NON-ISOGENOUS SUPERELLIPTIC JACOBIANS

YURI G. ZARHIN

Abstract. Let \( \ell \) be an odd prime. Let \( K \) be a field of characteristic zero with algebraic closure \( K_a \). Let \( n, m \geq 4 \) be integers that are not divisible by \( \ell \). Let \( f(x), h(x) \in K[x] \) be irreducible separable polynomials of degree \( n \) and \( m \) respectively. Suppose that the Galois group \( \text{Gal}(f) \) of \( f \) acts doubly transitively on the set \( \mathfrak{R}_f \) of roots of \( f \) and that \( \text{Gal}(h) \) acts doubly transitively on \( \mathfrak{R}_h \) as well. Let \( J(C_{f,\ell}) \) and \( J(C_{h,\ell}) \) be the Jacobians of the superelliptic curves \( C_{f,\ell} : y^\ell = f(x) \) and \( C_{h,\ell} : y^\ell = h(x) \) respectively. We prove that \( J(C_{f,\ell}) \) and \( J(C_{h,\ell}) \) are not isogenous over \( K_a \) if the splitting fields of \( f \) and \( h \) are linearly disjoint over \( K(\zeta_\ell) \).

1. Definitions, Notations, Statements

Let \( K \) be a field. Let us fix its algebraic closure \( K_a \) and denote by \( \text{Gal}(K) \) the absolute Galois group \( \text{Aut}(K_a/K) \) of \( K \). If \( L \supset K \) is an overfield of \( K \) and \( L_a \) contains \( K_a \) (i.e., \( K_a \) is the algebraic closure of \( K \) in \( L_a \)) then \( K_a \) is \( \text{Aut}(L_a/L) \)-stable and we write

\[
\text{res}(L, K) : \text{Gal}(L) = \text{Aut}(L_a/L) \to \text{Aut}(K_a/K) = \text{Gal}(K)
\]

for the corresponding restriction map. If \( X \) is an abelian variety over \( K_a \) then we write \( \text{End}(X) \) for the ring of all its \( K_a \)-endomorphisms; \( 1_X \) stands for the identity automorphism of \( X \). If \( Y \) is an abelian variety over \( K_a \) then we write \( \text{Hom}(X, Y) \) for the (free commutative) group of all \( K_a \)-homomorphisms from \( X \) to \( Y \). It is well-known that \( \text{Hom}(X, Y) = 0 \) if and only if \( \text{Hom}(Y, X) = 0 \). If \( X \) is defined over \( K \) then \( X(K_a) \) carries a natural structure of \( \text{Gal}(K) \)-module. One may also view \( X \) as an abelian variety over \( L \); the subgroup \( X(K_a) \subset X(L_a) \) is \( \text{Gal}(L) \)-stable and the corresponding homomorphism \( \text{Gal}(L) \to \text{Aut}(X(K_a)) \) is the composition of \( \text{res}(L, K) : \text{Gal}(L) \to \text{Gal}(K) \) and the structure homomorphism \( \text{Gal}(K) \to \text{Aut}(X(K_a)) \).

Let \( f(x) \in K[x] \) be a polynomial of degree \( n \geq 4 \) without multiple roots. We write \( \mathfrak{R}_f \subset K_a \) for the set of its roots, \( K(\mathfrak{R}_f) \subset K_a \) for the splitting field of \( f \) and \( \text{Gal}(f) = \text{Aut}(K(\mathfrak{R}_f)/K) = \text{Gal}(K(\mathfrak{R}_f)/K) \) for the Galois group of \( f \). Then \( \mathfrak{R}_f \) consists of \( n = \deg(f) \) elements. The group \( \text{Gal}(f) \) permutes elements of \( \mathfrak{R}_f \) and therefore can be identified with a certain subgroup of the group \( \text{Perm}(\mathfrak{R}_f) \) of all permutations of \( \mathfrak{R}_f \). Clearly, every ordering of \( \mathfrak{R}_f \) provides an isomorphism between \( \text{Perm}(\mathfrak{R}_f) \) and the full symmetric group \( S_n \) which makes \( \text{Gal}(f) \) a certain subgroup of \( S_n \). (This permutation subgroup is transitive if and only if \( f \) is irreducible over \( K_a \).)

Let \( \ell \) be an odd prime. We write \( \mathbb{Z}[\zeta_\ell] \) for the ring of all integers in the \( \ell \)th cyclotomic ring \( \mathbb{Q}(\zeta_\ell) \).

Let us assume that \( \text{char}(K) \neq \ell \) and consider the superelliptic curve

\[
C_{f,\ell} : y^\ell = f(x),
\]
defined over $K$. Its genus $g = g(C_{f,\ell})$ equals $(n - 1)(\ell - 1)/2$ if $\ell$ does not divide $n$ and $(n - 2)(\ell - 1)/2$ if $\ell \mid n$. Let $J(C_{f,\ell})$ be the Jacobian of $C_f$; it is a $g$-dimensional abelian variety over $K_a$ that is defined over $K$. Then $\text{End}(J(C_{f,\ell}))$ contains a certain subring isomorphic to $\mathbb{Z}[\zeta]/(\zeta^2)$ (see Sect. 3.2).

The main result of the present paper is the following statement.

**Theorem 1.1** (Main Theorem). Suppose that $K$ is a field of characteristic different from $\ell$ that contains a primitive $\ell$th root of unity. Let $f(x), h(x) \in K[x]$ be separable irreducible polynomials of degree $n \geq 4$ and $m \geq 4$ respectively. Suppose that the splitting fields of $f$ and $h$ are linearly disjoint over $K$.

Suppose that the following conditions hold:

(i) The group $\text{Gal}(f)$ acts doubly transitively on $\mathcal{R}_f$; if $\ell$ divides $n$ then this action is 3-transitive.

(ii) The group $\text{Gal}(h)$ acts doubly transitively on $\mathcal{R}_h$; if $\ell$ divides $n$ then this action is 3-transitive.

Then either

$$\text{Hom}(J(C_{f,\ell}), J(C_{h,\ell})) = 0, \quad \text{Hom}(J(C_{h,\ell}), J(C_{f,\ell})) = 0$$

or $p := \text{char}(K) > 0$ and there exists an abelian variety $Z$ defined over an algebraic closure $\overline{F}_p$ of $F_p$ such that both $J(C_{f,\ell})$ and $J(C_{h,\ell})$ are isogenous over $K_a$ to self-products of $Z$.

**Remark 1.2.** The case $\ell = 2$ (of hyperelliptic Jacobians) was treated in [26] [27]. See [11] for the list of known doubly transitive permutation groups.

The paper is organized as follows. In Sections 2 and 3 we study pairs of abelian varieties with homomorphism groups of big rank. We prove Theorem 1.1 in 41 Sections 5 and 6 contain the proof of some auxiliary results.

I am grateful to the referee, whose comments helped to improve the exposition.

2. Homomorphisms of abelian varieties: statements

First, we need to introduce some notions from the theory of abelian varieties. Let $K$ be a field and $d$ be a positive integer that is not divisible by $\text{char}(K)$. Let $X$ be an abelian variety of positive dimension defined over $K$. We write $X_d$ for the kernel of multiplication by $d$ in $X(K_a)$. The commutative group $X_d$ is a free $\mathbb{Z}/d\mathbb{Z}$-module of rank $2\dim(X)$ [11]. Clearly, $X_d$ is a Galois submodule in $X(K_a)$.

We write

$$\tilde{\rho}_{d,X} : \text{Gal}(K) \to \text{Aut}_{\mathbb{Z}/d\mathbb{Z}}(X_d) \cong \text{GL}(2\dim(X), \mathbb{Z}/d\mathbb{Z})$$

for the corresponding (continuous) homomorphism defining the Galois action on $X_d$. Let us put

$$\tilde{G}_{d,X} = \tilde{\rho}_{d,X}(\text{Gal}(K)) \subset \text{Aut}_{\mathbb{Z}/d\mathbb{Z}}(X_d).$$

Clearly, $\tilde{G}_{d,X}$ coincides with the Galois group of the field extension $K(X_d)/K$ where $K(X_d)$ is the field of definition of all points of order dividing $d$ on $X$. In particular, if $\ell \neq \text{char}(K)$ is a prime then $X_{\ell}$ is a $2\dim(X)$-dimensional vector space over the prime field $F_\ell = \mathbb{Z}/\ell\mathbb{Z}$ and the inclusion $\tilde{G}_{\ell,X} \subset \text{Aut}_{F_\ell}(X_{\ell})$ defines a faithful linear representation of the group $\tilde{G}_{\ell,X}$ in the vector space $X_{\ell}$. 
We write \( \text{End}_K(X) \subset \text{End}(X) \) for the (sub)ring of all \( K \)-endomorphisms of \( X \) and \( \text{End}_K^{0}(X) \subset \text{End}^{0}(X) \) for the corresponding \( \mathbb{Q} \)-(sub)algebra of all \( K \)-endomorphisms of \( X \). If \( Y \) is an abelian variety over \( K \) then we write \( \text{Hom}^{0}(X,Y) \) for the \( \mathbb{Q} \)-vector space \( \text{Hom}(X,Y) \otimes \mathbb{Q} \).

Let \( E \) be a number field and \( \mathcal{O} \subset E \) be the ring of all its algebraic integers. Let \((X, i)\) be a pair consisting of an abelian variety \( X \) over \( K_\alpha \) and an embedding

\[
i : E \hookrightarrow \text{End}^{0}(X)
\]

such that \( i(1) = 1_X \). The degree \([E : \mathbb{Q}]\) divides \( 2\dim(X) \) (see [27]).

If \( r \) is a positive integer then we write \( i^{(r)} \) for the composition

\[
E \hookrightarrow \text{End}^{0}(X) \subset \text{End}^{0}(X^r)
\]

of \( i \) and the diagonal inclusion \( \text{End}^{0}(X) \subset \text{End}^{0}(X^r) \).

If \((Y, j)\) is a pair consisting of an abelian variety \( Y \) over \( K_\alpha \) and an embedding \( j : E \hookrightarrow \text{End}^{0}(Y) \) with \( j(1) = 1_Y \) then we write

\[
\text{Hom}^{0}((X, i), (Y, j)) = \{ u \in \text{Hom}^{0}(X,Y) \mid ui(e) = j(e)u \quad \forall u \in E \}.
\]

Clearly, \( \text{Hom}^{0}((X, i), (Y, j)) \) carries a natural structure of finite-dimensional \( E \)-vector space. Notice that the \( \mathbb{Q} \)-vector space \( \text{Hom}^{0}(X,Y) \) carries a natural structure of \( E \otimes \mathbb{Q} \) \( E \)-module defined by the formula

\[
(e_1 \otimes e_2) \phi = j(e_1) \phi i(e_2) \quad \forall e_1, e_2 \in E, \phi \in \text{Hom}^{0}(X,Y).
\]

**Remark 2.1.** It is well-known that if the field extension \( E/\mathbb{Q} \) is normal then for each automorphism \( \sigma \in \text{Aut}(E) = \text{Gal}(E/\mathbb{Q}) \) there is a surjective \( E \)-algebra homomorphism

\[
\text{pr}_\sigma : E \otimes \mathbb{Q} E \twoheadrightarrow E, \quad e_1 \otimes e_2 \mapsto e_1 \sigma(e_2).
\]

(Here the structure of \( E \)-algebra on \( E \otimes \mathbb{Q} E \) is defined by

\[
e(e_1 \otimes e_2) = ee_1 \otimes e_2 \quad \forall e, e_1, e_2 \in E.
\]

The well-known \( E \)-linear independence of all \( \sigma : E \to E \) implies that the direct sum of all \( \text{pr}_\sigma \)'s is an isomorphism

\[
\bigoplus_{\sigma \in \text{Gal}(E/\mathbb{Q})} \text{pr}_\sigma : E \otimes \mathbb{Q} E \cong \bigoplus_{\sigma \in \text{Gal}(E/\mathbb{Q})} E.
\]

This allows us to view \( \text{pr}_\sigma \) as mutually orthogonal projection maps \( \text{pr}_\sigma : E \otimes \mathbb{Q} E \to E \otimes \mathbb{Q} E \), whose sum is the identity map. Also, the annihilator of \( \sigma(e) \otimes 1 - 1 \otimes e \) in \( E \otimes \mathbb{Q} E \) coincides with the image \( \text{pr}_\sigma : E \otimes \mathbb{Q} E \) of \( \text{pr}_\sigma \).

This implies easily that

\[
\text{Hom}^{0}((X,i), (Y,j)) = \text{pr}_\sigma(\text{Hom}^{0}(X,Y))
\]

and

\[
\text{Hom}^{0}(X, Y) = \bigoplus_{\sigma \in \text{Gal}(E/\mathbb{Q})} \text{Hom}^{0}((X,i), (Y,j)) \quad (1)
\]

where \( i : E \hookrightarrow \text{End}^{0}(X) \) is the composition of the automorphism \( \sigma : E \to E \) and \( i : E \hookrightarrow \text{End}^{0}(X) \).

Let us denote by \( \text{End}^{0}(X, i) \) the centralizer of \( i(E) \) in \( \text{End}^{0}(X) \). Clearly, \( \text{End}^{0}(X, i) = \text{Hom}^{0}((X,i), (X,i)) \) and \( i(E) \) lies in the center of the finite-dimensional \( \mathbb{Q} \)-algebra \( \text{End}^{0}(X, i) \). It follows that \( \text{End}^{0}(X, i) \) carries a natural structure of finite-dimensional \( E \)-algebra. One may easily check [27, Remark 4.1] that \( \text{End}^{0}(X, i) \) is a semisimple
Remark 2.5. For all positive integers \( r \)

Lemma 2.6. \( \dim_E(\text{End}^0((X, i))) \leq \frac{4 \cdot \dim(X)^2}{[E : \mathbb{Q}]^2} \).

Theorem 2.3. Suppose that

\[
\dim_E(\text{End}^0((X, i))) = \frac{4 \cdot \dim(X)^2}{[E : \mathbb{Q}]^2}.
\]

Then:

(i) \( \text{End}^0((X, i)) \) is a central simple \( E \)-algebra.

(ii) There exists an absolutely simple abelian variety \( B \) of CM-type over \( K_a \) such that \( X \) is isogenous to a self-product of \( B \).

(iii) If \( \text{char}(K) = 0 \) then \( [E : \mathbb{Q}] \) is even and there exist a \( [E : \mathbb{Q}]/2 \)-dimensional abelian variety \( Z \) over \( K_a \), an isogeny \( \psi : Z^r \to X \) and an embedding \( k : E \to \text{End}^0(Z) \) that send 1 to 1_{Z} and such that \( \psi \in \text{Hom}^0((Z^r, k^{(r)}), (X, i)) \).

Remark 2.4. Suppose that

\[
\dim_E(\text{End}^0((X, i))) = \frac{4 \cdot \dim(X)^2}{[E : \mathbb{Q}]^2}
\]

and \( \text{char}(K) > 0 \). In notations of Theorem 4.2, it follows from a theorem of Grothendieck [28 Th. 1.1] that \( B \) is isogenous to an abelian variety defined over a finite field. This implies that \( X \) is also isogenous to an abelian variety defined over a finite field.

If \( i(\mathcal{O}) \subset \text{End}(X) \) and \( j(\mathcal{O}) \subset \text{End}(Y) \) then we put

\[
\text{Hom}((X, i), (Y, j)) = \{ u \in \text{Hom}(X, Y) \mid ui(e) = j(e)u \quad \forall u \in E \}.
\]

Clearly,

\[
\text{Hom}^0((X, i), (Y, j)) = \text{Hom}((X, i), (Y, j)) \otimes \mathbb{Q},
\]

\[
\text{Hom}((X, i), (Y, j)) = \text{Hom}^0((X, i), (Y, j)) \cap \text{Hom}(X, Y),
\]

which is an \( \mathcal{O} \)-lattice in the \( E \)-vector space \( \text{Hom}^0((X, i), (Y, j)) \).

Remark 2.5. There are canonical isomorphisms of \( E \)-vector spaces

\[
\text{Hom}^0((X^r, i^{(r)}), (Y, j)) = (\text{Hom}^0((X, i), (Y, j)))^r = \text{Hom}^0((X^r, i), (Y, j^{(r)}))
\]

where \( (\text{Hom}^0((X, i), (Y, j)))^r \) is a direct sum of \( r \) copies of \( \text{Hom}^0((X, i), (Y, j)) \). It follows easily that there is a canonical isomorphism of \( E \)-vector spaces

\[
\text{Hom}^0((X^r, i^{(r)}), (Y, j^{(m)})) = (\text{Hom}^0((X, i), (Y, j)))^{rm}
\]

for all positive integers \( r \) and \( m \).

Lemma 2.6. (i) \( \dim_E(\text{Hom}^0((X, i), (Y, j))) \leq \frac{4 \cdot \dim(X) \dim(Y)}{[E : \mathbb{Q}]^2} \);

(ii) If \( \dim(X) = \dim(Y) \) and

\[
\dim_E(\text{Hom}^0((X, i), (Y, j))) = \frac{4 \cdot \dim(X) \dim(Y)}{[E : \mathbb{Q}]^2}
\]

then \( \text{Hom}^0((X, i), (Y, j)) \) contains an isogeny \( \phi : X \to Y \). In particular, \( \text{Hom}^0((X, i), (Y, j)) = \phi \cdot \text{End}^0(X, i) \), \( \text{End}^0(Y, j) = \phi \text{End}^0(X, i) \phi^{-1} \).
and
\[ \dim_E \text{End}^0(Y,j) = \dim_E \text{End}^0(X,i) = \dim_E \text{Hom}^0((X,i),(Y,j)) = \frac{4\dim(X)^2}{[E : \mathbb{Q}]^2} = \frac{4\dim(Y)^2}{[E : \mathbb{Q}]^2}. \]
of Lemma \[2.6\] Let us fix a prime \( \ell \neq \text{char}(K) \). Let us put
\[ E_\ell := E \otimes_\mathbb{Q} \mathbb{Q}_\ell. \]
Clearly, \( E_\ell \) is a direct sum of finitely many \( \ell \)-adic fields.
Let \( T_\ell(X) \) be the \( \mathbb{Z}_\ell \)-Tate module of \( X \) \[11\]. Recall that \( T_\ell(X) \) is a free \( \mathbb{Z}_\ell \)-module of rank \( 2\dim(X) \). Let us put
\[ V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell; \]
it is a \( 2\dim(X) \)-dimensional \( \mathbb{Q}_\ell \)-vector space. There are natural embeddings\n\[ \text{End}^0(X) \otimes_\mathbb{Q} \mathbb{Q}_\ell \hookrightarrow \text{End}_{\mathbb{Q}_\ell} V_\ell(X), \quad \text{End}^0(Y) \otimes_\mathbb{Q} \mathbb{Q}_\ell \hookrightarrow \text{End}_{\mathbb{Q}_\ell} V_\ell(Y), \]
\[ \text{Hom}^0(X,Y) \otimes_\mathbb{Q} \mathbb{Q}_\ell \hookrightarrow \text{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y)). \]
Now the injections \( i \) and \( j \) give rise to the injections
\[ E_\ell \hookrightarrow \text{End}^0(X) \otimes_\mathbb{Q} \mathbb{Q}_\ell \hookrightarrow \text{End}_{\mathbb{Q}_\ell} V_\ell(X), \quad E_\ell \hookrightarrow \text{End}^0(Y) \otimes_\mathbb{Q} \mathbb{Q}_\ell \hookrightarrow \text{End}_{\mathbb{Q}_\ell} V_\ell(Y). \]
These injections provide \( V_\ell(X) \) and \( V_\ell(Y) \) with the natural structure of free \( E_\ell \)-modules of rank \( \frac{2\dim(X)}{[E : \mathbb{Q}]} \) and \( \frac{2\dim(Y)}{[E : \mathbb{Q}]} \) respectively \[14\]. Clearly, the image of
\[ \text{Hom}^0((X,i),(Y,j)) \otimes_\mathbb{Q} \mathbb{Q}_\ell \subset \text{Hom}^0(X,Y) \otimes_\mathbb{Q} \mathbb{Q}_\ell \]
in \( \text{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y)) \) lies in \( \text{Hom}_{E_\ell}(V_\ell(X), V_\ell(Y)) \); in fact, it is a free \( E_\ell \)-submodule of \( \text{Hom}_{E_\ell}(V_\ell(X), V_\ell(Y)) \) of rank \( \dim_E(\text{Hom}^0((X,i),(Y,j))) \). The rank of the free \( E_\ell \)-module \( \text{Hom}_{E_\ell}(V_\ell(X), V_\ell(Y)) \) equals the product of the ranks of \( V_\ell(X) \) and \( V_\ell(Y) \), i.e. equals
\[ \frac{2\dim(X)}{[E : \mathbb{Q}]} \cdot \frac{2\dim(Y)}{[E : \mathbb{Q}]} \]
We conclude that
\[ \dim_E(\text{Hom}^0((X,i),(Y,j))) \leq \frac{2\dim(X)}{[E : \mathbb{Q}]} \cdot \frac{2\dim(Y)}{[E : \mathbb{Q}]} \]
Clearly, the equality holds if and only if
\[ \text{Hom}_{E_\ell}(V_\ell(X), V_\ell(Y)) = \text{Hom}^0((X,i),(Y,j)) \otimes_\mathbb{Q} \mathbb{Q}_\ell. \]
Suppose that the equality holds and assume, in addition, that \( \dim(X) = \dim(Y) \).
Then the ranks of \( V_\ell(X) \) and \( V_\ell(Y) \) do coincide and there exists an isomorphism
\( u : V_\ell(X) \cong V_\ell(Y) \) of \( E_\ell \)-modules. Since \( \mathbb{Q} \) is everywhere dense in \( \mathbb{Q}_\ell \) in the \( \ell \)-adic topology, there exists \( u' \in \text{Hom}^0((X,i),(Y,j)) \) that is also an isomorphism between \( V_\ell(X) \) and \( V_\ell(Y) \). Replacing \( u' \) by \( Nu' \) for suitable positive integer \( N \), we may assume that \( u' \in \text{Hom}(X,Y) \). Then \( u' \) must be an isogeny. \[ \square \]

**Theorem 2.7.** Suppose that \( E \) is a number field, \( X \) and \( Y \) are abelian varieties of positive dimension over an algebraically closed field \( K_a \),
\[ i : E \leftrightarrow \text{End}^0(X), \quad j : E \leftrightarrow \text{End}^0(Y) \]
are embeddings that send 1 to the identity automorphisms of \( X \) and \( Y \) respectively. Let us put
\[
r_X := \frac{2\dim(X)}{[E : \mathbb{Q}]}, \quad r_Y := \frac{2\dim(Y)}{[E : \mathbb{Q}]},
\]
Let us assume that
\[
\dim_E \text{Hom}^0((X, i), (Y, j)) = r_X \cdot r_Y.
\]
Then both \( \text{End}^0(X, i) \) and \( \text{End}^0(Y, j) \) are central simple \( E \)-algebras and
\[
\dim_E \text{End}^0(X, i) = r_X^2, \quad \dim_E \text{End}^0(Y, j) = r_Y^2.
\]
In addition, both \( X \) and \( Y \) are isogenous to self-products of a certain absolutely simple abelian variety \( B \) of CM-type.

of Theorem 2.7. Clearly,
\[
\dim(X^r_Y) = \frac{2\dim(X)\dim(Y)}{[E : \mathbb{Q}]} = \dim(Y^r_X).
\]
It follows from Remark 2.5 that
\[
\dim_E(\text{Hom}^0((X^r_Y, i^{(r_Y)}), (Y^r_X, j^{(r_X)}))) = \frac{4\dim(X^r_Y)\dim(Y^r_X)}{[E : \mathbb{Q}]}.
\]
By Lemma 2.6 there exists an isogeny \( \phi : X^r_Y \to Y^r_X \) that lies in \( \text{Hom}^0((X^r_Y, i^{(r_Y)}), (Y^r_X, j^{(r_X)})) \).
In addition, \( \text{End}^0(X, i) \) and \( \text{End}^0(Y, j) \) are central simple \( E \)-algebras and
\[
\dim_E \text{End}^0(X^r_Y, i^{(r_Y)}) = \left( \frac{2\dim(X^r_Y)}{[E : \mathbb{Q}]^2} \right) = (r_X r_Y)^2.
\]
Similarly,
\[
\dim_E \text{End}^0(Y^r_X, j^{(r_X)}) = (r_Y r_X)^2.
\]
This implies the first claim.

Applying Theorem 2.7 to both \((X, i)\) and \((Y, j)\), we conclude that there exist absolutely simple abelian varieties \( B \) and say, \( B' \) of CM-type such that \( X \) is isogenous to a self-product of \( B \) and \( Y \) is isogenous to a self-product of \( B' \). Since \( \text{Hom}^0((X, i), (Y, j)) \neq 0 \), we conclude that \( \text{Hom}(X, Y) \neq 0 \) and therefore \( \text{Hom}(B, B') \neq 0 \). This implies that \( B \) and \( B' \) are isogenous and therefore \( Y \) is isogenous to a self-product of \( B \).

Suppose that \( X \) is defined over \( K \) and \( i(\mathcal{O}) \subset \text{End}_K(X) \). Then we may view elements of \( \mathcal{O} \) as \( K \)-endomorphisms of \( X \).

Let \( \lambda \) be a maximal ideal in \( \mathcal{O} \). We write \( k(\lambda) \) for the corresponding (finite) residue field. Let us put
\[
X_\lambda = X_{\lambda,i} := \{ x \in X(K_\lambda) \mid i(e)x = 0 \quad \forall e \in \lambda \}.
\]
Clearly, if \( \text{char}(k(\lambda)) = \ell \) then \( \lambda \supset \ell \cdot \mathcal{O} \) and therefore \( X_\lambda \subset X_\ell \). Moreover, \( X_\lambda \) is a Galois submodule of \( X_\ell \) and \( X_\lambda \) carries a natural structure of \( \mathcal{O}/\lambda = k(\lambda) \)-vector space. It is known [14] that if \( \ell \neq \text{char}(K) \) then
\[
\dim_{k(\lambda)} X_\lambda = \frac{2\dim(X)}{[E : \mathbb{Q}]}.
\]
We write
\[ \tilde{\rho}_{\lambda,X} = \tilde{\rho}_{\lambda,X,K} : \text{Gal}(K) \to \text{Aut}_{k(\lambda)}(X_\lambda) \cong \text{GL}(d_{X,E}, k(\lambda)) \]
for the corresponding (continuous) homomorphism defining the Galois action on \( X_\lambda \). Let us put
\[ \tilde{G}_{\lambda,X} = \tilde{G}_{\lambda,i,X} := \tilde{\rho}_{\lambda,X}(\text{Gal}(K)) \subset \text{Aut}_{k(\lambda)}(X_\lambda). \]
Clearly, \( \tilde{G}_{\lambda,X} \) coincides with the Galois group of the field extension \( K(X_\lambda)/K \) where \( K(X_\lambda) = K(X_{\lambda,i}) \) is the field of definition of all points in \( X_\lambda \).

In order to describe \( \tilde{\rho}_{\lambda,X,K} \) explicitly, let us assume for the sake of simplicity that \( \lambda \) is the only maximal ideal of \( \mathcal{O} \) dividing \( \ell \), i.e., \( \ell \cdot \mathcal{O} = \lambda b \) where the positive integer \( b \) satisfies \( [E : \mathbb{Q}] = b \cdot \dim_{\mathbb{F}_\ell} k(\lambda) \). Then \( \mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_\lambda \) where \( \mathcal{O}_\lambda \) is the completion of \( \mathcal{O} \) with respect to \( \lambda \)-adic topology. Let us choose an element \( c \in \lambda \) that does not lie in \( \lambda^2 \). One may easily check [28, §3] that
\[ X_\lambda = \{ x \in X_\ell \mid cx = 0 \} \subset X_\ell. \]

Let \( T_\ell(X) \) be the \( \mathbb{Z}_\ell \)-Tate module of \( X \). Recall that \( T_\ell(X) \) is a free \( \mathbb{Z}_\ell \)-module of rank \( 2 \dim(X) \) provided with the continuous action
\[ \rho_{\ell,X} : \text{Gal}(K) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(X)) \]
and the natural embedding
\[ \text{End}_K(X) \otimes \mathbb{Z}_\ell \hookrightarrow \text{End}_{\mathbb{Z}_\ell}(T_\ell(X)), \]
whose image commutes with \( \rho_{\ell,X}(\text{Gal}(K)) \). In particular, \( T_\ell(X) \) carries the natural structure of \( \mathcal{O} \otimes \mathbb{Z}_\ell = \mathcal{O}_\lambda \)-module; it is known [14] that the \( \mathcal{O}_\lambda \)-module \( T_\ell(X) \) is free of rank \( d_{X,E} \). There is also the natural isomorphism of Galois modules
\[ X_\ell = T_\ell(X)/\ell T_\ell(X), \]
which is also an isomorphism of \( \text{End}_K(X) \supset \mathcal{O} \)-modules. One may easily check [28, §3] that the \( \mathcal{O}[\text{Gal}(K)] \)-module
\[ X_\lambda = T_\ell(X)/(\lambda \mathcal{O}_\lambda)T_\ell(X) = T_\ell(X) \otimes_{\mathcal{O}_\lambda} k(\lambda). \]

**Remark 2.8.** Let \( \sigma \) be an automorphism of \( E \). Clearly, \( \sigma(\mathcal{O}) = \mathcal{O} \) and \( \sigma(\lambda) = \lambda \) (since \( \lambda \) is the only maximal ideal dividing \( \ell \)). However, \( \sigma \) may induce a non-trivial automorphism of \( k(\lambda) \) (if \( k(\lambda) \neq \mathbb{F}_\ell \)). Let us consider the composition
\[ t := i \circ \sigma : E \hookrightarrow \text{End}^0_k(X). \]
Clearly, \( t(0) = i(0) \subset \text{End}_K(X) \). It is also clear that
\[ X_\lambda = X_{\lambda,i} = X_{\lambda,t}, \quad K(X_\lambda) = K(X_{\lambda,i}) = K(X_{\lambda,t}), \quad \tilde{G}_{\lambda,X} = \tilde{G}_{\lambda,i,X} = \tilde{G}_{\lambda,t,X}. \]
However, the structure of the \( k(\lambda) \)-vector space on \( X_{\lambda,t} \) is the twist via \( \sigma \) of the structure of the \( k(\lambda) \)-vector space on \( X_{\lambda,i} \). This means that multiplication by any \( a \in k(\lambda) \) in \( X_{\lambda,t} \) coincides with multiplication by \( \sigma(a) \) in \( X_{\lambda,i} \). However, this twist does not change the algebra of linear operators, i.e.
\[ \text{End}_{k(\lambda)}(X_{\lambda,i}) = \text{End}_{k(\lambda)}(X_{\lambda,t}), \quad \text{Aut}_{k(\lambda)}(X_{\lambda,i}) = \text{Aut}_{k(\lambda)}(X_{\lambda,t}). \]
This implies that the centralizers of \( \tilde{G}_{\lambda,X} \) in \( \text{End}_{k(\lambda)}(X_{\lambda,i}) \) and \( \text{End}_{k(\lambda)}(X_{\lambda}) \) do coincide. In particular, if the centralizer \( \text{End}_{k(\lambda)}(X_{\lambda,i}) \) is \( k(\lambda) \) (resp. a field) then the centralizer \( \text{End}_{k(\lambda)}(X_{\lambda,i}) \) is also \( k(\lambda) \) (resp. a field).
Remark 2.9. Suppose that $L$ is an overfield of $K$ and $K_\lambda$ is the algebraic closure of $K$ in $L_\alpha$. Then one may view $X$ as an abelian variety over $L$ and $i(\cal O) \subset \mathrm{End}_L(X)$. The base change (from $K$ to $L$) does not change the groups $X_\alpha$ and $X_\lambda$. One may easily check that $\tilde{\rho}_{\lambda,X,L} : \mathrm{Gal}(L) \to \mathrm{Aut}_{k(\lambda)}(X_\lambda)$ coincides with the composition of $\mathrm{res}(L,K) : \mathrm{Gal}(L) \to \mathrm{Gal}(K)$ and $\tilde{\rho}_{\lambda,X,K} : \mathrm{Gal}(K) \to \mathrm{Aut}_{k(\lambda)}(X_\lambda)$.

3. DISJOINT ABELIAN VARIETIES

Throughout this Section $E$ is a number field with the ring of integers $\cal O$ and $\lambda$ is a maximal ideal in $\cal O$, whose residue field $k(\lambda) = \cal O/\lambda$ has characteristic $\ell$. We assume that $\lambda$ is the only maximal ideal of $\cal O$ dividing $\ell$. Let $K$ a field of characteristic different from $\ell$. Let $X$ and $Y$ are abelian varieties of positive dimension over $K$ provided with embeddings

$$i : E \to \mathrm{End}^0_K(X) \subset \mathrm{End}^0(X), \hspace{1em} j : E \to \mathrm{End}^0_K(Y) \subset \mathrm{End}^0(Y)$$

such that

$$1_X = i(1) \in i(\cal O) \subset \mathrm{End}_K(X), \hspace{1em} 1_Y = j(1) \in j(\cal O) \subset \mathrm{End}_K(Y).$$

Let us consider the $k(\lambda)$-vector space

$$S(X,Y)_\lambda := \mathrm{Hom}_{k(\lambda)}(X_\lambda,Y_\lambda)$$

provided with the natural structure of $\mathrm{Gal}(K)$-module. Let

$$A(X,Y,\lambda,K) := \mathrm{End}_{\mathrm{Gal}(K)}(S(X,Y)_\lambda)$$

be the centralizer of $\mathrm{Gal}(K)$ in $\mathrm{End}_{k(\lambda)}(S(X,Y)_\lambda)$. Clearly, $A(X,Y,\lambda,K)$ is a finite-dimensional $k(\lambda)$-algebra containing the scalars $k(\lambda)$.

Remark 3.1. Suppose that $L$ is an overfield of $K$ and $K_\alpha$ is the algebraic closure of $K$ in $L_\alpha$. Let us consider $X$ and $Y$ as abelian varieties over $L$. It follows from Remark 2.9 that $\mathrm{Gal}(L) \to \mathrm{Aut}_{k(\lambda)}(S(X,Y)_\lambda)$ coincides with the composition of $\mathrm{res}(L,K) : \mathrm{Gal}(L) \to \mathrm{Gal}(K)$ and $\mathrm{Gal}(K) \to \mathrm{Aut}_{k(\lambda)}(S(X,Y)_\lambda)$. In particular, the image of $\mathrm{Gal}(L) \to \mathrm{Aut}_{k(\lambda)}(S(X,Y)_\lambda)$ lies in the image of $\mathrm{Gal}(K) \to \mathrm{Aut}_{k(\lambda)}(S(X,Y)_\lambda)$. It follows that

$$A(X,Y,\lambda,K) \subset A(X,Y,\lambda,L) \subset \mathrm{End}_{k(\lambda)}(S(X,Y)_\lambda).$$

Clearly, if $A(X,Y,\lambda,L)$ is a field then its every $k(\lambda)$-subalgebra is also a field, because $A(X,Y,\lambda,L)$ is finite-dimensional; in particular, $A(X,Y,\lambda,K)$ is also a field.

Definition 3.2. $(X,i)$ and $(Y,j)$ are disjoint at $\lambda$ over $K$ if $A(X,Y,\lambda,K)$ is a field.

Remark 3.3. It follows from Remark 3.1 that if $(X,i)$ and $(Y,j)$ are disjoint at $\lambda$ over $L \supset K$ then they are also disjoint over $K$.

Theorem 3.4. Suppose that the following conditions hold:

(i) The field extensions $K(X_\lambda)$ and $K(Y_\lambda)$ are linearly disjoint over $K$.

(ii) Consider the centralizer $k_1 := \mathrm{End}_{G_{\lambda,X}}(X_\lambda)$ of $G_{\lambda,X}$ in $\mathrm{End}_{k(\lambda)}(X_\lambda)$ and the centralizer $k_2 := \mathrm{End}_{G_{\lambda,Y}}(Y_\lambda)$ of $G_{\lambda,Y}$ in $\mathrm{End}_{k(\lambda)}(Y_\lambda)$. Then the $k(\lambda)$-algebras $k_1$ and $k_2$ are fields that are linearly disjoint over $k(\lambda)$.

Then $(X,i)$ and $(Y,j)$ are disjoint at $\lambda$ over $K$.

Theorem 3.5. If $(X,i)$ and $(Y,j)$ are disjoint at $\lambda$ over $K$ then one of the following two conditions holds:
We will prove Theorems 3.4 and 3.5 in §6. We will deduce Theorem 1.1 from the following statement.

**Corollary 3.6.** We keep all notations and assumptions of Theorem 3.4. Assume in addition that \( E \) is normal over \( \mathbb{Q} \). Then one of the following two conditions holds:

(i) \( \text{Hom}(X,Y) = 0, \text{Hom}(Y,X) = 0 \).

(ii) Both \( X \) and \( Y \) are isogenous over \( K_n \) to self-products of a certain absolutely simple abelian variety \( B \) of CM-type; in addition, \( \text{End}^0(X,i) \) is a \( r_X^2 \)-dimensional central simple \( E \)-algebra and \( \text{End}^0(Y,i) \) is a \( r_Y^2 \)-dimensional central simple \( E \)-algebra.

of Corollary 3.6 Applying Theorems 3.4 and 3.5 to \( (X,i),(Y,j) \) for all \( \sigma \in \text{Gal}(E/\mathbb{Q}) \), we conclude that either the assertion (ii) holds (and we are done) or all \( \text{Hom}^0((X,i),(Y,j)) = 0 \).

In the latter case, it follows from Remark 2.1 that \( \text{Hom}^0(X,Y) = 0 \) and therefore \( \text{Hom}(X,Y) = 0 \), which, in turn, implies that \( \text{Hom}(Y,X) = 0 \). □

### 4. Proof of Main Theorem

Throughout this section \( \ell \) is an odd prime, \( K \) a field of characteristic different from \( \ell \) and \( K_n \) its algebraic closure,

\[
E := \mathbb{Q}(\zeta_{\ell}) \supset \mathcal{O} := \mathbb{Z}[\zeta_{\ell}] \supset \lambda := (1 - \zeta_{\ell}) \cdot \mathbb{Z}[\zeta_{\ell}], \quad k(\lambda) = \mathbb{F}_\ell.
\]

Clearly, \( [E : \mathbb{Q}] = \ell - 1 \).

Let \( f(x) \in K[x] \) be a separable polynomial of degree \( n \geq 4 \).

Let \( \mathcal{R} = \mathcal{R}_f = \{a_1, \ldots, a_n\} \subset K_n \) be the set of all roots of \( f \). We may view the full symmetric group \( S_n \) as the group of all permutations of \( \mathcal{R} \). The Galois group \( G = \text{Gal}(f) \) of \( f \) permutes the roots and therefore becomes a subgroup of \( S_n \). The action of \( G \) on \( \mathcal{R} \) defines the standard permutational representation in the \( n \)-dimensional \( \mathbb{F}_\ell \)-vector space \( \mathbb{F}_p^\mathcal{R} \) of all functions \( \psi : \mathcal{R} \to \mathbb{F}_\ell \). This representation is not irreducible. Indeed, the "line" of constant functions \( \mathbb{F}_\ell \cdot 1 \) and the hyperplane \( (\mathbb{F}_p^\mathcal{R})^0 := \{\psi \mid \sum_{i=1}^n \psi(a_i) = 0\} \) are \( G \)-invariant subspaces in \( \mathbb{F}_p^\mathcal{R} \).

Then we define the *heart* \( (\mathbb{F}_\ell^\mathcal{R})^0 \) of the permutational action of \( G = \text{Gal}(f) \) on \( \mathcal{R} = \mathcal{R}_f \) over \( \mathbb{F}_\ell \) as follows \( \{100, 223\} \). If \( n \) is not divisible by \( \ell \) then we put

\[
(\mathbb{F}_\ell^\mathcal{R})^0 = (\mathbb{F}_\ell^\mathcal{R})^0 := (\mathbb{F}_\ell^\mathcal{R})^0.
\]

If \( n \) is divisible by \( \ell \) then \( (\mathbb{F}_\ell^\mathcal{R})^0 \) contains \( \mathbb{F}_\ell \cdot 1 \) and we obtain the natural representation of \( G = \text{Gal}(f) \) in the \( (n-2) \)-dimensional \( \mathbb{F}_\ell \)-vector quotient-space \( (\mathbb{F}_\ell^\mathcal{R})^0/(\mathbb{F}_\ell \cdot 1) \). In this case we put

\[
(\mathbb{F}_\ell^\mathcal{R})^0 = (\mathbb{F}_\ell^\mathcal{R})^0 := (\mathbb{F}_\ell^\mathcal{R})^0/(\mathbb{F}_p \cdot 1).
\]

In both cases it is known that the \( \text{Gal}(f) \)-module \( (\mathbb{F}_\ell^\mathcal{R})^0 \) is faithful (recall that \( n \geq 4 \) and \( \ell > 2 \)).
Remark 4.1. It is known \[\text{Sat} 4a\] (see also \[23\] Lemma 2.4) that if either \(n = \deg(f)\) is not divisible by \(\ell\) and \(\text{Gal}(f)\) is doubly transitive or \(n\) is divisible by \(\ell\) and \(\text{Gal}(f)\) is 3-transitive then the centralizer \(\text{End}_{\text{Gal}(f)}((\mathbb{F}_{\ell^m})^{00}) = \mathbb{F}_\ell\). (Conversely, one may easily check \[\text{Sat} 4a\] that if \(n\) is not divisible by \(\ell\) and \(H \subset \text{Perm}(\mathfrak{R})\) is a permutation group with \(\text{End}_{\mathfrak{H}}((\mathbb{F}_{\ell^m})^{00}) = \mathbb{F}_\ell\) then \(H\) is doubly transitive.)

Remark 4.2. Let us assume that \(K\) contains a primitive \(\ell\)-th root of unity \(\zeta\). Then the map

\[(x, y) \mapsto (x, \zeta y)\]

gives rise to a birational periodic automorphism \(\delta_\ell\) of \(C_{f, \ell}\) with exact period \(\ell\). By functoriality, \(\delta_\ell\) induces an automorphism of \(J(C_{f, \ell})\) which we still denote by \(\delta_\ell\).

It is known \[13, 15\] (see also \[23\]) that \(\delta_\ell\) satisfies the \(\ell\)-th cyclotomic equation in \(\text{End}_K(J(C_{f, \ell}))\). This gives rise to the embeddings

\[i_f : \mathbb{O} = \mathbb{Z}[\zeta_\ell] \rightarrow \text{End}_K(J(C_{f, \ell})), \ E = \mathbb{Q}[\zeta_\ell] \rightarrow \text{End}_K(J(C_{f, \ell}))\]

with \(i_f(1) = 1_{J(C_{f, \ell})}\) and \(i_f(\zeta_\ell) = \delta_\ell\).

Notice that \(\lambda = (1 - \zeta_\ell) \cdot \mathbb{Z}[\zeta_\ell]\) is the only maximal ideal dividing \(\ell\) in \(\mathbb{Z}[\zeta_\ell]\) and the corresponding residue field \(k(\lambda) = \mathbb{F}_\ell\). The finite Galois module \(J(C_{f, \ell})_\lambda\) admits the following description. The canonical surjection \(\text{Gal}(K) \rightarrow \text{Gal}(f)\) defines on the \(\mathbb{F}_\ell(\text{Gal}(K))-\)module \((\mathbb{F}_{\ell^m})^{00}\) the natural structure of \(\text{Gal}(K)\)-module. Then the \(\mathbb{F}_\ell(\text{Gal}(K))-\)modules \((\mathbb{F}_{\ell^m})^{00}\) and \(J(C_{f, \ell})_\lambda\) are canonically isomorphic \[13, 15\]. In particular, this implies that

\[K(J(C_{f, \ell})_\lambda) = K(\mathfrak{R}_f),\]

(recall that the the \(\text{Gal}(f)\)-module \((\mathbb{F}_{\ell^m})^{00}\) is faithful).

Theorem \[14.1\] now clearly is an immediate corollary of Remark \[14.1\] and the following result.

Theorem 4.3. Suppose that \(K\) is a field of characteristic different from \(\ell\) that contains a primitive \(\ell\)-th root of unity. Let \(f(x), h(x) \in K[x]\) be separable polynomials of degree \(n \geq 4\) and \(m \geq 4\) respectively. Suppose that the splitting fields of \(f\) and \(h\) are linearly disjoint over \(K\). Suppose that

\[\text{End}_{\text{Gal}(f)}((\mathbb{F}_{\ell^m})^{00}) = \mathbb{F}_\ell, \ \text{End}_{\text{Gal}(h)}((\mathbb{F}_{\ell^m})^{00}) = \mathbb{F}_\ell.\]

Then one the two following conditions hold:

(i) \(\text{Hom}(J(C_{f, \ell}), J(C_{h, \ell})) = 0\) and \(\text{Hom}(J(C_{h, \ell}), J(C_{f, \ell})) = 0\).

(ii) \(p := \text{char}(K) > 0\) and there exists an absolutely simple abelian variety \(Z\) defined over an algebraic closure \(\mathbb{F}_p\) of \(\mathbb{F}_p\) such that both \(J(C_{f, \ell})\) and \(J(C_{h, \ell})\) are abelian varieties of CM-type isogenous over \(K_a\) to self-products of \(Z\). In addition, the centralizer of \(\mathbb{Q}[\delta_\ell] \cong \mathbb{Q}(\zeta_\ell)\) in \(\text{End}^0(J(C_{f, \ell}))\) is a central simple \(\mathbb{Q}(\zeta_\ell)\)-algebra of dimension \(\left(\frac{2\dim(J(C_{f, \ell})))}{\ell-1}\right)^2\) and the centralizer of \(\mathbb{Q}[\delta_\ell] \cong \mathbb{Q}(\zeta_\ell)\) in \(\text{End}^0(J(C_{h, \ell}))\) is a central simple \(\mathbb{Q}(\zeta_\ell)\)-algebra of dimension \(\left(\frac{2\dim(J(C_{h, \ell})))}{\ell-1}\right)^2\).

of Theorem \[4.3\] By the assumption and Remark \[4.2\] \(K(J(C_{f, \ell})_\lambda)\) and \(K(J(C_{h, \ell})_\lambda)\) are linearly disjoint over \(K\).
Applying Corollary 5.6 (with $k_1 = F_\ell = k_2$, $X = J(C_{f,\ell}), Y = J(C_{h,\ell})$), we conclude that either
\[ \text{Hom}(J(C_{f,\ell}), J(C_{h,\ell})) = 0, \quad \text{Hom}(J(C_{h,\ell}), J(C_{f,\ell})) = 0 \]
(i.e. the case (i) holds) or both $J(C_{f,\ell})$ and $J(C_{h,\ell})$ are isogenous over $K_a$ to self-products of a certain absolutely simple abelian variety $B$ of CM-type; in addition, the centralizer of $Q(\zeta_\ell)$ in $\text{End}^0(J(C_{f,\ell}))$ is a $\left( \frac{2\dim(J(C_{f,\ell})))}{\ell-1} \right)$-dimensional central simple $Q(\zeta_\ell)$-algebra. By [23, Theorem 3.6], the last property cannot take place in characteristic zero and therefore $p := \text{char}(K_a) = \text{char}(K) > 0$. In order to check that the case (ii) holds, one has only to recall that in characteristic $p$ every absolutely simple abelian variety of CM-type is isogenous to an abelian variety over $F_p$ (a theorem of Grothendieck [12]). By the same token, we get the desired results for $J(C_{h,\ell})$. □

Remark 4.4. Theorem 4.3 suggests that it may be interesting to classify subgroups $G = \text{Gal}(f) \subset \text{Perm}(R)$ such that $n = \#(R)$ is divisible by $\ell$ and $\text{End}_G((F_\ell)_{00}) = F_\ell$ (or a field). According to [8, Satz 11], if $G$ is transitive (i.e. $f(x)$ is irreducible) then such $G$ must be doubly transitive (if $n \geq 4$ and $\ell$ is odd). The (almost) complete classification of known doubly transitive $G$ with (absolutely) irreducible $(F_\ell)_{00}$ is given in [10] (see also [11]). Of course, in the irreducible case the centralizer is a field (and even $F_\ell$ in the absolutely irreducible case).

Theorem 4.5. Suppose that $K$ is a field of prime characteristic different from $\ell$ that contains a primitive $\ell$th root of unity. Let $f(x), h(x) \in K[x]$ be separable polynomials of degree $n \geq 9$ and $m \geq 4$ respectively. Suppose that the splitting fields of $f$ and $h$ are linearly disjoint over $K$. Suppose that $\ell$ divides $n$ and $\text{Gal}(f)$ coincides either with full symmetric group $S_n$ or with the alternating group $A_n$. Suppose that
\[ \text{End}_{\text{Gal}(h)}((F_\ell^0)_{00}) = F_\ell \]
(e.g., $\ell$ does not divide $m$ and $\text{Gal}(h)$ is doubly transitive.) Then
\[ \text{Hom}(J(C_{f,\ell}), J(C_{h,\ell})) = 0, \quad \text{Hom}(J(C_{h,\ell}), J(C_{f,\ell})) = 0. \]

Proof. Clearly, $\text{Gal}(f)$ is $3$-transitive and, thanks to Remark 4.1
\[ \text{End}_{\text{Gal}(f)}((F_\ell^0)_{00}) = F_\ell. \]
Therefore we may apply Theorem 4.3. Assume that the assertion (ii) holds true.
In particular, the centralizer of $Q[\delta_\ell] \cong Q(\zeta_\ell)$ in $\text{End}^0(J(C_{f,\ell}))$ is a central simple $\left( \frac{2\dim(J(C_{f,\ell})))}{\ell-1} \right)$-dimensional $Q(\zeta_\ell)$-algebra. Recall that $r := \frac{2\dim(J(C_{f,\ell})))}{\ell} = n - 1$ or $n - 2$; in both cases we have $r > 1$ and therefore the $r^2$-dimensional centralizer of $Q[\delta_\ell]$ contains an overfield $E' \supset Q[\delta_\ell]$ that does not coincide with $Q[\delta_\ell]$. However, it follows from Theorem 0.1 of [23] that $Q[\delta_\ell]$ is a maximal commutative $Q$-subalgebra in $\text{End}^0(J(C_{f,\ell}))$. This gives us a desired contradiction. □

5. Representation theory

This Section contains auxiliary results that will be used in Section 6.

Lemma 5.1. Let $F$ be a field. Let $H_1$ and $H_2$ be groups. Let $\tau_i : H_i \rightarrow \text{Aut}_F(W_i)$ ($i = 1, 2$) be linear finite-dimensional representation of $H_i$ over $F$ and $F_i := \text{End}_{H_i}(W_i)$. Let $W_1^* = \text{Hom}_F(W_1, F)$ be the dual of $W_1$ and $\tau_i^* : H_i \rightarrow \text{Aut}_F(W_i^*)$
the dual of \( \tau_1 \). Let us assume that the \( F \)-algebras \( F_1 \) and \( F_2 \) are fields that are linearly disjoint over \( F \).

Let us consider the natural linear representation

\[
\tau^*_1 \otimes \tau^*_2 : H_1 \times H_2 \to \text{Aut}_F(\text{Hom}_F(W_1, W_2))
\]

of the group \( H := H_1 \times H_2 \) in the \( F \)-vector space \( S := \text{Hom}_F(W_1, W_2) \). Then \( \text{End}_H(S) \) is a field.

**Proof.** One may easily check that the centralizer of \( H_1 \) in \( \text{End}_F(W^*_1) \) still coincides with \( F_1 \). Let \( A_1 \) be the \( F \)-subalgebra of \( \text{End}_F(W^*_1) \) generated by \( \tau_1^*(H_1) \); clearly, the centralizer of \( A_1 \) in \( \text{End}_F(W^*_1) \) also coincides with \( F_1 \). Similarly, if \( A_2 \) is the \( F \)-subalgebra of \( \text{End}_F(W_2) \) generated by \( \tau_2(H_2) \) then the centralizer of \( A_2 \) in \( \text{End}_F(W_2) \) coincides with \( F_2 \). Clearly, the \( F \)-subalgebra of \( \text{End}_F(W^*_1 \otimes_F W_2) \) generated by \( \tau^*_1 \otimes \tau_2(H_1 \times H_2) \) coincides with

\[
A_1 \otimes_F A_2 \subset \text{End}_F(W^*_1) \otimes_F \text{End}_F(W_2) = \text{End}_F(W^*_1 \otimes_F W_2).
\]

It follows from Lemma (10.37) on p. 252 of \( \mathbb{G} \) that the centralizer of \( A_1 \otimes_F A_2 \) in \( \text{End}_F(W^*_1 \otimes_F W_2) \) coincides with \( F_1 \otimes_F F_2 \) and therefore is a field, thanks to the linear disjointness of \( F_1 \) and \( F_2 \). This implies that the centralizer of \( H_1 \times H_2 \) in \( \text{End}_F(W^*_1 \otimes_F W_2) \) is the field \( F_1 \otimes_F F_2 \). Since the \( H \)-modules \( W^*_1 \otimes F W_2 \) and \( \text{Hom}_F(W_1, W_2) \) are canonically isomorphic, the centralizer of \( H \) in \( \text{End}_F(\text{Hom}_F(W_1, W_2)) \) is also a field. \( \square \)

**Lemma 5.2.** Let \( L \) be a complete discrete valuation field with discrete valuation ring \( O_L \) its maximal ideal \( m = O_L/\mathfrak{m} \). Let \( V \) be a finite-dimensional vector space over \( L \), \( \tau : G \to \text{Aut}_L(V) \) a completely reducible linear representation of a group \( G \) in \( V \). Let \( T \) be a \( G \)-stable \( O_L \)-lattice in \( V \). Consider the finite-dimensional \( k \)-vector space \( \bar{V} = T \otimes_{O_L} k \) provided with a natural linear representation \( \bar{\tau} : G \to \text{Aut}_k(\bar{V}) \) that is the reduction of \( \tau \) modulo \( \mathfrak{m} \). If the centralizer of \( G \) in \( \text{End}_k(\bar{V}) \) is a field then \( \tau \) is irreducible.

**Proof.** Suppose that \( \tau \) is not irreducible. Since it is completely reducible, there exist non-zero \( u_1, u_2 \in \text{End}_O(V) \) with \( u_1 u_2 = 0 \). Multiplying (if necessary) both \( u_1 \) and \( u_2 \) by suitable powers of an uniformizer, we may assume that \( u_1(T) \subset T, u_2(T) \subset T \) but neither \( u_1 \) nor \( u_2 \) lies in \( m \cdot \text{End}_{O_L}(T) \). It follows that the images \( \bar{u}_1, \bar{u}_2 \) of \( u_1 \) and \( u_2 \) with respect to the reduction map \( \text{End}_{O_L}(T) \to \text{End}_k(\bar{V}) \) satisfy

\[
\bar{u}_1 \neq 0, \bar{u}_2 \neq 0, \bar{u}_1 \bar{u}_2 = 0.
\]

Since both \( \bar{u}_1, \bar{u}_2 \) obviously lie in the centralizer of \( G \) in \( \text{End}_k(\bar{V}) \), we get a contradiction. \( \square \)

**Lemma 5.3.** Let \( V \) be a finite-dimensional vector space over a field \( Q \) of characteristic zero, \( G \) a group, \( \tau : G \to \text{Aut}_Q(V) \) a completely reducible \( Q \)-linear representation in \( V \). Let \( L \) be an overfield of \( Q \) and \( i : L \hookrightarrow \text{End}_Q(V) \) is an embedding of \( Q \)-algebras that sends 1 to the identity automorphism of \( V \). Suppose that the image \( i(L) \) commutes with \( G \). Then the natural \( L \)-linear representation of \( G \) in \( V \) is also completely reducible.

**Proof.** Let \( A \subset \text{End}_Q(V) \) be the image of the natural \( Q \)-algebra homomorphism \( Q[G] \to \text{End}_Q(V) \). The complete reducibility of \( \tau \) means that \( A \) is a (finite-dimensional) semisimple \( Q \)-algebra. Therefore \( A_L := A \otimes_Q L \) is a semisimple
L-algebra. Clearly, $A \subset \text{End}_L(V)$. This implies that the image of the natural L-algebra homomorphism

$$L[G] \to \text{End}_L(V) \subset \text{End}_Q(V)$$

is isomorphic to a quotient of $A_L$ and therefore is also a semisimple L-algebra. But this means that the natural L-linear representation of $G$ in $V$ is also completely reducible. 

\[ \square \]

6. HOMOMORPHISMS OF ABELIAN VARIETIES: PROOFS

of Theorem 6.4 We need to prove that the centralizer $A(X,Y,\lambda,K) = \text{End}_{\text{Gal}(K)}(S(X,Y)_\lambda) = \text{End}_{\text{Gal}(K)}(\text{Hom}_{k(\lambda)}(X\lambda,Y_\lambda))$ of the natural representation

$$\text{Gal}(K) \to \text{Aut}_{k(\lambda)}(\text{Hom}_{k(\lambda)}(X\lambda,Y_\lambda))$$

is a field. Denote this representation by $\tau$ and let us put

$$F = k(\lambda), H_1 = \tilde{G}_{\lambda,X}, W_1 = X\lambda, H_2 = \tilde{G}_{\lambda,Y}, W_2 = Y_\lambda.$$

Denote by

$$\tau_1 : H_1 = \tilde{G}_{\lambda,X} \subset \text{Aut}_{k(\lambda)}(X\lambda) = \text{Aut}_{k(\lambda)}(W_1)$$

and

$$\tau_2 : H_2 = \tilde{G}_{\lambda,Y} \subset \text{Aut}_{k(\lambda)}(Y_\lambda) = \text{Aut}_{k(\lambda)}(W_2)$$

the corresponding inclusion maps.

It follows from Lemma 5.3 that the centralizer of the linear representation

$$\tau_1^* \otimes \tau_2 : \text{Gal}(K(X\lambda)/K) \times \text{Gal}(K(Y_\lambda)/K) \to \text{Aut}_{k(\lambda)}(\text{Hom}_{k(\lambda)}(X\lambda,Y_\lambda))$$

is a field.

One may easily check that $\tau$, which defines the structure of $\text{Gal}(K)$-module on $\text{Hom}_{k(\lambda)}(X\lambda,Y_\lambda)$, coincides with the composition of the natural surjection $\text{Gal}(K) \twoheadrightarrow \text{Gal}(K(X\lambda,Y_\lambda)/K)$, the natural embedding

$$\text{Gal}(K(X\lambda,Y_\lambda)/K) \hookrightarrow \text{Gal}(K(X\lambda)/K) \times \text{Gal}(K(Y_\lambda)/K)$$

and

$$\tau_1^* \otimes \tau_2 : \text{Gal}(K(X\lambda)/K) \times \text{Gal}(K(Y_\lambda)/K) \to \text{Aut}_{k(\lambda)}(\text{Hom}_{k(\lambda)}(X\lambda,Y_\lambda)).$$

Here $K(X\lambda,Y_\lambda)$ is the compositum of the fields $K(X\lambda)$ and $K(Y_\lambda)$. The linear disjointness of $K(X\lambda)$ and $K(Y_\lambda)$ means that

$$\text{Gal}(K(X\lambda,Y_\lambda)/K) = \text{Gal}(K(X\lambda)/K) \times \text{Gal}(K(Y_\lambda)/K).$$

This implies that $\tau$ is the composition of the surjection

$$\text{Gal}(K) \to \text{Gal}(K(X\lambda)/K) \times \text{Gal}(K(Y_\lambda)/K)$$

and $\tau_1^* \otimes \tau_2$. Since the centralizer of the representation

$$\tau_1^* \otimes \tau_2 : \text{Gal}(K(Y_\lambda)/K) \times \text{Gal}(K(X\lambda)/K) \to \text{Aut}_{k(\lambda)}(\text{Hom}_{k(\lambda)}(X\lambda,Y_\lambda))$$

is a field, the centralizer of the representation

$$\tau : \text{Gal}(K) \to \text{Aut}_{k(\lambda)}(\text{Hom}_{k(\lambda)}(X\lambda,Y_\lambda))$$

is the same field. 

\[ \square \]
allow us to consider $\text{Hom}_{\mathbb{Q}}(X)$ and $\text{Hom}_{\mathbb{Q}}(Y)$ of abelian varieties $X$ and $Y$. Recall that $T_\ell(X)$ and $T_\ell(Y)$ are free $O_\lambda$-modules provided with the continuous actions of $\text{Gal}(K)$ and one may view $\tilde{\rho}_{\ell,X} : \text{Gal}(K) \to \text{Aut}_{O_\lambda}(X_\lambda)$ as the reduction of $\rho_{\ell,X} : \text{Gal}(K) \to \text{Aut}_{O_\lambda}(T_\ell(X))$ modulo $\lambda$ and $\tilde{\rho}_{\lambda,Y} : \text{Gal}(K) \to \text{Aut}_{O_\lambda}(Y_\lambda)$ as the reduction of $\rho_{\ell,Y} : \text{Gal}(K) \to \text{Aut}_{O_\lambda}(T_\ell(Y))$ modulo $\lambda$.

It is known [14] that the Tate $\mathbb{Q}_\ell$-modules $V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and $V_\ell(Y) = T_\ell(Y) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ are $O_\lambda \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = E_\lambda$-vector spaces of dimension $\frac{2 \dim(X)}{\ell - 2}$ and $\frac{2 \dim(Y)}{\ell - 2}$ respectively. (Here $E_\lambda = E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is the completion of $E$ with respect to the $\lambda$-adic topology.) The groups $T_\ell(X)$ and $T_\ell(Y)$ are naturally identified with the $O_\lambda$-lattices in $V_\ell(X)$ and $V_\ell(Y)$ respectively and the inclusions

$$\text{Aut}_{O_\lambda}(T_\ell(X)) \subset \text{Aut}_{E_\lambda}(V_\ell(X)), \quad \text{Aut}_{O_\lambda}(T_\ell(Y)) \subset \text{Aut}_{E_\lambda}(V_\ell(Y))$$

allow us to consider $V_\ell(X)$ and $V_\ell(Y)$ as representations of $\text{Gal}(K)$ over $E_\lambda$.

Our task now is to prove that the natural representation of $\text{Gal}(K)$ in

$$V_1 := \text{Hom}_{E_\lambda}(V_\ell(Y), V_\ell(X))$$

over $E_\lambda$ is irreducible. For this, we may and will assume that $K$ is finitely generated over its prime subfield (replacing $K$ by a suitable subfield and using Remark [18]). Then the conjecture of Tate [20] (proven by the author in characteristic $> 2$ [21,22], Faltings in characteristic zero [15,6] and Mori in characteristic 2 [9]) asserts that the natural representation of $\text{Gal}(K)$ in $V_\ell(Z)$ over $\mathbb{Q}_\ell$ is completely reducible for any abelian variety $Z$ over $K$. In particular, the natural representations of $\text{Gal}(K)$ in $V_\ell(X)$ and $V_\ell(Y)$ over $\mathbb{Q}_\ell$ are completely reducible. It follows from Lemma 5.5 that the natural representations of $\text{Gal}(K)$ in $V_\ell(X)$ and $V_\ell(Y)$ over $E_\lambda$ are also completely reducible.

It follows easily that the dual Galois representation in $\text{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), E_\lambda)$ is also completely reducible. Since $E_\lambda$ has characteristic zero, it follows from a theorem of Chevalley [11, p. 88] that the Galois representation in the tensor product $\text{Hom}_{E_\lambda}(V_\ell(X), E_\lambda) \otimes_{E_\lambda} V_\ell(Y) = \text{Hom}_{E_\lambda}(V_\ell(X), V_\ell(Y)) = V_1$ is completely reducible.

Second, I claim that the natural representation of $\text{Gal}(K)$ in $V_1$ over $E_\lambda$ is irreducible. Indeed, the $O_\lambda$-module $\text{Hom}_{O_\lambda}(T_\ell(X), T_\ell(Y))$ is a $\text{Gal}(K)$-invariant $O_\lambda$-lattice in $\text{Hom}_{E_\lambda}(V_\ell(X), V_\ell(Y)) = V_1$. On the other hand, the reduction of this lattice modulo $\lambda$ coincides with

$$\text{Hom}_{O_\lambda}(T_\ell(X), T_\ell(Y)) \otimes_{O_\lambda} k(\lambda) = \text{Hom}_{k(\lambda)}(X_\lambda, Y_\lambda).$$

Now the desired irreducibility follows from Lemma 5.2.

Third, recall that there is a natural embedding [11, Sect. 19]

$$\text{Hom}^0(X,Y) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \subset \text{Hom}_{\mathbb{Q}_\ell}(V_\ell(X), V_\ell(Y)),$$

whose image is a $\text{Gal}(K)$-invariant $\mathbb{Q}_\ell$-vector subspace. Clearly, the image of $\text{Hom}^0((X,i),(Y,j)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ under this embedding lies in $\text{Hom}_{E_\lambda}(V_\ell(X), V_\ell(Y))$ and this image is a $\text{Gal}(K)$-invariant $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = E_\lambda$-vector subspace of $\text{Hom}_{E_\lambda}(V_\ell(X), V_\ell(Y))$. The irreducibility of $\text{Hom}_{E_\lambda}(V_\ell(X), V_\ell(Y))$ implies that either

$$\text{Hom}^0((X,i),(Y,j)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \text{Hom}_{E_\lambda}(V_\ell(X), V_\ell(Y))$$

or $\text{Hom}^0((X,i),(Y,j)) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = 0$. Since $\text{Hom}^0((X,i),(Y,j))$ is an $E$-vector space, either $\text{Hom}^0((X,i),(Y,j)) = 0$ or $\dim_E(\text{Hom}^0((X,i),(Y,j))) = \frac{4 \cdot \dim(X) \cdot \dim(Y)}{|E:Q|}$.
In the first case we are done. In the second case the result follows from Theorem □

REFERENCES

[1] Chevalley C.: Théorie des groupes de Lie, tome III. Hermann, Paris, 1954.
[2] Curtis, Ch. W., Reiner, I.: Methods of Representation Theory, Vol. I. John Wiley & Sons, New York Chichester Brisbane Toronto, 1981.
[3] Dixon J. D., Mortimer B., Permutation Groups. Springer-Verlag, New York Berlin Heidelberg, 1996.
[4] Faltings G.: Endlichkeitssätze für abelsche Varietäten über Zählkörpern. Invent. Math. 73, 349–366 (1983).
[5] Faltings G.: Complements to Mordell. In: in: Faltings G., Wustholz G. et al. (ed.) Rational points, Chapter VI. Third edition. Aspects of Mathematics, E6. Friedr. Vieweg & Sohn, Braunschweig, 1992.
[6] Herstein, I. N.: Noncommutative rings. Mathematical Association of America, Washington, DC, 1968.
[7] Ivanov, A. A., Praeger, Ch. E.: On finite affine 2-Arc transitive graphs. Europ. J. Combinatorics 14, 421–444 (1993).
[8] Klemm, M.: Über die Reduktion von Permutationsmoduln. Math. Z. 143, 113–117 (1975).
[9] Moret-Bailly, L.: Pinceaux de variétés abéliennes. Astérisque 129 (1985).
[10] Mortimer, B.: The modular permutation representations of the known doubly transitive groups. Proc. London Math. Soc. (3) 41, 1–20 (1980).
[11] Mumford, D.: Abelian varieties, Second edition. Oxford University Press, London, 1974.
[12] Oort, F.: The isogeny class of a CM-abelian variety is defined over a finite extension of the prime field. J. Pure Applied Algebra 3, 399–408 (1973).
[13] Poonen, B., Schaefer, E.: Explicit descent for Jacobians of cyclic covers of the projective line. J. reine angew. Math. 488, 141–188 (1997).
[14] Ribet, K.: Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. 98, 751–804 (1976).
[15] Schaefer, E.: Computing a Selmer group of a Jacobian using functions on the curve. Math. Ann. 310, 447–471 (1998).
[16] Schur, I.: Gleichungen ohne Affect. Sitz. Preuss. Akad. Wiss., Physik-Math. Klasse 443–449 (1930) (= Ges. Abh. III, 191–197).
[17] Serre, J.-P.: Lectures on the Mordell-Weil Theorem, 2nd edition, Friedr. Vieweg & Sons, Braunschweig/Wiesbaden, 1990.
[18] Serre, J.-P.: Topics in Galois Theory, Jones and Bartlett Publishers, Boston-London, 1992.
[19] Serre, J.-P.: Réprésentations linéaires des groupes finis, Troisième édition. Hermann, Paris, 1978.
[20] Tate, J. Endomorphisms of Abelian varieties over finite fields, Invent. Math. 2, 134–144 (1966).
[21] Zarhin, Yu. G.: Endomorphisms of Abelian varieties over fields of finite characteristic. Izv. Akad. Nauk SSSR ser. matem. 39, 272–277 (1975); Math. USSR Izv. 9, 255 - 260 (1975).
[22] Zarhin, Yu. G.: Abelian varieties in characteristic P. Mat. Zametki 19, 393–400 (1976); Mathematical Notes 19, 240–244 (1976).
[23] Zarhin, Yu. G.: Cyclic covers, their Jacobians and endomorphisms. J. reine angew. Math. 544, 91–110 (2002).
[24] Zarhin, Yu. G.: The endomorphism rings of Jacobians of cyclic covers of the projective line. Math. Proc. Cambridge Philos. Soc. 136, 257–267 (2004).
[25] Zarhin, Yu. G.: Endomorphism rings of certain Jacobians in finite characteristic. Matem. Sbornik 193, issue 8, 39–48 (2002); Sbornik Math. 193 (8), 1139-1149 (2002).
[26] Zarhin, Yu. G.: Homomorphisms of hyperelliptic Jacobians. In: Number Theory, Algebra and Algebraic Geometry (Shafarevich Festschrift). Trudy Mat. Inst. Steklov 241, 90–104 (2003); Proc. Steklov Inst. Math. 241, 79–92 (2003).
[27] Zarhin, Yu. G.: Homomorphisms of abelian varieties. In: Y. Aubry, G. Lachaude (ed.) Arithmetic, Geometry and Coding Theory (AGCT 2003), Séminaires et Congrès 11, 189-215 (2005).
[28] Zarhin, Yu. G.: Endomorphism algebras of superelliptic Jacobians. In: F. Bogomolov, Yu. Tschinkel (ed.) Geometric methods in Algebra and Number Theory, Progress in Math. 235, 339–362, Birkhäuser, Boston Basel Berlin, 2005.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802, USA

E-mail address: zarhin@math.psu.edu