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.

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 $n \geq 1$, we obtain a representation of $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$

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

Here we compare the representation $\overline{\rho}_{A,n}$ to the representation $\overline{\rho}_{A^\vee,n}$ associated with the dual abelian variety $A^\vee := \mathbf{Pic}^0_A$. The Weil pairing yields a canonical isomorphism

$$\overline{\rho}_{A^\vee,n} \cong \overline{\rho}^{*}_{A,n} \otimes \varepsilon_n \tag{1.1.2}$$

of Galois representations, where * denotes the contragredient representation.

In general, these two linear representations are quite challenging to distinguish. For most abelian varieties one encounters, there is an isomorphism $\overline{\rho}_{A,n} \simeq \overline{\rho}_{A^\vee,n}$. Indeed, if A has a polarization $\lambda \colon A \to A^\vee$ over K whose degree is coprime to n—such as if A is principally polarized over K—then the polarization induces such an isomorphism. In general, the number fields $K(A[n])$ and $K(A^\vee[n])$ are always *equal*, taken inside K^{al} (Lemma 3.2.2). Of course, since A and $A^\vee$ are isogenous over K, they have isomorphic ℓ-adic representations for all primes ℓ and hence the characteristic polynomials of $\overline{\rho}_{A,n}(\sigma)$ and $\overline{\rho}_{A^\vee,n}(\sigma)$ agree for all $\sigma \in \mathrm{Gal}_K$. In fact, for $n = \ell$ prime, the semi-simplifications of $\overline{\rho}_{A,\ell}$ and $\overline{\rho}_{A^\vee,\ell}$ are also isomorphic (Lemma 3.2.1).

1.2. **Results.** Our main result shows that these representations need not be isomorphic in general.

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 (1.1.2), 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.

It is enough to prove the theorem for $n = \ell \leqslant 7$ prime. We construct the abelian surfaces in Theorem 1.2.1 by choosing elliptic curves E_1, E_2 and nontrivial $P \in E_1[\ell](\mathbb{Q})$, $Q \in E_2[\ell](\mathbb{Q})$

Date: March 16, 2025.

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

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

and gluing 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* $\operatorname{char} k = 0$ *are not isomorphic.*

In general, we could consider the 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. We classify these groups in the case $g = n = 2$ in Proposition 3.2.4. 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. Theorem 1.2.1 can then be understood as exhibiting an explicit two-dimensional rational subspace for several such groups G.

1.3. **Application.** 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 [Huy19, §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 3.1.1) 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 3.2.2 below.

Also in the direction of derived equivalence, recall that, as seen in the proof of Theorem 2.5.1, 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].

1.4. **Contents.** In section 2 we exhibit our family of abelian surfaces, describe its basic properties, and complete the proof of Theorem 1.2.1. In section 3, 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. Constructions and computations

We begin with the construction of the abelian surfaces A used in Theorem 1.2.1. We then 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 $A^\vee$. Finally, we give the proof of our main theorem.

2.1. **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 2.6 how it can be generalized.

Construction 2.1.1. 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 2.5, we will use Construction 2.1.1 in the proof of Theorem 1.2.1.

Lemma 2.1.2. *With setup as in Construction 2.1.1, 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 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

$\phi := \lambda_0^{-1} \circ q^*\lambda \in \mathrm{End}(E_1 \times E_2)$ is an endomorphism of degree $(\ell d)^2$, fixed under the Rosati involution. Since E_1 and E_2 are not isogenous, we have

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

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. ☐

2.2. **Background on Hilbert irreducibility.** In this section, we quickly adapt the statement of the Hilbert irreducibility theorem for our purposes. For a reference, see Serre [Ser97, sections 9.2, 9.6] or [Ser92, Chapter 3], or Lang [Lang83, Chapter 9].

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). Suppose that $f_t(x)$ has 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 $K(t) = K(t_1, \ldots, t_n)$.

Theorem 2.2.1 (Hilbert irreducibility theorem)**.** *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]. ☐

Theorem 2.2.1 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 $G := \mathrm{Gal}(K(X) \mid K(U))$ 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.

We will need to apply Theorem 2.2.1 under multiple specializations: we will want not just that there are infinitely many G-extensions, but for these to be as disjoint as possible. See also recent work of Zywina [Zyw23], who studies families of abelian varieties with large Galois image in an effective manner.

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 2.2.2. *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 $K' = L(U \times U)$. $\square$

2.3. **Computation of the Galois action on** A. Let A be an abelian surface over $\mathbb{Q}$ as in Construction 2.1.1 with (E_1, P) and (E_2, Q) satisfying $P \in E_1[\ell](\mathbb{Q})$ and $Q \in E_2[\ell](\mathbb{Q})$.

Lemma 2.3.1. *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

$$\left\{ \begin{pmatrix} a & b \\ \ell c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_\ell) : a, d \in \mathbb{Z}_\ell^\times, a \equiv 1 \bmod \ell \right\} \leqslant \mathrm{GL}_2(\mathbb{Z}_\ell) \tag{2.3.2}$$

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

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

(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 (2.3.2).*

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 2.3.1(b) holds for a density 1 subset.

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

Part (b) follows from Hilbert irreducibility (Theorem 2.2.1), 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 $Y_H \to Y_1(\ell)$ 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 2.3.1, 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

$$\left\{ \begin{pmatrix} 1 & b_1 & 0 & 0 \\ 0 & d_1 & 0 & 0 \\ 0 & 0 & 1 & b_2 \\ 0 & 0 & 0 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : a_1, d_1, a_2, d_2 \in \mathbb{F}_\ell^\times \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell). \tag{2.3.3}$$

The Galois equivariance of the Weil pairing (given explicitly by the determinant) [Sil09, section III.8], which holds for any ℓ^n-torsion points (or more generally on $T_\ell(E)$), further implies that $\rho_{E_1\times E_2,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is contained in

$$G_\ell := \left\{ \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ \ell c_1 & d_1 & 0 & 0 \\ 0 & 0 & a_2 & b_2 \\ 0 & 0 & \ell c_2 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{l} a_1, d_1, a_2, d_2 \in \mathbb{Z}_\ell^\times, \\ a_1 \equiv a_2 \equiv 1 \bmod \ell, \text{ and} \\ a_1 d_1 - \ell b_1 c_1 = a_2 d_2 - \ell b_2 c_2 \end{array} \right\} \leqslant \mathrm{GL}_4(\mathbb{Z}_\ell). \tag{2.3.4}$$

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

Proposition 2.3.5. *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 (2.3.4); 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 2.3.1(b), we now apply HIT (Theorem 2.2.1), 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 (2.3.4). For this, we apply Proposition 2.2.2, 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. $\square$

For convenience, we rewrite the elements in G_ℓ (defined in (2.3.4)) as

$$\begin{pmatrix} 1+x_1\ell & b_1+y_1\ell & 0 & 0 \\ w_1\ell & d+z_1\ell & 0 & 0 \\ 0 & 0 & 1+x_2\ell & b_2+y_2\ell \\ 0 & 0 & w_2\ell & d+z_2\ell \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \tag{2.3.6}$$

where:

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

still subject to the condition (Weil pairing) that

$$\det A_1 = \det A_2. \tag{2.3.7}$$

Recall that $A = (E_1 \times E_2)/\langle (P,Q)\rangle$. Because A and $E_1 \times E_2$ are isogenous, we may choose the following change of coordinates matrix $M_{q,\ell}$ that allows us to compute the Galois action on A from the action on $E_1 \times E_2$:

$$M_{q,\ell} = \begin{pmatrix} 1 & 0 & 1/\ell & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.3.8}$$

Conjugating the elements (2.3.6) above by this change of coordinates matrix (i.e. we compute $M_{q,\ell}^{-1} G_\ell M_{q,\ell}$), gives

$$\begin{pmatrix} 1 + x_1\ell & b_1 + y_1\ell & x_1 - x_2 & -b_2 - y_2\ell \\ w_1\ell & d + z_1\ell & w_1 & 0 \\ 0 & 0 & 1 + x_2\ell & b_2\ell + y_2\ell^2 \\ 0 & 0 & w_2 & d + z_2\ell \end{pmatrix} \tag{2.3.9}$$

with the same conditions on the variables. This computation of the Galois action on $T_\ell(A)$ via the action on $T_\ell(E_1 \times E_2)$, including why $M_{q,\ell}$ is the appropriate matrix by which to conjugate, is explained in detail in [FHV25].

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 2.3.10. *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 (2.3.7) 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

$$z_1 - z_2 = b_1w_1 - b_2w_2 - dx_1 + dx_2 \in \mathbb{F}_\ell, \tag{2.3.11}$$

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. $\square$

2.4. **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 2.4.1. *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 $T_\ell A \times T_\ell A^\vee \to \mathbb{Z}_\ell(1)$ is 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. $\square$

By the Weil pairing, the cyclotomic character is given by multiplication by d [Sil09, section III.8]. Thus, when we take the inverse transpose of matrices as in Proposition 2.3.10 and scale by this factor, we get the following.

Proposition 2.4.2. *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 $z_1 - z_2 = b_1 w_1 - b_2 w_2 - d x_1 + d x_2 \in \mathbb{F}_\ell$.

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

$$b_1 w_1 - b_2 w_2 - d x_1 + d x_2 = z_1 - z_2$$

by the determinant condition (2.3.11). □

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

Theorem 2.5.1. *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 2.1.1, with the pair E_1, E_2 coming from the infinite set in Proposition 2.3.5.

Let $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. Then Proposition 2.3.10 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 2.4.2 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

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

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 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 2.4.2.) 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). □

2.6. **Generalizing the construction.** It is possible to generalize Construction 2.1.1 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 2.1–2.5 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 2.1.1.

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 (2.3.2), 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 (2.3.3) and (2.3.4). Then the proof of Proposition 2.3.5 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 2.3-2.4. 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 $\mathbb{Q}$.

3. Further analysis and discussion

With Theorem 1.2.1 now proven, we conclude with an application and some final remarks. In section 3.1, we examine the associated permutation representations, proving Corollary 1.2.2 and giving an application to derived equivalences of Kummer fourfolds. In section 3.2, 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.

3.1. **Associated permutation representations.** 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 2.1.1 are also non-isomorphic, which proves Corollary 1.2.2.

Proposition 3.1.1. *Let A be an abelian surface constructed as in Construction 2.1.1, coming from a pair E_1, E_2 as in Proposition 2.3.5.*

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 $\operatorname{char} F = 0$ are not isomorphic.

Proof. We can see this computationally in multiple ways; see the Magma code provided [FHV23]. For the permutation representations, we 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 3.1.2. 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 3.1.1. We check in Magma that the subgroups from Propositions 2.3.10 and 2.4.2 are conjugate subgroups in S_{2^4} [FHV23].

(2) In section 2.6, 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 3.1.1 stands in contrast to these results.

3.2. **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 3.2.1. *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 3.2.2. *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 3.2.3. 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 3.2.4.) 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 3.2.4. *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 3.2.4(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

[AKW17] Benjamin Antieau, Daniel Krashen, and Matthew Ward, *Derived categories of torsors for abelian schemes*, Adv. Math. **306** (2017), 1–23. 1.3

[BS23] Pawel Borówka and Anatoli Shatsila, *Hyperelliptic genus 3 curves with involutions and a Prym map*, 2023, preprint, `arXiv:2308.07038`. 2.1

[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. 2.5

[Bru17] Peter Bruin, *Dual pairs of algebras and finite commutative group schemes*, 2017, preprint, `arXiv:1709.09847`. 3.2

[CP10] Brian Conrad and Bjorn Poonen, *Non-principally polarized complex abelian varieties*, 2010, https://mathoverflow.net/q/17014. 2.1

[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. 2.3

[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. 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. 2.5, 3.1, 1, 2, 3.2

[FHV25] Sarah Frei, Katrina Honigs, and John Voight, *A framework for Tate modules of abelian varieties under isogeny*, 2025, in preparation. 2.3

[FLV23+] Victoria Cantoral-Farfán, Davide Lombardo, and John Voight, *Monodromy groups of Jacobians with definite quaternionic multiplication*, 2023, preprint, `arXiv:2203.08593`. 2.3

[Gor02] Eyal Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Ser., vol. 14, Amer. Math. Soc., Providence, RI, 2002. 2.1

[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. 3.2

[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. 1.3

[Huy19] Daniel Huybrechts, *Motives of isogenous K3 surfaces*, Comment. Math. Helv. **94** (2019), no. 3, 445–458. 1.3

[Lang83] Serge Lang, *Fundamentals of Diophantine geometry*, Springer, New York, 1983. 2.2

[Mil12] James S. Milne, *Algebraic geometry (v5.22)*, 2012, available at http://www.jmilne.org/math/. 2.2

[Muk81] Shigeru Mukai, *Duality between $D(X)$ and $D(X^\vee)$ with its application to Picard sheaves*, Nagoya Math. J.81(1981), 153–175. 1.3

[Rém18] Gaël Rémond, *Conjectures uniformes sur les variétés abéliennes*, Q. J. Math. **69** (2018), no. 2, 459–486. 3.2

[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. 2.3

[Sal82] David J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), no. 3, 250–283. 2.2

[Ser92] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett, Boston, MA, 1992. 2.2, 2.2

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Aspects Math., Friedr. Vieweg & Sohn, Braunschweig, 1997. 2.2, 2.2

[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. 2.6

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

[Wit24] Olivier Wittenberg, *Park City lecture notes: around the inverse Galois problem*, IAS/Park City Mathematics Series, AMS, to appear. 2.2

[Zyw23] David Zywina, *Families of abelian varieties and large Galois images*, Int. Math. Res. (2002), published online, 1–58. 2.2

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