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 $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$

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

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

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

of Galois representations, where * denotes the contragredient representation and ε_n is the cyclotomic character.

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); so $\rho_{A,n}$ and $\rho_{A^\vee,n}$ arise from representations of the same finite Galois group. 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 particular, 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 with nontrivial $P \in E_1[\ell](\mathbb{Q})$, $Q \in E_2[\ell](\mathbb{Q})$ and gluing E_1, E_2 along the diagonal subgroup $\langle(P,Q)\rangle$. The resulting abelian surfaces 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 essentially the product $Y_1(\ell) \times Y_1(\ell)$ of modular curves (with a slight reinterpretation required for $\ell = 2$); for $\ell \leqslant 7$, this space is birational to $\mathbb{A}^2$. We may therefore adjust the setup or ask for additional properties to be satisfied in Theorem 1.2.1. For example, our results can be extended over any number field K with $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$, see section 2.5. On the other hand, for $\ell > 7$, $Y_1(\ell)$ has genus greater than zero and fails to have infinitely many points over $\mathbb{Q}$; thus our construction cannot guarantee a distinction in $A[\ell]$ and $A^\vee[\ell]$ over $\mathbb{Q}$.

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 we exhibit to prove Theorem 1.2.1 satisfy the stronger property that $\pi_{A,n} \not\simeq \pi_{A^\vee,n}$ for $\ell \in \{3, 5, 7\}$.

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

One could further consider 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 3.2.5. 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 Huybrechts [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 $K(A^\vee[3]) = K(A[3])$.

Also in the direction of derived equivalence, recall that, as seen in the proof of Theorem 1.2.1, the abelian surfaces are such that $A[3](\mathbb{Q})$ is nontrivial but $A^\vee[3](\mathbb{Q})$ is trivial. 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.

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 $V_\ell A_0$, where A_0 is a product of two elliptic curves and A is isogenous to A_0. 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 $\mathrm{Gal}_k := \mathrm{Gal}(k^{\mathrm{sep}} \mid k)$ and let $\ell \neq \mathrm{char}\, k$ 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 recently exhibited [BS23, Theorem 2.5]. We present our own 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 points of order ℓ. Let

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

and let $q \colon E_1 \times E_2 \to A$ be the quotient map.

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. First part (a). Since G is defined over k, so too is A defined over k. We have the principal product polarization λ_0 on $E_1 \times E_2$; it is a symmetric isogeny, so $\lambda_0^\vee = \lambda_0$ under the canonical isomorphism of an abelian variety with its double dual. Since G is isotropic (the pairing is alternating and the group is cyclic) and λ_0 is a principal polarization, the pushforward under q of λ_0 provides a $(1, \ell)$-polarization λ on A.

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 $q^*\lambda := q^\vee \circ \lambda \circ q$, a polarization on $E_1 \times E_2$, so again $(q^*\lambda)^\vee = q^*\lambda$. The composition $\phi := \lambda_0^{-1} \circ q^*\lambda \in \mathrm{End}(E_1 \times E_2)$ is an endomorphism of degree $(\ell d)^2$. Further, ϕ is fixed under the Rosati involution † (associated to λ_0):

$$(2.1.3) \qquad \phi^\dagger := \lambda_0^{-1}\phi^\vee\lambda_0 = \lambda_0^{-1}(\lambda_0^{-1} \circ q^*\lambda)^\vee\lambda_0 = \lambda_0^{-1}(q^*\lambda)(\lambda_0^{-1})\lambda_0 = \lambda_0^{-1}(q^*\lambda) = \phi.$$

Since by hypothesis E_1 and E_2 are not isogenous over k, we have

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

(endomorphisms over k). 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 $d_1d_2 = \ell d$. Since ϕ factors through q, we have the containment $\ker q \subseteq \ker \phi = E_1[d_1] \times E_2[d_2]$.

Now assume for purposes of contradiction 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. $\qquad\square$

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

$$(2.2.1) \qquad f_t(x) = f(t_1, ..., t_n; x) \in K(t_1, ..., t_n)[x]$$

be an irreducible polynomial of degree d over $K(t_1, \ldots, t_n)$, the function field of $\mathbb{A}_K^n$ in the variables $t_1, \ldots, t_n$. The coefficients of $f_t(x)$ are simultaneously defined on a nonempty open subset $U \subseteq \mathbb{A}_K^n$ (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).

Theorem 2.2.2 (Hilbert irreducibility theorem). *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 nontrivial 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]. $\qquad\square$

Since K is Hilbertian, the set of points of $U(K)$ outside a thin set $Z \subseteq U$ has density 1 in the sense that

$$(2.2.3) \qquad \lim_{B \to \infty} \frac{\#\{P \in (U \smallsetminus Z)(K) : \mathrm{ht}(P) \leq B\}}{\#\{P \in U(K) : \mathrm{ht}(P) \leq B\}} = 1$$

where $\mathrm{ht} \colon U(K) \to \mathbb{Q}_{>0}$ is the usual height [Ser97, §9.7].

Theorem 2.2.2 can be understood geometrically, as follows.

Corollary 2.2.4. *Let $X \to U$ be a finite morphism over K with X irreducible. Then for points $t \in U(K)$ outside of a thin set, the fiber X_t is irreducible over K. If further $X \to U$ is generically Galois with generic Galois group $G := \operatorname{Gal}(K(X) \mid K(U))$, then for $a \in U(K)$ outside of a thin set the fiber $X_a \to \operatorname{Spec} K$ is also a G-Galois cover.*

Proof. This is merely a restatement of Theorem 2.2.2. Explicitly, if $U = \operatorname{Spec} A \subseteq \mathbb{A}_K^n$ is affine with $A \subseteq K(t_1, \ldots, t_n)$ (a finitely generated K-subalgebra with fraction field equal to $K(t_1, \ldots, t_n)$), we could take $X = \operatorname{Spec} A[x]/(f_t(x)) \to U$. $\qquad\square$

We will need to apply Theorem 2.2.2 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.

Proposition 2.2.5. *Let X be irreducible and $X \to U$ a finite morphism that is generically Galois with group $G := \operatorname{Gal}(K(X) \mid K(U))$. Let $L \supseteq K$ be the algebraic closure of K in $K(X) \supseteq K(U)$. Then the following statements hold.*

(a) *X has a canonical structure as a variety over L, corresponding to a factorization $X \to U_L \to U$ where $U_L := U \times_K L$.*

(b) *$X \times_L X$ is irreducible, and when considered as a K-scheme $(X \times_L X)_K$ it is irreducible.*

(c) *Let $G_0 := \operatorname{Gal}(L \mid K) \cong \operatorname{Gal}(L(U) \mid K(U))$ and let $\pi \colon G \to G_0$ be the restriction map. Then the natural morphism $(X \times_L X)_K \to U \times_K U$ is a finite generically Galois morphism with Galois group*

$$(2.2.6) \qquad G \times_{G_0, \pi} G := \{(\sigma_1, \sigma_2) : \pi(\sigma_1) = \pi(\sigma_2)\}.$$

(d) *For all $(a, b) \in (U \times_K U)(K)$ outside a thin set, the fiber $(X \times_K X)_{(a,b)} \to \operatorname{Spec} K$ has splitting field with Galois group $G \times_{G_0, \pi} G$.*

Proof. We first prove part (a). The fact that X is an L-variety is a standard fact: in an affine patch as above with $B := A[x]/(f_t(x))$, we have $L \hookrightarrow \operatorname{Frac}(B)$ so $B \cap L$ has $\operatorname{Frac}(B \cap L) = L$ but contains K so must be L, and so we get injective maps $A \hookrightarrow A \otimes_K L \hookrightarrow B$ (the second map under multiplication) giving the desired factorization.

For (b), we briefly recall the standard proof that $X \times X$ is irreducible, taking $L = K$. Since X is irreducible there is a dense open affine domain $\operatorname{Spec} A \subseteq X$. Since K is algebraically closed in $K(X)$, it is algebraically closed in A. We then recall that $A \otimes_K A$ is a domain (see e.g. the proof of Milne [Mil12, Proposition 4.15]). Thus $\operatorname{Spec}(A \otimes_K A) \subseteq X \times X$ is irreducible, and we conclude the proof by taking the Zariski closure. And in general if Y is irreducible over L then the K-scheme Y_K is also irreducible (the topology has not changed, just the structure map).

Next, part (c). We first prove the statement for $K = L$. Then $X \times_K X$ is irreducible by (b), and we want to show $\operatorname{Gal}(K(X \times X) \mid K(U \times U)) = G \times G$. We have a diagram

(2.2.7)

$$
\begin{array}{ccc}
 & X \times_K X & \\
\swarrow & & \searrow \\
X \times_K U & & U \times_K X \\
\searrow & & \swarrow \\
 & U \times_K U &
\end{array}
$$

where the bottom maps are G-extensions. By irreducibility, we get a corresponding field diagram of function fields over K. By basic Galois theory (e.g. [DF04, §14.4, Proposition 21, p. 592]), we need to show that $K(X \times U)$ and $K(U \times X)$ are linearly disjoint over $K(U \times U)$. By the universal property of the fiber product we have

$$X \times X \cong (U \times X) \times_{U \times U} (X \times U)$$

as K-schemes (the condition that maps factor through is automatic). Taking generic points shows that

$$K(X \times X) \cong K(U \times X) \otimes_{K(U \times U)} K(X \times U);$$

since $K(X \times X)$ is a field (as $X \times X$ is irreducible), we conclude that $K(U \times X)$ and $K(X \times U)$ are linearly disjoint over $K(U \times U)$ and $K(X \times_K X)$ is their compositum. The claim follows.

Now the general case, finishing (c). In an open affine as in (a), the natural map is

$$A \otimes_K A \to B \otimes_K B \to (B \otimes_L B)_K.$$

By (b), the scheme $X \times_L X$ is irreducible. We consider the diagram of fields, using (a):

(2.2.8)

$$
\begin{array}{ccc}
& L(X \times_L X) = K((X \times_L X)_K) & \\
L(X \times_L U_L) & & L(U_L \times_L X) \\
& L(U_L \times_L U_L) = L(U \times_K U) & \\
& | & \\
& K(U \times_K U) &
\end{array}
$$

Applying the case over $L = K$, we get that the top diamond (2.2.8) is a compositum of linearly disjoint extensions. Since $\operatorname{Gal}(L(U \times_K U) \mid K(U \times_K U)) \cong \operatorname{Gal}(L \mid K)$, we conclude that (2.2.6) holds as above by basic Galois theory.

Part (d) follows by applying Corollary 2.2.4 to (c) as follows. We have $X_a = \operatorname{Spec} B_a$ and $X_b = \operatorname{Spec} B_b$ where B_a, B_b are fields, so $(X \times_K X)_{(a,b)} \cong \operatorname{Spec}(B_a \otimes_K B_b)$ and similarly $((X \times_L X)_K)_{(a,b)} \cong \operatorname{Spec}(B_a \otimes_L B_b)$. Outside of a thin set, we have B_a, B_b linearly disjoint over L so $B_a \otimes_L B_b = B_a B_b$ is the compositum and $B_a \otimes_K B_b \simeq \prod_{\sigma \in \operatorname{Gal}(L|K)} B_a B_b$ [FT93, Exercise I.2, p. 335], showing that the two fibers have the same splitting field. □

2.3. **Computation of the Galois action on** A. Now let K be a number field linearly disjoint from $\mathbb{Q}(\zeta_\ell)$ (i.e., $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$), and let K^{al} be the algebraic closure. Let A be an abelian surface over K as in Construction 2.1.1 with (E_1, P) and (E_2, Q) satisfying $P \in E_1[\ell](K)$ and $Q \in E_2[\ell](K)$ nontrivial.

We recall that the modular curve $Y_1(\ell)$ is a coarse moduli space for the functor which associates to a scheme S the set of isomorphism classes of pairs (E, P) where E is an elliptic curve over S and $P \in E(S)$ is a point of order ℓ. For $\ell \geq 5$, in fact $Y_1(\ell)$ is a fine moduli space, so any point $[(E, P)] \in Y_1(\ell)(K)$ comes from a unique pair (E, P) over K. Explicitly and classically, we have the universal families in Tate normal form:

(2.3.1) $$\mathsf{E}_\ell \colon y^2 + (1 - c_\ell(t))xy - b_\ell(t)y = x^3 - b_\ell(t)x$$

where $(0,0)$ has order ℓ, and

(2.3.2)
$$(b_5(t), c_5(t)) = (t, t)$$
$$(b_7(t), c_7(t)) = (t^3 - t^2, t^2 - t)$$

For $\ell = 3$, the same conclusion holds whenever $j(E) \neq 0$ (such points have trivial stabilizer), and we may take the family

$$(2.3.3) \qquad\qquad\qquad \mathsf{E}_3 \colon y^2 + xy + ty = x^3$$

with $(0,0)$ of order 3 and $Y_1(3) \simeq \mathbb{P}^1 \smallsetminus \{0, 1/27, \infty\}$ in the variable t. Finally, for $\ell = 2$ the generic stabilizer is $\{\pm 1\}$, so with mild resignation we choose the family

$$(2.3.4) \qquad\qquad\qquad \mathsf{E}_2 \colon y^2 + xy = x^3 + tx$$

and again $(0,0)$ has order 2 and $Y_1(2) \simeq \mathbb{P}^1 \smallsetminus \{0, 1/64, \infty\}$ in t.

Lemma 2.3.5. *Let $\ell \leqslant 7$ be prime. Then the following statements hold.*

(a) *For all $t \in Y_1(\ell)(K)$ corresponding to $E = \mathsf{E}_{\ell,t}$, the image of the ℓ-adic Galois representation*

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

is contained in

$$(2.3.6) \qquad \left\{ \begin{pmatrix} a & b \\ \ell c & d \end{pmatrix} \in \operatorname{M}_2(\mathbb{Z}_\ell) : a, d \in \mathbb{Z}_\ell^\times, a \equiv 1 \ (\mathrm{mod}\ \ell) \right\} \leqslant \operatorname{GL}_2(\mathbb{Z}_\ell)$$

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

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

has image contained in

$$(2.3.7) \qquad\qquad \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in \operatorname{M}_2(\mathbb{F}_\ell) : d \in \mathbb{F}_\ell^\times \right\} \leqslant \operatorname{GL}_2(\mathbb{F}_\ell).$$

(b) *For all $n \geq 1$, the generic Galois group of $\mathsf{E}_\ell[\ell^n] \to Y_1(\ell) \subseteq \mathbb{P}^1_t$ is equal to G_{ℓ^n}, the reduction of (2.3.6) modulo ℓ^n. Moreover, the algebraic closure of K in $K(\mathsf{E}_\ell[\ell^n])$ is equal to $K(\zeta_{\ell^n})$.*

(c) *Outside of a thin set in $Y_1(\ell)(K)$, the image $\rho_{E,\ell}(\operatorname{Gal}_K)$ in (a) is the entire subgroup in (2.3.6).*

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

For part (b), for each $n \geq 1$ we will apply Hilbert irreducibility in the form of Corollary 2.2.4 applied to the cover $Y_{\mathrm{full}}(\ell^n) \to Y_1(\ell)$ where $Y_{\mathrm{full}}(\ell^n)$ is the modular curve parametrizing full level ℓ^n structure (see Deligne–Rapoport [DR73, IV-3.1] or Katz–Mazur [KM85, §3.1]). The same calculation in (a) shows that the generic Galois group is contained in G_{ℓ^n}, the reduction of (2.3.6) modulo ℓ^n; we need to show that equality holds.

We show equality by computing degrees. On base change to $L = K(\zeta_{\ell^n})$, we have $Y_{\mathrm{full}}(\ell^n)_L$ a disjoint union of components with a simply transitive action of $\operatorname{Gal}(L \mid K) \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ (since $K \cap \mathbb{Q}(\zeta_{\ell^n}) = K$), indexed by the value taken by the Weil pairing on the basis of ℓ^n-torsion. All components become isomorphic upon further base change to $\mathbb{C}$ to the usual modular curve $Y(\ell^n)(\mathbb{C})$ (rescaling the basis). The fundamental group of the cover $Y(\ell^n)(\mathbb{C}) \to Y_1(\ell)(\mathbb{C})$ is $G_{\ell^n} \cap \operatorname{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ (as the corresponding quotients of the upper half-plane, which is simply connected). This shows that the image of the generic Galois group modulo ℓ^n has size at least

$$\varphi(\ell^n)[\operatorname{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) : G_{\ell^n} \cap \operatorname{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})] = [\operatorname{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) : G_{\ell^n}]$$

so equality must hold. This argument proves the second moreover clause as well.

For part (c), we first apply Corollary 2.2.4 (Hilbert irreducibility) to $\mathsf{E}[\ell^n] \to Y_1(\ell)$ with $n = 2$ for $\ell \geq 3$ and $\ell^n = 8$ for $\ell = 2$. The result then holds after we recall the simple inductive lemma that if $H \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ is a closed subgroup such that

$$H \cap \left(1 + \ell^{n-1}\mathrm{M}_2(\mathbb{Z}/\ell\mathbb{Z})\right) = \left(1 + \ell^{n-1}\mathrm{M}_2(\mathbb{Z}/\ell\mathbb{Z})\right) \leq \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}),$$

then H is the full preimage of its image under natural projection $\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Indeed, computing degrees this follows from the fact the ℓth power map gives a surjection $1 + \ell^m\mathrm{M}_2(\mathbb{Z}/\ell\mathbb{Z}) \to 1 + \ell^{m+1}\mathrm{M}_2(\mathbb{Z}/\ell\mathbb{Z})$ (by the binomial formula) for all $m \geq n-1$. $\square$

Remark 2.3.8. In fact, all we need in our construction is to have surjectivity modulo ℓ^2: see Proposition 2.3.16.

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 2.3.5:
- $P_1 \bmod \ell = P \in E_1[\ell](K)$,
- $Q_1 \bmod \ell = Q \in E_2[\ell](K)$,
- $\{P_1, P_2\}$ 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 $(E_1 \times E_2)[\ell](K^{\mathrm{al}})$ has image contained in the subgroup

$$(2.3.9) \qquad \left\{ \begin{pmatrix} 1 & b_1 & 0 & 0 \\ 0 & d_1 & 0 & 0 \\ 0 & 0 & 1 & b_2 \\ 0 & 0 & 0 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : a_1, d_1, a_2, d_2 \in \mathbb{F}_\ell^\times \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell).$$

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 $\rho_{E_1 \times E_2, \ell}(\mathrm{Gal}_K)$ is contained in

$$(2.3.10) \qquad \left\{ \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ \ell c_1 & d_1 & 0 & 0 \\ 0 & 0 & a_2 & b_2 \\ 0 & 0 & \ell c_2 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{l} a_1, d_1, a_2, d_2 \in \mathbb{Z}_\ell^\times, \\ a_1 \equiv a_2 \equiv 1 \pmod{\ell}, \text{ and} \\ a_1 d_1 - \ell b_1 c_1 = a_2 d_2 - \ell b_2 c_2 \end{array} \right\} \leqslant \mathrm{GL}_4(\mathbb{Z}_\ell).$$

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

Proposition 2.3.11. *Let $\ell \leqslant 7$ be prime. There are infinitely many pairs E_1, E_2 of elliptic curves satisfying both of the following:*

(i) *The image of $\rho_{E_1 \times E_2, \ell}$ is the subgroup* (2.3.10)*; in particular, there exist points $P \in E_1[\ell](K)$ and $Q \in E_2[\ell](K)$ of order ℓ; and*

(ii) *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. To satisfy condition (i), analogous to Lemma 2.3.5(b), we now apply HIT (Theorem 2.2.2), taking the cover $\mathsf{E}_\ell[\ell^n] \times \mathsf{E}_\ell[\ell^n] \to Y_1(\ell) \times Y_1(\ell)$. For each factor, by Lemma 2.3.5(b) we know that the generic Galois group is G_{ℓ^n}, and the constant subextension is given by $L = K(\zeta_{\ell^n})$. The result then follows by applying Proposition 2.2.5(d).

To further satisfy (ii), let $E_1 \times E_2$ have large image as in (i), and suppose that there is an isogeny $\phi \colon E_1 \to E_2$ over a finite extension $K' \supseteq K$. Then the image of the restriction of $\rho_{E_1 \times E_2, \ell}$ to $\mathrm{Gal}_{K'}$ has finite index in $\rho_{E_1 \times E_2, \ell}(\mathrm{Gal}_K)$. And moreover the Tate module $T_\ell(E_{2,K'})$

is conjugate to $T_\ell(E_{1,K'})$ inside the latter's Tate representation $V_\ell(E_{1,K'}) := T_\ell(E_{1,K'}) \otimes \mathbb{Q}_\ell$. In particular, the image of $\rho_{(E_1 \times E_2)_{K'}, \ell}$ is contained in the subgroup

$$\left\{ \begin{pmatrix} A & 0 \\ 0 & PAP^{-1} \end{pmatrix} : A \in \mathrm{GL}_2(\mathbb{Z}_\ell) \right\} \leq \mathrm{GL}_4(\mathbb{Z}_\ell)$$

where P is the matrix of $\phi_\ell \colon T_\ell(E_{1,K'}) \to T_\ell(E_{2,K'})$. This subgroup has infinite index in the subgroup given by (b), a contradiction.

The final statement follows quite a bit more generally, see Cantoral-Farfán–Lombardo–Voight [FLV23+, Proposition 6.6.1]. In fact, we claim that even for fixed E_1, the curves E_2 that satisfy (i) and (ii) fall into infinitely many distinct geometric isogeny classes. We give a proof of this stronger statement. Recall (Tate's algorithm) that E has bad potentially multiplicative reduction at a prime $\mathfrak{p}$ if and only if $\mathrm{ord}_\mathfrak{p}(j(E)) < 0$ has negative valuation. Let t be a parameter on $Y_1(\ell)$. We conclude in the style of Euclid: for any finite set $\{(E_i', P_i')\}_i \subset Y_1(\ell)(K)$ corresponding to $t_i \in K$, we can find $\mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p}(j(E_i')) \geq 0$ and there exists $t^* \in K$ giving $(E^*, P^*) \in Y_1(\ell)(K)$ such that $\mathrm{ord}_\mathfrak{p}(j(E_{t^*})) < 0$. Indeed, this is determined by congruence conditions on the numerator and denominator, and the resulting set has positive density so cannot be contained in the thin set excluded by Hilbert irreducibility. 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 at $\mathfrak{p}$ whereas E^* has bad potentially multiplicative reduction. It follows that the set of products $E_1 \times E_2$ of this form fall into infinitely many distinct geometric isogeny classes: indeed, since none of E_1, E_2 and E_2' are geometrically isogenous, by the Poincaré Complete Reducibility Theorem, $E_1 \times E_2$ is not geometrically isogeneous to $E_1 \times E_2'$. $\qquad\square$

For convenience, we rewrite the elements in (2.3.10) as

$$(2.3.12) \qquad \begin{pmatrix} 1 + x_1\ell & b_1 + y_1\ell & 0 & 0 \\ w_1\ell & d + z_1\ell & 0 & 0 \\ 0 & 0 & 1 + x_2\ell & b_2 + y_2\ell \\ 0 & 0 & w_2\ell & d + z_2\ell \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

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

$$(2.3.13) \qquad\qquad\qquad\qquad \det A_1 = \det A_2.$$

Recall that $A = (E_1 \times E_2)/\langle (P, Q) \rangle$. Because A and $E_1 \times E_2$ are isogenous via $q \colon E_1 \times E_2 \to A$, 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 $E_1 \times E_2$:

$$(2.3.14) \qquad\qquad\qquad M_{q,\ell} = \begin{pmatrix} 1 & 0 & 1/\ell & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $\det M_{q,\ell}^{-1} = \ell$ and maps the lattice $\mathbb{Z}_\ell^4 + \mathbb{Z}_\ell \cdot (1/\ell, 1, 1/\ell, 1) \subset \mathbb{Q}_\ell^4$ into $\mathbb{Z}_\ell^4$. Conjugating the elements (2.3.12) above by this change of coordinates matrix (i.e. we compute $M_{q,\ell}^{-1} G_\ell M_{q,\ell}$)

gives

$$(2.3.15) \qquad \begin{pmatrix} 1 + x_1\ell & b_1 + y_1\ell & x_1 - x_2 & -b_2 - y_2\ell \\ w_1\ell & d + z_1\ell & w_1 & 0 \\ 0 & 0 & 1 + x_2\ell & b_2\ell + y_2\ell^2 \\ 0 & 0 & w_2 & d + z_2\ell \end{pmatrix},$$

with the same conditions on the variables. See also our companion paper [FHV25] for more on computing Galois actions on Tate modules within an isogeny class.

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

Proposition 2.3.16. *The image of $\bar{\rho}_{A,\ell} \colon \mathrm{Gal}_K \to \mathrm{GL}_4(\mathbb{F}_\ell)$ is*

$$(2.3.17) \qquad \left\{ \begin{pmatrix} 1 & b_1 & x_1 - x_2 & -b_2 \\ 0 & d & w_1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & w_2 & d \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : \begin{matrix} d \in \mathbb{F}_\ell^\times \\ b_i, w_i, x_i \in \mathbb{F}_\ell \end{matrix} \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell).$$

Proof. We need to check that the determinant condition (2.3.13) being satisfied does not constrain our choices of variables above: it requires that

$$d + (dx_1 + z_1 - b_1 w_1)\ell + (x_1 z_1 - w_1 y_1)\ell^2 = d + (dx_2 + z_2 - b_2 w_2)\ell + (x_2 z_2 - w_2 y_2)\ell^2.$$

Given $d \in \mathbb{F}_\ell^\times$, $b_i, w_i, x_i \in \mathbb{F}_\ell$, choose lifts of w_i, x_i to $\mathbb{Z}_\ell$ (which we continue to call w_i, x_i). One can check that taking $z_2 = y_1 = y_2 = 0$ and $z_1 = (1 + x_2\ell)^{-1}(dx_2 - dx_1 + b_1 w_1 - b_2 w_2)$ gives a solution to the determinant equation, and thus an element in the image of $\rho_{A,\ell}$ reducing to an element as in (2.3.17) with the given entries. $\square$

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 $A^\vee[\ell](K^{\mathrm{al}})$. To do so, we make use of the following, as indicated in the introduction.

Lemma 2.4.1. *Given the representation $\rho_{A,\ell} \colon \mathrm{Gal}_K \to \mathrm{Aut}(T_\ell A)$, 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, if $\bar{\rho}_{A,\ell}(\sigma) = M$ for M as in (2.3.12), then $\varepsilon_\ell(\sigma) = d$ [Sil09, section III.8]. Thus, when we take the inverse transpose of matrices as in Proposition 2.3.16 and scale by this factor, we get the following.

Proposition 2.4.2. *If* $\bar{\rho}_{A,\ell}(\sigma) = \begin{pmatrix} 1 & b_1 & x_1 - x_2 & -b_2 \\ 0 & d & w_1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & w_2 & d \end{pmatrix}$ *as in* (2.3.17), *then*

(2.4.3)
$$\bar{\rho}_{A^\vee,\ell}(\sigma) = \begin{pmatrix} d & 0 & 0 & 0 \\ -b_1 & 1 & 0 & 0 \\ z_1 - z_2 & -w_1 & d & -w_2 \\ b_2 & 0 & 0 & 1 \end{pmatrix}$$

where $z_1 - z_2 = b_1 w_1 - b_2 w_2 - dx_1 + dx_2 \in \mathbb{F}_\ell$.

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

$$b_1 w_1 - b_2 w_2 - dx_1 + dx_2 = z_1 - z_2$$

by the determinant condition (2.3.13). $\qquad\square$

2.5. Proof of the main result. We now prove Theorem 1.2.1.

Proof of Theorem 1.2.1. Let K be a number field with $K \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$ and A an abelian surface over K as in Construction 2.1.1, with the pair E_1, E_2 coming from the infinite set in Proposition 2.3.11.

Let $\sigma \in \mathrm{Gal}_K$. We apply Proposition 2.4.2. 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 $\sigma \in \mathrm{Gal}_K$; see the Magma [BCP97] code [FHV23]. Hence, these representations are not isomorphic and $A[2]$ is not isomorphic to $A^\vee[2]$ over K.

It remains to show that the same is true for $\ell \in \{3, 5, 7\}$. We claim that this can be seen directly from just the images of the representations $\bar{\rho}_{A,\ell}$ and $\bar{\rho}_{A^\vee,\ell}$. Indeed, $A[\ell](K) \neq \emptyset$, since the first basis element is fixed by Gal_K. 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 $\sigma \in \mathrm{Gal}_K$, so $A^\vee[\ell](K) = \emptyset$. More precisely, although each matrix $\bar{\rho}_{A^\vee,\ell}(\sigma)$ has fixed vectors, 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.) $\qquad\square$

2.6. Generalizing the construction. Construction 2.1.1 can be generalized 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 suppose 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. We then take

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

When $\ell = 2$ or when the Galois action on $C_1 \simeq C_2$ is trivial, we recover Construction 2.1.1.

For $\ell = 3, 5, 7$, there are again infinitely many elliptic curves E over K with a cyclic subgroup $C \leqslant E[\ell](K^{\mathrm{al}})$ stable under Gal_K—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 $a \pmod{\ell}$ in (2.3.6), 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 (2.3.9) and (2.3.10). Then the proof of Proposition 2.3.11 goes through the same, replacing $\mathsf{E}_{C,\ell}$ with a versal family 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. For $\ell = 3, 5, 7$, it will no longer be the case that $A[\ell](K) \neq \emptyset$; rather, both $A[\ell](K^{\mathrm{al}})$ and $A^\vee[\ell](K^{\mathrm{al}})$ have a unique Galois-stable line. The Galois actions on these lines can be shown to differ—more precisely, if χ is the character on the common Galois-stable line in $E_1[\ell]$ and $E_2[\ell]$, then the action on the line in $A[\ell]$ is χ whereas for $A^\vee[\ell]$ it is χ' where $\chi\chi' = \varepsilon_\ell$—and so $A[\ell]$ and $A^\vee[\ell]$ cannot be isomorphic group schemes over K.

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 over K, let $\pi_{A,\ell}\colon \mathrm{Gal}_K \to \mathrm{Sym}(A[\ell]) \simeq S_{\ell^4}$ 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 as in Construction 2.1.1, coming from a pair E_1, E_2 as in Proposition 2.3.11. Then for $\ell \in \{3, 5, 7\}$, the permutation representations $\pi_{A,\ell}$ and $\pi_{A^\vee,\ell}$ are not isomorphic. Moreover, the induced linear representations over any field F with $\mathrm{char}\, F = 0$ are not isomorphic.*

Proof. We can see this computationally in multiple ways; see the Magma code provided [FHV23]. For the permutation representations, we can check that the permutation characters are inequivalent. 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 for F a field with $\mathrm{char}\, F = 0$, the multiplicity of the trivial representation does not change under base change to F. Since the induced linear representations are not isomorphic, this also shows that the permutation representations cannot be isomorphic. $\qquad\square$

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 $\pi_{A,\ell}$ and then further to the induced linear representations—in each case, there are more possible elements to conjugate by.

For $\ell = 2$ above, we check in Magma that the permutation representations $\pi_{A,2} \not\cong \pi_{A^\vee,2}$ are not isomorphic, but the linear representations are isomorphic [FHV23] (so the first but not the second statement holds in Proposition 3.1.1 for $\ell = 2$).

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 via λ, the Tate module $T_\ell A$ is conjugate to $T_\ell A^\vee$ as Gal_K-lattices inside $V_\ell A := (T_\ell A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Therefore the reductions modulo ℓ have the same semisimplifications (the sum given by the factors in a Jordan–Hölder filtration).

We can also see this through point counts as follows. 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 $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}_K$. The traces determine the semisimplifications up to isomorphism, by the Brauer–Nesbitt theorem. $\square$

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 $\sigma \in \mathrm{Gal}(K^{\mathrm{al}} \,|\, K)$. We prove the containment ($\subseteq$) and suppose that $\overline{\rho}_{A,n}(\sigma) = 1$. Then $\overline{\rho}_{A^\vee,n}(\sigma) = \overline{\rho}_{A,n}(\sigma)^* \varepsilon_n(\sigma) = 1$ if and only if $\varepsilon_n(\sigma) = 1$, so we prove this. Since A has a primitive polarization λ over K, there exist $P, Q \in A[n](K^{\mathrm{al}})$ with Weil pairing $\langle P, Q\rangle_\lambda = \zeta_n$: indeed, if the polarization is of type $(d_1, \ldots, d_g)$ with corresponding Frobenius basis $P_1, \ldots, P_g, Q_1, \ldots, Q_g$ (i.e., $\langle P_i, Q_j\rangle_\lambda = d_i, 0$ as $i = j$ or not), then $\gcd(d_1, \ldots, d_g) = 1$ so there exist $a_1, \ldots, a_g \in \mathbb{Z}$ such that $d_1 a_1 + \cdots + d_g a_g = 1$ and thus $P := \sum_{i=1}^g a_i P_i$ and $Q := \sum_{i=1}^g Q_i$ have $\langle P, Q\rangle_\lambda = \zeta_n^{\sum_i a_i d_i} = \zeta_n$. Therefore

$$(3.2.3) \qquad \zeta_n = \langle P, Q\rangle_\lambda = \langle \sigma(P), \sigma(Q)\rangle_\lambda = \zeta_n^{\varepsilon_n(\sigma)}$$

the latter by the Galois equivariance of the pairing. We conclude indeed that $\varepsilon_n(\sigma) = 1$.

The containment ($\supseteq$) follows from interchanging A with $A^\vee$ and applying the canonical isomorphism $(A^\vee)^\vee \cong A$. $\square$

Remark 3.2.4. 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 3.2.5.) 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 isomorphic. In the following result, we enumerate such possible Galois images in the case of $\ell = 2$.

Proposition 3.2.5. *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 conjugate (in $\mathrm{GL}_4(\mathbb{F}_2)$) to its (twisted) contragredient, and a further 26 for which the groups are conjugate but the corresponding representations are not equivalent.*

For the additional 26 groups in part (b), there exists $g \in \mathrm{GL}_4(\mathbb{F}_2)$ such that $g^{-1}Hg = H^\vee$ but there is no $g \in \mathrm{GL}_4(\mathbb{F}_2)$ such that $g^{-1}hg = h^\vee$ for all $h \in H$.

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 3.2.5(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 generic component 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 families of abelian varieties of dimension g defined over an open $U \subseteq \mathbb{P}^n$ with a polarization of minimal degree $d > 1$. Even the existence of a *single* such abelian variety is constrained: for abelian varieties A with fixed dimension g over number fields of fixed degree d, the minimal degree of a polarization on A is conjecturally bounded by a constant $c(d, g)$, see Rémond [Rém18, Théorème 1.1(1)] who deduces this finiteness from Coleman's conjecture on endomorphism algebras using Zarhin's trick. In particular, if g and d are fixed, then we can only have $A[\ell] \not\simeq A^\vee[\ell]$ for $\ell \leq c(d, g)$.

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

[DF04]   David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd. ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. 2.2

[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, 3.1.2, 3.2

[FHV25]   Sarah Frei, Katrina Honigs, and John Voight, *A framework for Tate modules of abelian varieties under isogeny*, 2025, preprint, `arXiv:2503.12756`, to appear in *Essent. Number Theory*. 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

[FT93]   A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Stud. Adv. Math., vol. 27, Cambridge University Press, Cambridge, 1993. 2.2

[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

[KM85]   Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Ann. Math. Stud., vol. 108, Princeton University Press, Princeton, NJ, 1985. 2.3

[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

[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, 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 MS 136, Rice University, 6100 S. Main St, Houston, TX 77005, USA

Email address: sarah.frei@rice.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