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 $\ell \leqslant 7$ prime, the ℓ-torsion subgroup of A is not isomorphic as a Galois module to the ℓ-torsion subgroup of the dual $A^\vee$. We do this by analyzing the action of the Galois group on the ℓ-adic Tate module and its reduction modulo ℓ.

Contents

1. Introduction

1.1. **Setup.** Let A be an abelian variety over a number field K with $g = \dim A$. Many important arithmetic features of A are reflected in its torsion subgroups $A[n]$, equipped with the action of the absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{al}} \,|\, K)$ as encoded in the Galois representation

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

Let $A^\vee$ be the abelian variety dual to A. Then the torsion subgroup $A[n]$ is Cartier-dual to $A^\vee[n]$ via the (tautological) Weil pairing:

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

Concretely, from (1.1.2) we obtain an isomorphism

$$\overline{\rho}_{A^\vee,n} \simeq \overline{\rho}^*_{A,n} \otimes \varepsilon_n, \tag{1.1.3}$$

where * denotes the contragredient representation (transpose inverse) and ε_n is the mod n cyclotomic character.

If A has a polarization $\lambda \colon A \to A^\vee$ over K whose degree is coprime to n—for instance, if A has a principal polarization over K, which holds if A is an elliptic curve—then the polarization induces an isomorphism $A[n] \simeq A^\vee[n]$ of Galois modules. Moreover, for $n = \ell$ prime, the semi-simplifications of $\overline{\rho}_{A,\ell}$ and $\overline{\rho}_{A^\vee,\ell}$ are always isomorphic (Lemma 4.3.1).

Date: August 31, 2023.

1.2. **Results.** Our main result shows that in general we need not have $A[n]$ isomorphic to $A^\vee[n]$.

Theorem 1.2.1. *Let $\ell \leqslant 7$ be prime. Then there exist infinitely many pairwise geometrically non-isogenous abelian surfaces A over $\mathbb{Q}$ such that $A[\ell] \not\simeq A^\vee[\ell]$ as group schemes over $\mathbb{Q}$.*

Equivalently, for the surfaces in Theorem 1.2.1, we have $\overline{\rho}_{A,\ell} \not\simeq \overline{\rho}_{A^\vee,\ell}$ as linear representations, which by (1.1.3) says that the representation $\overline{\rho}_{A,\ell}$ is not self-dual up to twist by its similitude character (the cyclotomic character).

We construct the abelian surfaces in Theorem 1.2.1 by gluing two elliptic curves E, E' along a Galois-stable, diagonal subgroup isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ as an abelian group. In particular, 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 then finish by a direct calculation of the Galois representations. (To provide a more general context for these calculations, and streamline ours, we set up in section 2 a categorical framework.)

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 conversely. In fact, abelian surfaces among those exhibited in Theorem 1.2.1 satisfy this stronger property for $\ell = 3$.

Corollary 1.2.2. *There exist infinitely many geometrically nonisogenous abelian surfaces A over $\mathbb{Q}$ such that $\pi_{A,3} \not\simeq \pi_{A^\vee,3}$ as permutation representations. Moreover, the linear representations over any field k with $\operatorname{char} k = 0$ induced by the permutation representations are not isomorphic.*

1.3. **Discussion and applications.** The underlying parameter space for our construction is a twist of the product $Y_0(\ell) \times Y_1(\ell)$ 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. Our results can be extended over any number field K with $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$.

One impetus for exhibiting these abelian varieties came from studying the cohomology and derived categories of symplectic varieties of Kummer type. 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. In particular, Corollary 1.2.2 implies that there are infinitely many abelian surfaces A defined over $\mathbb{Q}$ where $K_2(A)$ and $K_2(A^\vee)$ are not derived equivalent over $\mathbb{Q}$; it would be interesting to determine if they become derived equivalent over $K(A[3], A^\vee[3])$.

Quite generally (see Proposition 4.3.2 for a start), we can 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. Exhibiting such abelian varieties systematically or explicitly presents an attractive challenge.

1.4. **Contents.** Before proceeding with our construction, in section 2 we explain (in a categorical context) how Tate modules change under isogenies and duals. In section 3 we exhibit our family and describe its basic properties, and we complete the proof of Theorem 1.2.1 and Corollary 1.2.2 in section 4 and then conclude with some final remarks.

Acknowledgements. The authors would like to thank Asher Auel, Nils Bruin, Johan de Jong, Pablo Magni, Bjorn Poonen, Ari Shnidman, and Alexei Skorobogatov for helpful comments. Honigs was supported by an NSERC Discovery grant. Voight was supported by a Simons Collaboration grant (550029).

2. Approach to Galois action computations

Our results depend on analyzing the Galois action on torsion subgroups of certain abelian surfaces that are isogenous quotients of products of elliptic curves. We are able to characterize the Galois action on the elliptic curves, which is comparatively well-understood, and then use matrix algebra to compute how the action changes under isogeny.

In this section we give a discussion of our computational methods, including practical considerations and examples as well as a formal categorical framework for our approach. The reader may wish to skip ahead to the next section and flip back to this section as needed.

In 2.1, we will begin by discussing the relationship between Tate modules of isogenous abelian varieties. We then give a general approach to choosing matrices to relate the Galois actions on the Tate modules of isogenous abelian varieties in 2.2. In 2.3 we discuss how matrices giving these actions can be selected in some practical situations. Finally in 2.4, we focus on the case where some of the isogenies in question are polarizations.

In this section, we work over a field k of characteristic p (where p may be 0) and set the convention that A_0 over k is an abelian variety of dimension g.

2.1. **From isogenies to Tate modules.** A complex abelian variety of dimension g is isomorphic to a g-dimensional complex vector space modulo a lattice of rank $2g$, i.e. $\mathbb{C}^g/\Lambda$. An isogeny of complex abelian varieties $\mathbb{C}^g/\Lambda_1 \to \mathbb{C}^g/\Lambda_2$ is given by an inclusion of lattices $\Lambda_2 \subseteq \Lambda_1$. Working over an arbitrary field k, Tate modules allow us to consider separable isogenies in an analogous way: for any $\ell \neq p$, an isogeny $A_0 \to A$ gives an inclusion of Tate modules $T_\ell A_0 \hookrightarrow T_\ell A$. Given the Galois action 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 introduce a functor that assigns isogenous quotients of A_0 to sublattices of $V_\ell A_0$. We begin by introducing notation to simultaneously keep track of all Tate modules where $\ell \neq p$.

Definition 2.1.1. Let $\widehat{\mathbb{Z}}^{(p)} := \prod_{\ell \neq p} \mathbb{Z}_\ell$ the prime-to-p profinite completion of $\mathbb{Z}$. Let A over k be a g-dimensional abelian variety. The (prime-to-p) adelic Tate module is the free $\widehat{\mathbb{Z}}^{(p)}$-module of rank $2g$:

$$\mathbb{T}A := \varprojlim_{\operatorname{char} k \nmid m} A[m](k^{\mathrm{sep}}) \simeq \prod_{\ell \neq \operatorname{char} k} T_\ell A. \tag{2.1.2}$$

Let $\mathbb{V}A := \mathbb{T}A \otimes_{\mathbb{Z}} \mathbb{Q}$.

Remark 2.1.3. We could extend the results in this section to include the factor at p by using the Dieudonné module. (Our application is in characteristic 0.)

Definition 2.1.4. Let $\mathcal{I}$ be the category whose objects are abelian varieties over k and whose morphisms are k-isogenies with degree prime to p. Then the objects of the coslice category $\mathcal{I}^{A_0} := A_0 \downarrow \mathcal{I}$ are isogenies $A_0 \to A$ and its morphisms are commuting triangles of isogenies:

(2.1.5)
$$\begin{tikzcd}
& A_0 \arrow[dl, "(\varphi)"'] \arrow[dr, "(\psi)"] & \\
A \arrow[rr, "f"'] & & B.
\end{tikzcd}$$

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

Remark 2.1.6. The identity morphism (id_{A_0}) is initial in $\mathcal{I}^{A_0}$. For any $(\varphi) \in \operatorname{Ob} \mathcal{I}^{A_0}$, φ is the unique morphism that maps $(\mathrm{id}_{A_0}) \to (\varphi)$.

Next we give the category of sublattices of $\mathbb{V}A_0$.

Definition 2.1.7. Let $\mathcal{T}_{A_0}$ be the category whose objects are $\widehat{\mathbb{Z}}^{(p)}$-lattices of rank $2g$ contained in $\mathbb{V}A_0$ and whose morphisms are injective maps of lattices in $\mathbb{V}A_0$:

(2.1.8)
$$\begin{tikzcd}
T \arrow[rr, hook] \arrow[dr, hook] & & T' \arrow[dl, hook'] \\
& \mathbb{V}A_0 & .
\end{tikzcd}$$

We now define a functor $\Psi \colon \mathcal{I}^{A_0} \to \mathcal{T}_{A_0}$.

Definition 2.1.9. For any $(\varphi) \colon A_0 \to A \in \operatorname{Ob} \mathcal{I}^{A_0}$, we have the injective $\widehat{\mathbb{Z}}^{(p)}$-linear map $\mathbb{T}\varphi \colon \mathbb{T}A_0 \hookrightarrow \mathbb{T}A$ and the isomorphism $\mathbb{V}\varphi \colon \mathbb{V}A_0 \xrightarrow{\sim} \mathbb{V}A$. We define $\Psi(\varphi) := (\mathbb{V}\varphi)^{-1}(\mathbb{T}A)$, which is the image of $\mathbb{T}A$ in $\mathbb{V}A_0$ under the dotted arrow in the following commutative diagram:

(2.1.10)
$$\begin{tikzcd}
\mathbb{T}A_0 \arrow[r, hook, "\mathbb{T}\varphi"] \arrow[d, hook, "\otimes\mathbb{Q}"'] & \mathbb{T}A \arrow[d, hook, "\otimes\mathbb{Q}"] \arrow[dl, hook', dashed] \\
\mathbb{V}A_0 \arrow[r, "\sim", "\mathbb{V}\varphi"'] & \mathbb{V}A.
\end{tikzcd}$$

For any morphism f in $\mathcal{I}^{A_0}$ as in (2.1.5), we have the following commutative diagram.

(2.1.11)
$$\begin{tikzcd}
\mathbb{T}A_0 \arrow[r, hook, "\mathbb{T}\varphi"] \arrow[d, hook, "\otimes\mathbb{Q}"'] & \mathbb{T}A \arrow[r, hook, "\mathbb{T}f"] \arrow[d, hook, "\otimes\mathbb{Q}"'] \arrow[dl, hook', dashed] & \mathbb{T}B \arrow[d, hook, "\otimes\mathbb{Q}"] \arrow[dll, hook', dashed] \\
\mathbb{V}A_0 \arrow[r, "\sim", "\mathbb{V}\varphi"'] & \mathbb{V}A \arrow[r, "\sim", "\mathbb{V}f"'] & \mathbb{V}B
\end{tikzcd}$$

We define $\Psi f\colon \Psi(\varphi) \to \Psi(\psi)$ to be the map between sublattices of $\mathbb{V}A_0$ given by the image of $\mathbb{T}f$ in $\mathbb{V}A_0$ under the dotted arrows.

The functoriality of Ψ is a consequence of the functoriality of $\mathbb{T}$ and $\mathbb{V}$ acting on $\mathcal{I}$.

Remark 2.1.12. Since $\mathbb{T}$ 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. Understanding the essential image of Ψ is equivalent to characterizing which sublattices of $\mathbb{V}A_0$ 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 $\mathbb{V}A_0$, working over an algebraically closed field.

2.2. **From Tate modules to group representations.** In our computations in section 3, we will consider questions such as the following: Given a diagram of isogenies such as (2.1.11) and a choice of matrices giving the Galois representation on $\mathbb{T}A_0$, how should we choose matrices to compute the Galois representations on $\mathbb{T}A$ and $\mathbb{T}B$ and relate those via f?

In section 2.1, we showed how we may consider $\mathbb{T}A$ and $\mathbb{T}B$ as sublattices of $\mathbb{V}A_0$. All the maps involved in that identification are Galois invariant, so the Galois action on $\mathbb{T}A$ and $\mathbb{T}B$ is simply the restriction of the action on $\mathbb{V}A_0$ to these sublattices. Our question is now a matter of choosing compatible change of basis matrices. We will first show this is equivalent to choosing a certain functor, and discuss equivalent ways of specifying such a functor.

Our setting for Galois representations and change of basis is the following category.

Definition 2.2.1. Let $\mathrm{RepMat}_{G,g}$ be the category whose objects are products of $2g$-dimensional $\mathbb{Q}_\ell$-representations $\rho = \prod_{\ell \neq p} \rho_\ell$ where $\rho_\ell\colon\ \mathrm{Gal}_k \to \prod_{\ell\neq p} \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$. We abbreviate $\mathrm{Gal}_k = G$.

Morphisms $M\colon \rho \to \rho'$ consist of sets of matrices $M := \{M_\ell\}_{\ell\neq p}$, $M_\ell \in \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$, so that $\rho'_\ell(a) = M_\ell^{-1}\rho_\ell(a)M_\ell$ for all $a \in \mathrm{Gal}_k$. Composing morphisms, i.e., successively conjugating a representation, is given by multiplying matrices: $M' \circ M = \{M_\ell M'_\ell\}_{\ell\neq p}$.

The Galois representations we asked for above could be considered as a functor from the image of (the subcategory generated by) (2.1.5) under Ψ to $\mathrm{RepMat}_{G,g}$. However, this setting has the disadvantage of not recording the representation on $\mathbb{T}A_0$ and its relationship with the other representations. We remedy this shortcoming by adding the initial object (id_{A_0}) and all the maps out of it to (2.1.5), yielding the following subcategory of $\mathcal{I}^{A_0}$ (identity maps not shown) in which (id_{A_0}) is now initial:

(2.2.2)
$$\begin{tikzcd}
 & A_0 \arrow[dl, "(\mathrm{id}_{A_0})"'] \arrow[d, "(\varphi)"'] \arrow[dr, "(\psi)"] & \\
A_0 \arrow[r, "\varphi"'] \arrow[rr, bend right, "\psi"'] & A \arrow[r, "f"'] & B
\end{tikzcd}$$

If we like, we can think of this process more formally as taking the closure of the subcategory (2.1.5) of $\mathcal{I}^{A_0}$ under the initial object (id_{A_0}).

Definition 2.2.3. Let $\mathcal{C}$ be a category containing an initial object I and a subcategory $\mathcal{S}$. The closure $\mathcal{S}'$ of $\mathcal{S}$ under the initial object I is the smallest subcategory $\mathcal{S} \subseteq \mathcal{S}' \subseteq \mathcal{C}$ such that $I \in \mathrm{Ob}\,\mathcal{S}'$ and I is initial in $\mathcal{S}'$.

We may construct $\mathcal{S}'$ from $\mathcal{S}$ by adding the initial object I, its identity morphism, and the (unique) morphisms from I to each object in $\mathcal{S}$. The initialness of I guarantees that $\mathcal{S}'$ is closed under composition of morphisms.

Now call $\mathcal{E}$ be the subcategory of $\mathcal{I}^{A_0}$ shown in (2.2.2). The image $\Psi\mathcal{E}$ in $\mathcal{T}_{A_0}$ is the following (again not showing identity morphisms):

$$\begin{tikzcd}
\Psi(\mathrm{id}_{A_0}) \arrow[r, hook, "\Psi\varphi"] \arrow[rr, hook, bend left, "\Psi\psi"] \arrow[dr, hook] & \Psi(\varphi) \arrow[r, hook, "\Psi f"] \arrow[d, hook] & \Psi(\psi) \arrow[dl, hook] \\
 & \mathbb{V}A_0 &
\end{tikzcd} \tag{2.2.4}$$

Giving a Galois representation on $\mathbb{T}A_0$, representations on $\mathbb{T}A$ and $\mathbb{T}B$ along with change of basis matrices relating them all determines a functor $F\colon \Psi\mathcal{E} \to \mathrm{RepMat}_{G,g}$. We can make the following straightforward observations about such a functor F being completely determined by just some of its information:

- The choice of $F\Psi(\mathrm{id}_{A_0})$ and a change of basis matrix such as $F\Psi\varphi$ determines the representation $F\Psi(\varphi)$.
- The matrices $F\Psi\varphi$ and $F\Psi f$ determine $F\Psi\psi$. In fact, the choice of any two of these determines the third.

We can use these ideas to make a more general statement as follows.

Lemma 2.2.5. *Let $\mathcal{D}$ be a subcategory of $\mathcal{I}^{A_0}$ closed under the initial object* (id_{A_0})*. A functor*

$$F\colon \Psi\mathcal{D} \to \mathrm{RepMat}_{G,g}$$

is determined by the representation $F\Psi(\mathrm{id}_{A_0})$, and, for each object $(\varphi) \in \mathcal{I}^{A_0}$, the change of basis matrices $F\Psi\varphi$.

Proof. This statement is a consequence of the fact that (id_{A_0}) is initial in $\mathcal{D}$ in combination with the following properties of $\mathrm{RepMat}_{G,g}$: For any morphism $M\colon \rho \to \rho'$ in $\mathrm{RepMat}_{G,g}$, the data of the representation ρ and the change of basis matrices in M determines the representation ρ'. Furthermore, the matrices giving the morphisms in $\mathrm{RepMat}_{G,g}$ are invertible, so if we have a composition of morphisms $M_j = M_h \circ M_f$, then any two of the morphisms determine the third, e.g. M_j and M_f determine M_h. □

2.3. **Producing change of basis matrices.** In this section, we continue our examination of the question posed at the beginning of section 2.2, now focusing on choosing matrices. From our discussion in the previous section, we know we may reduce such questions to the following: Given an isogeny $\varphi\colon A_0 \to A$ and a choice of basis for $\mathbb{T}A_0 \subset \mathbb{V}A_0$, how do we choose change of basis matrices from $\mathbb{T}A_0$ to $\Psi(\varphi)$?

The answer to this question depends on how the isogeny is given two us. In this section, we give methods for two different situations, and show some small examples of isogenies between elliptic curves:

(1) $A = A_0$ and we have matrices for the transformation $\mathbb{V}\varphi\colon \mathbb{V}A_0 \xrightarrow{\sim} \mathbb{V}A_0$.
(2) We are given $\ker\varphi$.

We set the notational convention that the change of basis matrix between the ℓ-adic portions of $\mathbb{T}A_0$ and $\Psi(\varphi)$ is called $M_{\varphi,\ell}$.

Case (1): Matrices of transformation. This case applies to, for instance, multiplication maps as in Example 2.3.3.

Lemma 2.3.1. *Let $\varphi\colon A_0 \to A$ be an isogeny. Suppose we have a fixed basis for $\mathbb{T}A_0 \subseteq \mathbb{V}A_0$ and the linear transformation $\mathbb{V}\varphi\colon \mathbb{V}A_0 \to \mathbb{V}A_0$ is given by matrices $\{N_{\varphi,\ell}\}_\ell$. Then we may choose $M_{\varphi,\ell}$ to be $N_{\varphi,\ell}^{-1}$.*

Proof. Fix a prime ℓ and let $P_1, \dots, P_{2g}$ be the fixed basis for $T_\ell A_0$, where $N_{\varphi,\ell}$ is given in terms of this basis. In this situation, the diagram (2.1.10) is as follows:

(2.3.2)
$$\begin{tikzcd}
T_\ell A_0 \arrow[r, hook, "T_\ell\varphi"] \arrow[d, hook, "\otimes\mathbb{Q}"'] & T_\ell A_0 \arrow[d, hook, "\otimes\mathbb{Q}"] \arrow[dl, hook, dashed, "\Psi(\varphi)"'] \\
V_\ell A_0 \arrow[r, "\sim", "V_\ell\varphi = N_{\varphi,\ell}"'] & V_\ell A_0,
\end{tikzcd}$$

The elements $\varphi(P_1), \dots, \varphi(P_{2g})$ are a basis for $\Psi(\varphi)$. The ith column of $N_{\varphi,\ell}$ is the coefficients of the equation $\varphi(P_i) = c_1 P_1 + \cdots + c_{2g}P_{2g}$. Thus, $N_{\varphi,\ell}^{-1}$ gives a change of basis matrix as desired. Put another way, the matrix $N_{\varphi,\ell}$ maps the basis of $T_\ell A$, identified with the standard coordinates, to a basis for the image $T_\ell\varphi(T_\ell A)$; a change of coordinates matrix should do the inverse. □

Example 2.3.3. 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 $N_{[\ell],\ell}$ for $V_\ell[\ell]\colon V_\ell E \to V_\ell E$ and the change of basis matrix $M_{[\ell],\ell}$ chosen as in Lemma 2.3.1 are the following:

$$N_{[\ell],\ell} = \begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}, \quad M_{[\ell],\ell} = \begin{pmatrix} \frac{1}{\ell} & 0 \\ 0 & \frac{1}{\ell} \end{pmatrix}$$

Remark 2.3.4. If φ is a homothety, as in Example 2.3.3, conjugating a representation by the matrices $M_{\varphi,\ell}$ has no effect since it amounts to multiplying by a scalar and its inverse.

Case (2): Kernels. The kernel of an isogeny identifies it up to isomorphism. In diagram (2.1.11), if f is an isomorphism between $\varphi\colon A_0 \to A$ and $\psi\colon A_0 \to B$, then $\mathbb{V}f^{-1}(\mathbb{T}B) = \mathbb{T}A$ 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 $M_{\varphi,\ell}$.

Lemma 2.3.5. *The following statements hold.*

(a) *If $H \subseteq A_{0,k^{\mathrm{sep}}}[m]$, then $\Psi(\varphi) \subseteq \frac{1}{m}\mathbb{T}A_0 \subseteq \mathbb{V}A_0$.*

(b) *Moreover, $\Psi(\varphi)$ is the unique sublattice of $\frac{1}{m}\mathbb{T}A_0$ having the property that $m(\Psi(\varphi)/\mathbb{T}A_0)$ 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 (2.1.11) with $\psi = [m]$ that $\Psi([m])$ is an overlattice of $\Psi(\varphi)$ inside $\mathbb{V}A_0$. Furthmore, if we consider the diagram (2.1.10) in the case $\varphi = [m]$, $\Psi([m]) = \frac{1}{m}\mathbb{T}A_0 \subseteq \mathbb{V}A_0$.

(b) Let ℓ be a prime with ℓ^n the highest power dividing m, $H_\ell := H \cap A_0[\ell^n]$, and $\Psi_\ell(\varphi)$ the ℓ-adic part of $\Psi(\varphi)$. It suffices to prove the result on the ℓ-primary sublattice.

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

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

where the second isomorphism is given by projection onto $A_0[\ell^n]$, where the projection $T_\ell A_0 \to A_0[\ell^n]$ 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 $x = (x_m)_m \in T_\ell A_0$. Note that this isomorphism is canonical.

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 show that the image of the restriction is contained in H_ℓ. To see this, it is enough to show 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

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

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

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

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

Thus, the canonical isomorphism allows us to canonically identify $\ell^n (\Psi_\ell(\varphi) / T_\ell A_0) \cong H_\ell$, and hence $m(\Psi(\varphi) / \mathbb{T} A_0) \cong H$. □

Remark 2.3.6. It is a standard fact 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 $\mathbb{T}\varphi \colon \mathbb{T} A_0 \to \mathbb{T} A$. The isomorphism in Lemma 2.3.5(b) can also be deduced from this perspective.

Construction 2.3.7. Lemma 2.3.5 suggests a method for choosing a basis of $\Psi(\varphi)$ from a minimal set of generators for H. Let m be (possibly a multiple of) the exponent of $H := \ker \varphi$. For each prime $\ell \nmid (\#H)$, we may choose $M_{\varphi,\ell}$ to be the identity matrix. Otherwise, we handle each prime divisor of $\#H$ separately, so suppose ℓ^n is the highest power of ℓ dividing m.

Let $P_1, \ldots P_{2g}$ be a symplectic 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 $P_{1,n}, \ldots, P_{2g,n}$ with coefficients in

$\{0, 1, \ldots, \ell^n - 1\}$. If $a_1 P_{1,n} + \cdots + a_{2g} P_{2g,n}$ is one of the generators for H_ℓ, we may choose an element

$$\frac{\tilde{a}_1}{\ell^n} P_1 + \cdots + \frac{\tilde{a}_{2g}}{\ell^n} P_{2g} \tag{2.3.8}$$

of $\Psi\varphi \subseteq \frac{1}{\ell^n}\mathbb{T}A_0$, where $\tilde{a}_i$ is any choice of lift of a_i to $\mathbb{Z}_\ell$. The element (2.3.8) is indeed in $\Psi(\varphi)$ by Lemma 2.3.5(b): it is contained in $\frac{1}{\ell^n}\mathbb{T}A_0$ and if we consider the quotient $\ell^n(\frac{\tilde{a}_1}{\ell^n} P_1 + \cdots + \frac{\tilde{a}_{2g}}{\ell^n} P_{2g}) \bmod \langle P_1, \ldots, P_{2g}\rangle$, we recover $a_1 P_{1,n} + \cdots + a_{2g} P_{2g,n}$.

To find a basis for $\Psi(\varphi)$ in $V_\ell A_0$, first take these lifts of each element in a minimal generating set for H. Then, we need to complete the result as necessary to a ($2g$-dimensional) basis for $\Psi\varphi$ by using linear combinations of $P_1, \ldots, P_{2g}$ with coefficients in $\{0, 1, \ldots, \ell^n - 1\}$. The coefficients of $P_1, \ldots, P_{2g}$ in each basis element will give the columns of the change of basis matrix $M_{\varphi,\ell}$.

We now put this recipe into practice with an example of an isogeny between elliptic curves.

Example 2.3.9. Let E be an elliptic curve. Choose a symplectic basis $P_1 = \{P_{1,n}\}, P_2 = \{P_{2,n}\}$ for $T_\ell E$. Consider the isogeny $\varphi\colon E \to F$ with kernel $\langle P_{1,1}\rangle$.

The exponent of $\ker\varphi$ is ℓ. We may lift the coefficient 1 to $1 \in \mathbb{Z}_\ell$, choosing the element $\frac{1}{\ell}P_1 \in \Psi_\ell\varphi$. 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, which gives:

$$M_{\varphi,\ell} = \begin{pmatrix} \frac{1}{\ell} & 0 \\ 0 & 1 \end{pmatrix}.$$

By Construction 2.3.7, in fact any combination $c_1 P_1 + c_2 P_2$ with $c_1, c_2 \in \{0, 1, \ldots, \ell - 1\}$ that is linearly independent from $\frac{1}{\ell}P_1$ will work as a choice of second basis vector.

2.4. **Change of basis matrices for polarizations.** In this section, we look at transformation matrices in the case where the isogenies are polarizations or dual to isogenies we already understand. 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 these transformation matrices, Lemma 2.3.1 can be applied to determine change of basis matrices.

Polarization constructions.

Definition 2.4.1. An isogeny $\lambda_0\colon A_0 \to A_0^\vee$ is a polarization if there is a finite separable field extension $K \supset k$ and an ample line bundle L on $A_{0,K}$ so that $\lambda_{0,K} = \varphi_L$, where $\varphi_L(x) := t_x^* L \otimes L^{-1}$.

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

Definition 2.4.2. 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.

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

Definition 2.4.3. 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].

$$\begin{tikzcd} A_0 \arrow[r, "d\lambda_0"] \arrow[d, "g"'] & A_0^\vee \\ A \arrow[r, "g_*\lambda_0"] & A^\vee \arrow[u, "g^\vee"'] \end{tikzcd} \tag{2.4.4}$$

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

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

Given the type D of a polarization λ_0, there is a standard choice of matrices giving the transformation $\mathbb{V}\lambda_0\colon \mathbb{V}A_0 \to \mathbb{V}A_0^\vee$. If A_0 is complex, we may choose a symplectic basis for its underlying torus and the dual basis for $A_0^\vee$, so that the following matrix gives the polarization, where D denotes the diagonal matrix with entries given by the type [BL04, §3.1]:

$$\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}. \tag{2.4.5}$$

This is also the matrix for the bilinear pairing that $\mathbb{T}\lambda_0$ gives on $\mathbb{T}A_0$. Working over k, we may replace D with D_ℓ, the factors of ℓ in the type, to choose the matrices $\{N_{\lambda_0,\ell}\}_\ell$ of the transformation $\mathbb{V}\lambda_0\colon \mathbb{V}A_0 \to \mathbb{V}A_0^\vee$. In making these choices, we are identifying $V_\ell A_0^\vee$ with the dual vector space of $V_\ell A_0$ and choosing its basis to be dual to that of $V_\ell A_0$. We may choose the change of basis matrix $M_{\lambda_0,\ell}$ to be $N_{\lambda_0,\ell}^{-1}$ by Lemma 2.3.1. We may apply Lemma 2.3.1 to this situation since we have chosen isomorphisms $\mathbb{V}A_0 \simeq \mathbb{V}A_0^\vee$ identifying the coordinates of these two vector spaces.

Let $f\colon A \to B$ be an isogeny and suppose we have matrices $\{N_{f,\ell}\}_\ell$ for the transformation $\mathbb{V}f\colon \mathbb{V}A \to \mathbb{V}B$. Inherent in such a choice of matrices is a choice of bases on $V_\ell A$ and $V_\ell B$ (and if we like, isomorphisms $V_\ell A \simeq V_\ell B$ identifying those bases). We may identify $V_\ell A^\vee, V_\ell B^\vee$ with the dual vector spaces of $V_\ell A, V_\ell B$ and choose their bases to be dual to those of $V_\ell A, V_\ell B$. Having made these choices, the matrices of the transformation $\mathbb{V}f\colon \mathbb{V}B^\vee \to \mathbb{V}A^\vee$ are:

$$\{N_{f^\vee,\ell}\}_\ell, \quad N_{f^\vee,\ell} := N_{f,\ell}^T. \tag{2.4.6}$$

Putting these ideas together, if we are given matrices $\{N_{\lambda_0,\ell}\}_\ell$ of the transformation $\mathbb{V}\lambda_0\colon \mathbb{V}A_0 \to \mathbb{V}A_0^\vee$ for a polarization $\lambda_0\colon A_0 \to A_0^\vee$ and matrices $\{N_{f,\ell}\}_\ell$ for an isogeny $f\colon A \to A_0$, then the matrices giving the pullback transformation $\mathbb{V}f^*\lambda_0\colon \mathbb{V}A \to \mathbb{V}A^\vee$ are:

$$\{N_{f^*\lambda,\ell}\}_\ell, \quad N_{f^*\lambda,\ell} = N_{f,\ell}^T N_{\lambda,\ell} N_{f,\ell}. \tag{2.4.7}$$

The matrices $\{N_{f^*\lambda,\ell}\}_\ell$ also give the bilinear pairing on $\mathbb{V}A$ associated with polarization $f^*\lambda_0$. Similarly to the discussion for polarizations above, we may apply Lemma 2.3.1 to find change of basis matrices.

We now examine a specific example of a pushforward of a polarization.

Example 2.4.8. Let E be an elliptic curve and $\varphi\colon E \to F$ a cyclic isogeny as in Example 2.3.9. We add the assumption that the choice of basis for $V_\ell E$ is such that the transformation matrices for the principal polarization λ of E and the isogeny φ acting on $V_\ell E$ are the following:

$$N_{\lambda,\ell} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad N_{\varphi,\ell} = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}.$$

The kernel of φ is isotropic under the pairing given by $N_{\lambda,\ell}$ and ℓ is the smallest value so that $\ker(g) \subseteq \ker(\ell\lambda)$. Thus, we can determine the pushforward $\varphi_*\lambda$, which we compute using (2.4.4):

$$N_{\varphi_*\lambda,\ell} = N^{-1}_{\varphi^\vee,\ell} N_{\ell\lambda_0,\ell} N^{-1}_{\varphi,\ell} = (N^T_{\varphi,\ell})^{-1} N_{\ell\lambda_0,\ell} N^{-1}_{\varphi,\ell} = \begin{pmatrix} \frac{1}{\ell} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \ell \\ -\ell & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\ell} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thus, the pushforward $\varphi_*\lambda$ is a principal polarization on F.

3. Constructions and computations

In this section, we construct the abelian surfaces A arising in Theorem 1.2.1. We will then use the technical tools developed in section 2 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.

3.1. 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.

Construction 3.1.1. Let E_1 and E_2 be elliptic curves over k and let $C_1 \leqslant E_1[\ell]$ and $C_2 \leqslant E_2[\ell]$ be cyclic subgroups such that $c\colon C_1 \xrightarrow{\sim} C_2$ are isomorphic as Gal_k-modules. Let

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

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

In section 4.1, we will use Construction 3.1.1 in the proof of Theorem 1.2.1.

Lemma 3.1.2. *With setup as in Construction 3.1.1, 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 stable under Gal_k by construction, and A obtains a $(1,\ell)$-polarization λ from the pushforward under q (cf. section 2.4) of the principal product polarization ι 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 $\phi := \iota^{-1} \circ q^*\lambda \in \operatorname{End}(E_1 \times E_2)$ is a symmetric (fixed under the Rosati involution) endomorphism of degree $(\ell d)^2$. 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 symmetric endomorphisms of an elliptic curve is $\mathbb{Z}$, 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, $\ker q \subseteq \ker \phi = E_1[d_1] \times E_2[d_2]$, so $\ker q \cap E_2 = \ker q \cap E_2[d_2]$. Now suppose that $\ell \nmid d$. Without loss of generality, $\ell \mid d_1$ and $\ell \nmid d_2$, which implies $\ker q \cap E_2$ must be trivial. However, $\ker q$ intersects both E_1 and E_2 nontrivially, and we have a contradiction. □

Over number fields, we can exhibit infinitely many generic instances of Construction 3.1.1 as follows. We begin with the elliptic curves.

Proposition 3.1.3. *Let $\ell \leqslant 7$ be prime and let K be a number field. Then the following statements hold.*

(a) *There exist infinitely many elliptic curves E over K with a cyclic subgroup $C \leqslant E[\ell](K^{\mathrm{al}})$ stable under Gal_K.*

(b) *Let (E, C) be as in* (a)*. Then there exist infinitely many pairs (E', C') as in* (a) *such that $C \simeq C'$ as Gal_K-modules.*

Proof. First part (a). Recall that the modular curve $Y_0(\ell)$ parametrizes isomorphism classes of pairs (E, C) where E is an elliptic curve and $C \leqslant E[\ell]$ is a cyclic subgroup of order ℓ, and that $Y_0(\ell) \subseteq X_0(\ell)$ is an open subscheme. Then part (a) follows from the fact that we have $X_0(\ell) \simeq \mathbb{P}^1$ 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 a cyclic subgroup of order ℓ stable under Gal_K.

We next prove (b), with (E, C) as in (a). By twisting $Y_1(\ell)$, we will construct a moduli space for the desired pairs (E', C'). We follow the same strategy as in the construction of families of elliptic curves with a fixed mod N representation (see e.g. Silverberg [Sil97]). For $\ell = 2$ we just refer again to (a): the Gal_K-action on C is trivial.

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 $\ell = 3$, a similar statement holds over the open subset of $Y_1(\ell)$ removing the points above $j = 0$ (universal for elliptic curves over a base S such that j is invertible on S). For $\ell \leqslant 7$, we have $Y_1(\ell)$ birational to $\mathbb{P}^1$.

Choosing an isomorphism $\iota \colon C_{K^{\mathrm{al}}} \to (\mathbb{Z}/\ell\mathbb{Z})_{K^{\mathrm{al}}}$ over K^{al}, the map $\sigma \mapsto \iota^{-1} \circ \sigma(\iota)$ defines a cocycle on Gal_K with values in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. By universality, there is a natural injective homomorphism

$$(\mathbb{Z}/\ell\mathbb{Z})^\times \to \operatorname{Aut} E_{\mathrm{univ},1}(\ell) \tag{3.1.4}$$

defined by $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ sends $P_{\mathrm{univ}} \mapsto aP_{\mathrm{univ}}$. Composing, we obtain a cocycle c on Gal_K with values in $\operatorname{Aut} E_{\mathrm{univ},}(\ell)$. We let $E_{\mathrm{univ},C}(\ell)$ be the twist of $E_{\mathrm{univ},1}(\ell)$ by c.

We similarly obtain a map $(\mathbb{Z}/\ell\mathbb{Z})^\times \to (\operatorname{Aut} Y_1(\ell))(\mathbb{Q})$ (factoring through $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$), giving a twist $Y_C(\ell)$ defined over K. But $[(E, C)] \in Y_C(\ell)(K)$ and $Y_C(\ell)$ still has genus zero, so $Y_C(\ell)$ is again birational to $\mathbb{P}^1$. By compatibility, we obtain an elliptic surface $\pi_C \colon E_{\mathrm{univ},C}(\ell) \to Y_C(\ell)$.

Let $P_{\mathrm{univ},C}$ be the section of $E_{\mathrm{univ},C}(\ell)$ defined over K^{al} obtained from the image of P_{univ} under the isomorphism $E_{\mathrm{univ},1}(\ell)_{K^{\mathrm{al}}} \simeq E_{\mathrm{univ},C}(\ell)_{K^{\mathrm{al}}}$. Then for every $t \in Y_C(\ell)(K)$ we obtain an elliptic curve $E' := \pi_C^{-1}(t)$ and it follows by definition of the twist that $C' := \langle P_{\mathrm{univ,C}}|_t \rangle$ is a cyclic subgroup of order ℓ, stable under Gal_K, and isomorphic to C as a Gal_K-module. $\square$

Example 3.1.5. If C has trivial Gal_K-action, i.e., if $C = \langle P \rangle$ with $P \in E[\ell](K)$, then the twist $Y_C(\ell)$ is again just $Y_1(\ell)$. This case is enough for our constructions, so part (b) of Proposition 3.1.3 is extra—we keep it for the added generality and naturality in the construction.

3.2. **Computation of the Galois action on A.** Let A be an abelian surface over $\mathbb{Q}$ as in Construction 3.1.1 with (E_1, C_1) and (E_2, C_2) satisfying $C_1 \simeq C_2$ as $\mathrm{Gal}_{\mathbb{Q}}$-modules. (There are infinitely many, by Proposition 3.1.3.) 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 Lemma 2.2.5.

Here and in subsequent sections we use the computational ideas outlined in section 2. 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 3.2.1. *Let $\ell \leqslant 7$ be prime. Then the following statements hold.*

(a) *For (E, C) such that $[(E, C)] \in Y_0(\ell)(\mathbb{Q}) \subset \mathbb{P}^1$, the image of the ℓ-adic Galois representation*

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

is contained in

$$\left\{ \begin{pmatrix} a & b \\ \ell c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_\ell) : a, d \in \mathbb{Z}_\ell^\times \right\} \leqslant \mathrm{GL}_2(\mathbb{Z}_\ell) \tag{3.2.2}$$

in any basis P_1, P_2 for $T_\ell(E)$ such that P_1 $\mathrm{mod}\ \ell$ generates C. In particular,

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

has image contained in

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

(b) *Outside of a thin set in $Y_0(\ell)(\mathbb{Q})$, the image $\rho_{E,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is the entire subgroup in (3.2.2).*

Since $\mathbb{Q}$ is Hilbertian, when $E_t \in Y_0(\ell)(\mathbb{Q}) \subseteq \mathbb{P}^1$ are ordered by the height of $t \in \mathbb{P}^1$, the conclusion of Lemma 3.2.1(b) holds for a density 1 subset.

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

Part (b) follows from Hilbert irreducibility, which we can make 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 $Y_H \to Y_0(\ell)$ 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 $[(E, C)] \in Y_0(\ell)(\mathbb{Q})$ 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 $Y_0(\ell)(\mathbb{Q})$. $\square$

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 3.2.1, specifically:

- $(P_1 \bmod \ell) \in C_1(\mathbb{Q}^{\mathrm{al}}) \subset E_1[\ell](\mathbb{Q}^{\mathrm{al}})$,
- $(Q_1 \bmod \ell) \in C_2(\mathbb{Q}^{\mathrm{al}}) \subset E_2[\ell](\mathbb{Q}^{\mathrm{al}})$,
- $\{P_1, P_2\}$ 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

$$\left\{ \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ 0 & d_1 & 0 & 0 \\ 0 & 0 & a_2 & b_2 \\ 0 & 0 & 0 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : a_1, d_1, a_2, d_2 \in \mathbb{F}_\ell^\times \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell). \tag{3.2.3}$$

When we pick an isomorphism $C_1 \simeq C_2$, this identifies the cyclic subgroups generated by P_1 and Q_1 as Galois modules, hence they have the same Galois action: this implies that $a_1 = a_2$. Similarly, the Galois equivariance of the Weil pairing (given explicitly by the determinant) [Sil09, section III.8] implies that $\rho_{E_1 \times E_2, \ell}(\mathrm{Gal}_\mathbb{Q})$ is contained in

$$G_\ell := \left\{ \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ \ell c_1 & d_1 & 0 & 0 \\ 0 & 0 & a_2 & b_2 \\ 0 & 0 & \ell c_2 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{l} a_1, d_1, a_2, d_2 \in \mathbb{Z}_\ell^\times, \\ a_1 \equiv a_2 \pmod{\ell}, \text{ and} \\ a_1 d_1 - \ell b_1 c_1 = a_2 d_2 - \ell b_2 c_2 \end{array} \right\} \leqslant \mathrm{GL}_4(\mathbb{Z}_\ell). \tag{3.2.4}$$

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

Proposition 3.2.5. *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 (3.2.4); in particular, there exist cyclic subgroups $C_1 \leqslant E_1[\ell](\mathbb{Q}^{\mathrm{al}})$ and $C_2 \leqslant E_2[\ell](\mathbb{Q}^{\mathrm{al}})$ stable under $\mathrm{Gal}_\mathbb{Q}$ such that $C_1 \simeq C_2$ as $\mathrm{Gal}_\mathbb{Q}$-modules; 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. Let (E, C) be such that $[(E, C)] \in Y_0(\ell)(\mathbb{Q})$ lies outside the thin set of Lemma 3.2.1(b), so $\rho_{E,\ell}$ has the large image (3.2.2). By an entirely analogous argument, outside of a thin subset of $Y_C(\ell)$, every $[(E', C')] \in Y_C(\ell)$ also has image (3.2.2).

We consider the family $A_C := E \times E_{\mathrm{univ},C}(\ell)$ over $Y_C(\ell)$. We claim that over the generic point, the ℓ-adic Galois representation $\rho_{A_C,\ell} \colon \mathrm{Gal}_Q \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ has image given by (3.2.4): indeed, the only constant subextension of $\mathbb{Q}(E_{\mathrm{univ},C}[\ell^\infty])$ over $\mathbb{Q}(E_{\mathrm{univ},C}) \simeq \mathbb{Q}(t)$ is given by $\mathbb{Q}(C, \zeta_\ell)$. The result then follows by the Hilbert irreducibility theorem: see Zywina [Zyw23, Lemma 2.2]. In particular, the desired conclusion holds for a density 1 subset of $t \in Y_C(\ell)(\mathbb{Q}) \subseteq \mathbb{P}^1$.

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 $\rho_{E_{1,K},\ell}$, a contradiction as this is a proper subgroup of G_ℓ.

The final statement follows quite 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 $\operatorname{ord}_p(j(E)) < 0$ has negative valuation. Let t be a parameter on $Y_C(\ell)$. We conclude in the style of Euclid: for any finite set $\{(E_i', C_i')\}_i \in Y_C(\ell)(\mathbb{Q})$ corresponding to $t_i \in \mathbb{Q}$, we can find p such that $\operatorname{ord}_p(j(E_i')) \geq 0$ and there exists $t^* \in \mathbb{Q}$ giving $(E^*, C^*) \in Y_C(\ell)(\mathbb{Q})$ such that $\operatorname{ord}_{\mathfrak{p}}(j(E_{t^*})) < 0$. 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^*, C^*) 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. □

We will also make use of the following variant, when C has trivial Galois action.

Proposition 3.2.6. *There are infinitely many pairs E_1, E_2 of elliptic curves satisfying the following:*

(i) *The image of $\rho_{E_1 \times E_2, \ell}$ is the subgroup*

$$\left\{ \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ \ell c_1 & d_1 & 0 & 0 \\ 0 & 0 & a_2 & b_2 \\ 0 & 0 & \ell c_2 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{l} a_1 \equiv a_2 \equiv 1 \pmod{\ell}, \textit{ and} \\ a_1 d_1 - \ell b_1 c_1 = a_2 d_2 - \ell b_2 c_2 \end{array} \right\} \leqslant \mathrm{GL}_4(\mathbb{Z}_\ell); \tag{3.2.7}$$

in particular, there exist points $P_1 \in E_1[\ell](\mathbb{Q})$ and $P_2 \in E_2[\ell](\mathbb{Q})$ of order ℓ; and

(ii) *The products $E_1 \times E_2$ fall into infinitely many distinct geometric isogeny classes.*

Proof. Repeat the same argument as in Proposition 3.2.5, but sourcing the initial pair in the parameter space $Y_1(\ell)$. □

For convenience, we rewrite the elements in G_ℓ (defined in (3.2.4)) as

$$\begin{pmatrix} a + x_1\ell & b_1 + y_1\ell & 0 & 0 \\ w_1\ell & d + z_1\ell & 0 & 0 \\ 0 & 0 & a + x_2\ell & b_2 + y_2\ell \\ 0 & 0 & w_2\ell & d + z_2\ell \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \tag{3.2.8}$$

where:

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

still subject to the condition (Weil pairing) that

$$\det(A_1) = \det(A_2). \tag{3.2.9}$$

Now, we follow the recipe given in Construction 2.3.7 to write down the change of coordinates matrix for $\Psi(q) \subseteq V_\ell(E_1 \times E_2)$. Let $P_{1,1} := P_1 \bmod \ell \in E_1[\ell](\mathbb{Q}^{\mathrm{al}})$ and $Q_{1,1} := Q_1 \bmod \ell \in E_2[\ell](\mathbb{Q}^{\mathrm{al}})$, so we can write $\bar{A} = \left(\bar{E}_1 \times \bar{E}_2\right) / \langle P_{1,1} + Q_{1,1} \rangle$. Then the change of coordinates matrix $M_{q,\ell}$ is given by

$$M_{q,\ell} = \begin{pmatrix} 1 & 0 & 1/\ell & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{3.2.10}$$

As explained in section 2.2 (cf. Lemma 2.2.5), to understand the Galois action on $A[\ell](\mathbb{Q}^{\mathrm{al}})$, we conjugate the elements (3.2.8) above by this change of coordinates matrix, which gives

$$\begin{pmatrix} a+x_1\ell & b_1+y_1\ell & x_1-x_2 & -b_2-y_2\ell \\ w_1\ell & d+z_1\ell & w_1 & 0 \\ 0 & 0 & a+x_2\ell & b_2\ell+y_2\ell^2 \\ 0 & 0 & w_2 & d+z_2\ell \end{pmatrix} \tag{3.2.11}$$

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

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

Proof. We need to check that the determinant condition (3.2.9) being satisfied does not constrain our choices of variables above: it requires that

$$ad + (dx_1 + az_1 - b_1w_1)\ell + (x_1z_1 - w_1y_1)\ell^2 = ad + (dx_2 + az_2 - b_2w_2)\ell + (x_2z_2 - w_2y_2)\ell^2.$$

We may deduce that

$$z_1 - z_2 = a^{-1}(b_1w_1 - b_2w_2 - dx_1 + dx_2) \in \mathbb{F}_\ell \tag{3.2.13}$$

so for every $a,d \in \mathbb{F}_\ell^\times$ 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. □

3.3. **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 3.3.1. *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 $n \in \mathbb{Z}_{\geq 1}$, where $\bar{\rho}_{A,\ell^n}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_\ell}(A[\ell^n])$.*

Proof. There is a 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 $A[\ell^n] \times A^\vee[\ell^n] \to \mu_{\ell^n}$. This is a perfect bilinear pairing, hence non-degenerate, and so the result follows. □

By the Weil pairing, the cyclotomic character is given by multiplication by ad [Sil09, section III.8]. Thus, when we take the inverse transpose of matrices as in Proposition 3.2.12 and scale by this factor, we get the following.

Proposition 3.3.2. *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*

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

where $z_1 - z_2 = a^{-1}(b_1w_1 - b_2w_2 - dx_1 + dx_2) \in \mathbb{F}_\ell$.

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

$$a^{-1}(b_1w_1 - b_2w_2 - dx_1 + dx_2) = z_1 - z_2$$

by the determinant condition (3.2.13). □

Remark 3.3.3. We observe directly that the semisimplifications remain as they were for $E_1 \times E_2$, corresponding to the representation $\chi^{\oplus 2} \oplus (\varepsilon_\ell \chi^{-1})^{\oplus 2}$ where $\chi\colon \mathrm{Gal}_{\mathbb{Q}} \to (\mathbb{F}_\ell)^\times$ corresponds to the Galois action on $C_1 \simeq C_2$.

3.4. **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 2, 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 3.1.2 to relate their Galois representations.

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 2.4.3), as shown in the following commutative diagram:

(3.4.1)
$$\begin{tikzcd}
E_1 \times E_2 \arrow[r, "\ell\lambda_0"] \arrow[d, "q"] & (E_1 \times E_2)^\vee \\
A \arrow[r, "\lambda"] & A^\vee. \arrow[u, "q^\vee"']
\end{tikzcd}$$

Using the framework developed in section 2.2, 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 $V_\ell(E_1 \times E_2)$. Taking $E_1 \times E_2$ to be A_0, we have already chosen a change of basis matrix $M_{q,\ell}$ (3.2.10) for $\Psi(q)$ in $V_\ell(E_1 \times E_2)$ and computed the Galois action on $T_\ell A$ in (3.2.11). We could compute the Galois action on $T_\ell A^\vee$ either by choosing a change of basis matrix $M_{\lambda\circ q,\ell}$ and using it to conjugate the action on $T_\ell(E_1 \times E_2)$ or, equivalently, by choosing a change of basis matrix $M_{\lambda,\ell}$ relating $\Psi(q)$ to $\Psi(\lambda \circ q)$and using it to conjugate the action on $T_\ell A \simeq \Psi(q)$. We will take the second approach here.

First, we compute a matrix of transformation for the map $V_\ell\lambda\colon V_\ell A \to V_\ell A^\vee$ induced by the polarization λ, which will also allow us to computationally verify that the pushforward of λ_0 by q is a $(1,\ell)$-polarization.

We will use the choices of basis for $T_\ell(E \times F)$ and $T_\ell A$ from section 3.2 and then pick the basis of $T_\ell A^\vee$ to be dual to that of $T_\ell A$. We may take the matrix of $N_{\ell\lambda_0,\ell}$ to be the following:

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

Then from (3.4.1) we have $N_{\ell\lambda_0,\ell} = N_{q^\vee,\ell} N_{\lambda,\ell} N_{q,\ell}$. Using Lemma 2.3.1 and (2.4.6), we may rearrange this to $N_{\lambda,\ell} = M_{q,\ell}^T N_{\ell\lambda_0,\ell} M_{q,\ell}$, which we now compute:

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

The cokernel of this matrix (which is isomorphic to the kernel of λ) applied to $T_\ell A$ has ℓ^2 elements, confirming that the type of this polarization λ is $(1,\ell)$. As discussed in section 2.4, we may apply Lemma 2.3.1 to find that the change of coordinates matrix $M_{\lambda,\ell} = N_{\lambda,\ell}^{-1}$. Thus,

$$M_{\lambda,\ell} = \begin{pmatrix} 0 & -1/\ell & 0 & 1/\ell \\ 1/\ell & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ -1/\ell & 0 & 1 & 0 \end{pmatrix}.$$

Now, to understand the action of the Galois group on $\Psi(\lambda \circ q)$, we conjugate the subgroup corresponding to the action on $T_\ell A$ given in (3.2.11), by $M_{\lambda,\ell}$. This gives the subgroup

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

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

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

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

which agrees with that calculated in Section 3.3, as it should.

4. Proofs of Theorems

4.1. **Proof of the main result.**

We now prove Theorem 1.2.1, which we restate for convenience.

Theorem 4.1.1. *Let $\ell \leqslant 7$ be prime. Then there exist infinitely many pairwise geometrically non-isogenous abelian surfaces A over $\mathbb{Q}$ such that $A[\ell] \not\simeq A^\vee[\ell]$ as group schemes over $\mathbb{Q}$.*

Proof. Let A be an abelian surface over $\mathbb{Q}$ as in Construction 3.1.1, with E_1, E_2 coming from the infinite set in Proposition 3.2.5.

Let $\sigma \in \mathrm{Gal}_\mathbb{Q}$. Then Proposition 3.2.12 gives

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

for some $a, b_1, b_2, x_1, x_2, w_1, w_2, d \in \mathbb{F}_\ell$ with $a, d \in \mathbb{F}_\ell^\times$. Then Proposition 3.3.2 gives

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

where

$$z_1 - z_2 = a^{-1}(b_1 w_1 - b_2 w_2 - d x_1 + d x_2) \in \mathbb{F}_\ell.$$

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 consider one-dimensional subspaces in $\mathbb{F}_\ell^4$ fixed by either subgroup of $\mathrm{GL}_4(\mathbb{F}_\ell)$. We observe that both subgroups have a unique Galois-stable line: in $A[\ell](\mathbb{Q}^{\mathrm{al}})$, it is the span of P_1, the first basis element, and the Galois group acts on it by multiplcation by a. In $A^\vee[\ell](\mathbb{Q}^{\mathrm{al}})$, the fixed line is the span of Q_1, the third basis element, and the Galois group acts on it by multiplication by d. On $A[\ell](\mathbb{Q}^{\mathrm{al}})$, the action by a is the character χ of $\mathrm{Gal}_\mathbb{Q}$ (introduced in Remark 3.3.3). On $A^\vee[\ell](\mathbb{Q}^{\mathrm{al}})$, by the Weil pairing, the action by d is the character $\varepsilon_\ell\chi^{-1}$, where ε_ℓ is the cyclotomic character of $\mathrm{Gal}_\mathbb{Q}$. Of course $\chi \simeq \varepsilon_\ell\chi^{-1}$ if and only if $\chi^2 \simeq \varepsilon_\ell$. But this equation has no solution in the character group of $\mathrm{Gal}_\mathbb{Q}$! Indeed, the character χ has order dividing $\ell - 1$ so χ^2 has order a proper divisor of $\ell - 1$; but ε_ℓ has order exactly $\ell - 1$. □

4.2. **Associated permutation representations.** Often, in understanding the cohomology of a smooth projective variety X over a field k, we may first try to identify the image of the cycle class map

$$\mathrm{CH}^i X_{k^{\mathrm{sep}}} \to H^{2i}_{\text{ét}}(X_{k^{\mathrm{sep}}}, \mathbb{Q}_{\ell'}(i)),$$

where ℓ' is a prime different from the characteristic of k. The image, as a Gal_k-subrepresentation of $H^{2i}_{\text{ét}}(X_{k^{\mathrm{sep}}}, \mathbb{Q}_{\ell'}(i))$, is the $\mathbb{Q}_{\ell'}$-linear representation associated to the permutation representation determined by the Galois action on the codimension i algebraic cycles in $X_{k^{\mathrm{sep}}}$.

Thus, 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. In fact, in [FH23], the induced linear representations corresponding to $A[3](\mathbb{Q}^{\mathrm{al}})$ and $A^\vee[3](\mathbb{Q}^{\mathrm{al}})$ arise as sub-representations in the middle ℓ'-adic cohomology of generalized Kummer fourfolds over $\mathbb{Q}$ associated to A and $A^\vee$, respectively.

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 $\bar{\rho}_{A,\ell}$.

Proposition 4.2.1. *Let A be an abelian surface constructed as in Construction 3.1.1 and and coming from a pair E_1, E_2 as in Proposition 3.2.5. Then the following statements hold.*

(i) *If $\ell = 2$, then $\pi_{A,2}$ and $\pi_{A^\vee,2}$ are isomorphic.*

(ii) *If $\ell = 3$ and the Galois action on $C_1 \simeq C_2$ is nontrivial, then $\pi_{A,3}$ and $\pi_{A^\vee,3}$ are isomorphic.*

Proof. The subgroups from Propositions 3.2.12 and 3.3.2 can be considered as subgroups of S_{ℓ^4} acting on $\mathbb{F}_\ell^4$. We check in Magma that these subgroups are conjugate subgroups in S_{ℓ^4} for $\ell = 2, 3$ [FHV23]. □

The above proposition shows, interestingly, that the change from the representation $\bar{\rho}_{A,\ell}$ to the permutation representation $\pi_{A,\ell}$ is non-trivial (that is, information is lost). However, this is not always the case, as the next result shows.

Next, we consider abelian surfaces A constructed as in Construction 3.1.1 but with $C_1 \simeq C_2 \simeq (\mathbb{Z}/\ell\mathbb{Z})_{\mathbb{Q}}$ having trivial Galois action, as in Proposition 3.2.6. In this case, the fact that $A[\ell] \not\simeq A^\vee[\ell]$ as finite group schemes can be read off directly from the Galois representations in Proposition 3.2.12 and Proposition 3.3.2: for $\ell \in \{3,5,7\}$, $A[\ell](\mathbb{Q}) \neq \emptyset$ while $A^\vee[\ell](\mathbb{Q}) = \emptyset$ (as above, we check $\ell = 2$ separately by hand, since both have ℓ-torsion points over $\mathbb{Q}$). Moreover, at least for $\ell = 3$, the following shows that the permutation and linear representations remain non-isomorphic.

Proposition 4.2.2. *Let A be an abelian surface constructed as in Construction 3.1.1 with $C_1 \simeq C_2$ having trivial Galois action and coming from a pair E_1, E_2 as in Proposition 3.2.6.*

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

Proof. We can see this computationally in multiple ways; see the Magma code provided [FHV23]. For the permutation representations, we 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. (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. □

4.3. **Final remarks.** We pause to prove the statement about semisimplifications made in the introduction.

Lemma 4.3.1. *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. □

Proposition 4.3.2. *The following statements hold.*

(a) *The subgroup $G \leqslant \mathrm{GL}_4(\mathbb{F}_2)$ of elements preserving (up to scaling) the unique rank 1 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 78 for which the natural inclusion $H \hookrightarrow G \leqslant \mathrm{GL}_4(\mathbb{F}_2)$ is not equivalent to its (twisted) contragredient. Of these, 52 have the property that the image in $\mathrm{GL}_4(\mathbb{F}_2)$ of the twisted contragredient is not even a conjugate subgroup.*

Proof. This follows from a direct calculation with matrix groups, which was performed in Magma; see the code accompanying this paper. □

The list of groups from Proposition 4.3.2(b) is already quite interesting: the smallest group has size 4, the largest is G itself!

We conclude with a few final remarks.

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.

Finally, 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

[BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd. ed., Grundlehren der Mathematischen Wissenschaften, vol. 302, Springer-Verlag, Berlin, 2004. 2.4

[BS23] Pawel Borówka and Anatoli Shatsila, *Hyperelliptic genus 3 curves with involutions and a Prym map*, 2023, preprint, `arXiv:2308.07038`. 3.1

[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. 4.1

[Bru17] Peter Bruin, *Dual pairs of algebras and finite commutative group schemes*, 2017, preprint, `arXiv:1709.09847`. 4.3

[CP10] Brian Conrad and Bjorn Poonen, *Non-principally polarized complex abelian varieties*, 2010, `https://mathoverflow.net/q/17014`. 3.1

[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. 3.2

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[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. 1.3, 4.2

[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`. 4.1, 4.2, 4.2

[FLV23+] Victoria Cantoral-Farfán, Davide Lombardo, and John Voight, *Monodromy groups of Jacobians with definite quaternionic multiplication*, 2023, preprint, `arXiv:2203.08593`. 3.2

[Gor02] Eyal Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Ser., vol. 14, Amer. Math. Soc., Providence, RI, 2002. 3.1

[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. 4.3

[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. 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.

[Lan13] Kai-Wen Lan, *Arithmetic compactifications of PEL-type Shimura varieties*, London Math. Soc. Monogr. Ser., vol. 36, Princeton University Press, Princeton, 2013. 2.1.12

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

[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. 2.4.3

[Rém18] Gaël Rémond, *Conjectures uniformes sur les variétés abéliennes*, Q. J. Math. **69** (2018), no. 2, 459–486. 4.3

[Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804.

[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. 3.2

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

[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. 3.1

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009. 3.2, 3.3

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Zyw23] David Zywina, *Families of abelian varieties and large Galois images*, Int. Math. Res. (2002), published online, 1–58. 3.2

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
Email address: jvoight@gmail.com