math., vol. 349, 143–316. 4.3

[FH23] Sarah Frei and Katrina Honigs, *Groups of symplectic involutions on symplectic varieties of Kummer type and their fixed loci*, Forum of Math. Sigma **11**, 2023, E40. 5.1.3

[FHV23] Sarah Frei, Katrina Honigs, and John Voight, *Code accompanying "On abelian varieties whose torsion is not self-dual"*, 2023. `https://github.com/sjfrei/FHV-abeliansurfaces`. 4.6, 5.1, 1, 2, 5.2

[FLV23+] Victoria Cantoral-Farfán, Davide Lombardo, and John Voight, *Monodromy groups of Jacobians with definite quaternionic multiplication*, 2023, preprint, `arXiv:2203.08593`. 4.3

[Gor02] Eyal Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Ser., vol. 14, Amer. Math. Soc., Providence, RI, 2002. 4.1

[HSS21] Jeroen Hanselman, Sam Schiavone, and Jeroen Sijsling, *Gluing curves of genus 1 and 2 along their 2-torsion*, Math. Comp. **90** (2021), no. 331, 2333–2379. 5.2

[HT13] Brendan Hassett and Yuri Tschinkel, *Hodge theory and Lagrangian planes on generalized Kummer fourfolds*, Mosc. Math. J. **13** (2013), no. 1, 33–56, 189. 5.1.3

[HS00] Marc Hindry and Joseph S. Silverman, *Diophantine geometry: an introduction*, Grad. Texts in Math., vol. 201, Springer, New York, 2000. 2, 2.3

[H19] Daniel Huybrechts, *Motives of isogenous K3 surfaces*, Comment. Math. Helv. **94** (2019), no. 3, 445–458. 5.1.3

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Ann. Math. Stud., vol. 108, Princeton University Press, Princeton, NJ, 1985.

[Kle14] Steven L. Kleiman, *The Picard scheme*, Alexandre Grothendieck: a mathematical portrait, 35–74. Int. Press, Somerville, MA, 2014. 2.2

[Lan13] Kai-Wen Lan, *Arithmetic compactifications of PEL-type Shimura varieties*, London Math. Soc. Monogr. Ser., vol. 36, Princeton University Press, Princeton, 2013. 3.2.10

[Lang83] Serge Lang, *Fundamentals of Diophantine geometry*, Springer, New York, 1983. 4.2

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Mil86a] J.S. Milne, *Abelian varieties,* Arithmetic geometry (Storrs, Conn., 1984), Springer-Verlag, New York, 1986, 103–150. 2

[Mil86b] J.S. Milne, *Jacobian varieties,* Arithmetic geometry (Storrs, Conn., 1984), Springer-Verlag, New York, 1986, 167–212. 2.4.6

[Mil08] James S. Milne, *Abelian varieties (v2.00)*, 2008, available at `http://www.jmilne.org/math/`. 2

[Mil12] James S. Milne, *Algebraic geometry (v5.22)*, 2012, available at `http://www.jmilne.org/math/`. 4.2

[Muk81] Shigeru Mukai, *Duality between $D(X)$ and $D(X^\vee)$ with its application to Picard sheaves*, Nagoya Math. J.81(1981), 153–175. 5.1.3

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, reprint of 2nd ed., Hindustan Book Agency, New Delhi, 2008. 2, 2.2, 2.3, 2.4, 3.5.2

[Oda69] Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4)2(1969), 63–135. 2.3

[Rém18] Gaël Rémond, *Conjectures uniformes sur les variétés abéliennes*, Q. J. Math. **69** (2018), no. 2, 459–486. 5.2

[RZB15] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Res. Number Theory **1** (2015), Art. 12, 34 pages. 4.3

[RSZB+22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$*, appendix with John Voight, Forum Math., Sigma **10** (2022), e62. 3.1

[Sal82] David J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), no. 3, 250–283. 4.2

[Ser92] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett, Boston, MA, 1992. 4.2, 4.2

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Aspects Math., Friedr. Vieweg & Sohn, Braunschweig, 1997. 4.2, 4.2

[Sil97] Alice Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, Modular forms and Fermat's last theorem, Springer-Verlag, New York, 1997, 447–461. 4.7

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009. 1.1, 2, 2.2.9, 2.3, 2.4.3, 2.4, 4.3

[SD74] H. P. F. Swinnerton-Dyer, *Analytic theory of abelian varieties*, London Mathematical Society Lecture Note Series, no. 14, Cambridge Univ. Press, London-New York, 1974. 2.2

[Wit24] Olivier Wittenberg, *Park City lecture notes: around the inverse Galois problem*, IAS/Park City Mathematics Series, AMS, to appear. 4.2

[Zyw10] David Zywina, *Hilbert's irreducibility theorem and the larger sieve*, 2010, `arXiv:1011.6465`.

[Zyw23] David Zywina, *Families of abelian varieties and large Galois images*, Int. Math. Res. (2002), published online, 1–58. 4.2

Department of Mathematics, Dartmouth College, Kemeny Hall, Hanover, NH 03755, USA
Email address: `sarah.frei@dartmouth.edu`

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, British Columbia V5A 1S6, Canada
Email address: `khonigs@sfu.ca`

Department of Mathematics, Dartmouth College, Kemeny Hall, Hanover, NH 03755, USA; Carslaw Building (F07), Department of Mathematics and Statistics, University of Sydney, NSW 2006, Australia
Email address: `jvoight@gmail.com`