ENOMORPHISM ALGEBRAS OF HYPERELLIPTIC JACOBIANS AND FINITE PROJECTIVE LINES

ARSEN ELKIN AND YURI G. ZARHIN

1. Statement of results

Let $K$ be a field with char($K$) $\neq 2$. Let us fix an algebraic closure $K_a$ of $K$. If $X$ is an abelian variety of positive dimension over $K_a$ then we write $\text{End}(X)$ for the ring of all its $K_a$-endomorphisms and $\text{End}^0(X)$ for the corresponding (semisimple finite-dimensional) $\mathbb{Q}$-algebra $\text{End}(X) \otimes \mathbb{Q}$. We write $\text{End}_K(X)$ for the ring of all $K$-endomorphisms of $X$ and $\text{End}^0_K(X)$ for the corresponding (semisimple finite-dimensional) $\mathbb{Q}$-algebra $\text{End}_K(X) \otimes \mathbb{Q}$. The absolute Galois group $\text{Gal}(K)$ of $K$ acts on $\text{End}(X)$ (and therefore on $\text{End}^0(X)$) by ring (resp. algebra) automorphisms and

$$\text{End}_K(X) = \text{End}(X)^{\text{Gal}(K)}, \quad \text{End}^0_K(X) = \text{End}^0(X)^{\text{Gal}(K)},$$

since every endomorphism of $X$ is defined over a finite separable extension of $K$.

If $n$ is a positive integer that is not divisible by char($K$) then we write $X_n$ for the kernel of multiplication by $n$ in $X(K_a)$. It is well-known [21] that $X_n$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2\dim(X)$. In particular, if $n = \ell$ is a prime then $X_\ell$ is an $\mathbb{F}_\ell$-vector space of dimension $2\dim(X)$.

If $X$ is defined over $K$ then $X_n$ is a Galois submodule in $X(K_a)$. It is known that all points of $X_n$ are defined over a finite separable extension of $K$. We write $\bar{\rho}_{n,X,K} : \text{Gal}(K) \to \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X_n)$ for the corresponding homomorphism defining the structure of the Galois module on $X_n$,

$$\tilde{G}_{n,X,K} \subset \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X_n)$$

for its image $\bar{\rho}_{n,X,K}(\text{Gal}(K))$ and $K(X_n)$ for the field of definition of all points of $X_n$. Clearly, $K(X_n)$ is a finite Galois extension of $K$ with Galois group $\text{Gal}(K(X_n)/K) = \tilde{G}_{n,X,K}$. If $n = \ell$ then we get a natural faithful linear representation

$$\tilde{G}_{\ell,X,K} \subset \text{Aut}_{\mathbb{F}_\ell}(X_\ell)$$

of $\tilde{G}_{\ell,X,K}$ in the $\mathbb{F}_\ell$-vector space $X_\ell$. Recall [29] that all endomorphisms of $X$ are defined over $K(X_4)$; this gives rise to the natural homomorphism

$$\kappa_{X,4} : \tilde{G}_{4,X,K} \to \text{Aut}(\text{End}^0(X))$$

and $\text{End}^0_K(X)$ coincides with the subalgebra $\text{End}^0(X)^{\tilde{G}_{4,X,K}}$ of $\tilde{G}_{4,X,K}$-invariants [38, Sect. 1].

Let $f(x) \in K[x]$ be a polynomial of degree $n \geq 3$ without multiple roots. Let $\mathfrak{R}_f \subset K_a$ be the $n$-element set of roots of $f$. Then $K(\mathfrak{R}_f)$ is the splitting field of $f$ and $\text{Gal}(f) := \text{Aut}(K(\mathfrak{R}_f)/K)$ is the Galois group of $f$ (over $K$). One may view $\text{Gal}(f)$ as a group of permutations of $\mathfrak{R}_f$; it is transitive if and only if $f(x)$ is irreducible.
Let us consider the hyperelliptic curve \( C_f : y^2 = f(x) \) and its Jacobian \( J(C_f) \). It is well-known [33] that \( J(C_f) \) is a \( \left\lfloor \frac{n+1}{2} \right\rfloor \)-dimensional abelian variety defined over \( K \). The aim of this paper is to study \( \text{End}^0(J(C_f)) \), assuming that \( n = q + 1 \) where \( q \) is a power of a prime \( p \) and \( \text{Gal}(f) = \text{PSL}_2(\mathbb{F}_q) \) acts via fractional-linear transformations on \( \mathbb{P}_f \) identified with the projective line \( \mathbb{P}^1(\mathbb{F}_q) \). It follows from results of [32, 35, 37] that for every \( q \) in all characteristics there exist \( K \) and \( f \) with \( \text{End}^0(J(C_f)) = \mathbb{Q} \). On the other hand, it is known that \( \text{End}^0(J(C_f)) = \mathbb{Q} \) \([32, 33, 39]\) if \( p = 2 \) and \( q \geq 8 \). (It is also true for \( q = 4 \) if one assumes that \( \text{char}(K) \neq 3 \) [37].) However, if \( q = 5 \) then there are examples where \( \text{End}^0(J(C_f)) \) is a (real) quadratic field (even in characteristic zero) \([4, 11, 31, 7]\).

Our main result is the following statement.

**Theorem 1.1.** Let us assume that \( \text{char}(K) = 0 \). Suppose that \( n = q + 1 \) where \( q \geq 5 \) is a prime power that is congruent to \( \pm 3 \) modulo 8. Suppose that \( f(x) \) is irreducible and \( \text{Gal}(f) \cong \text{PSL}_2(\mathbb{F}_q) \). Then one of the following two conditions holds:

(i) \( \text{End}^0(J(C_f)) = \mathbb{Q} \) or a quadratic field. In particular, \( J(C_f) \) is an absolutely simple abelian variety.

(ii) \( q \) is congruent to 3 modulo 8 and \( J(C_f) \) is \( K_n \)-isogenous to a self-product of an elliptic curve with complex multiplication by \( \mathbb{Q}(\sqrt{-q}) \).

**Remark 1.2.** It follows from results of [14] (see also [28], [25]) that if the case (ii) of Theorem 1.1 holds then \( J(C_f) \) is isomorphic over \( K_n \) to a product of mutually isogenous elliptic curves with complex multiplication by \( \mathbb{Q}(\sqrt{-q}) \).

The paper is organized as follows. Section 2 contains auxiliary results about endomorphism algebras of abelian varieties. In Section 3 we prove the main result. In Section 4 (and Section 5) we prove the absolute simplicity of \( J(C_f) \) when \( q \geq 11 \) is congruent to 3 modulo 8 and \( K = \mathbb{Q} \). Section 6 contains examples.

## 2. Endomorphism Algebras of Abelian Varieties

**Remark 2.1.** Recall [8] (see also [34, p. 199]) that a surjective homomorphism of finite groups \( \pi : G_1 \rightarrow G \) is called a minimal cover if no proper subgroup of \( G_1 \) maps onto \( G \). If \( H \) is a normal subgroup of \( G_1 \) that lies in \( \ker(\pi) \) then the induced surjection \( G_1/H \rightarrow G \) is also a minimal cover.

(i) If a surjection \( G_2 \rightarrow G_1 \) is also a minimal cover then one may easily check that the composition \( G_2 \rightarrow G \) is surjective and a minimal cover.

(ii) Clearly, if \( G \) is simple then every proper normal subgroup in \( G_1 \) lies in \( \ker(\pi) \).

(iii) If \( G \) is perfect then its universal central extension is a minimal cover [30].

(iv) If \( G' \rightarrow G \) is an arbitrary surjective homomorphism of finite groups then there always exists a subgroup \( H \subset G' \) such that \( H \rightarrow G \) is surjective and a minimal cover. Clearly, if \( G \) is perfect then \( H \) is also perfect.

The field inclusion \( K(X_2) \subset K(X_4) \) induces a natural surjection [38, Sect. 1]

\[ \tau_{2,X} : \tilde{G}_{4,X,K} \rightarrow \tilde{G}_{2,X,K}. \]

**Definition 2.2.** We say that \( K \) is 2-balanced with respect to \( X \) if \( \tau_{2,X} \) is a minimal cover.
Remark 2.3. Clearly, there always exists a subgroup \( H \subset \tilde{G}_{2,X,K} \) such that \( H \rightarrow \tilde{G}_{2,X,K} \) is surjective and a minimal cover. Let us put \( L = K(X_4)^H \). Clearly, \( K \subset L \subset K(X_4) \), \( L \cap K(X_2) = K \) and \( L \) is a maximal overfield of \( K \) that enjoys these properties. It is also clear that \( K(X_2) \subset L(X_2) \), \( L(X_4) = K(X_4) \), \( H = \tilde{G}_{4,X,L} \), \( \tilde{G}_{2,X,L} = \tilde{G}_{2,X,K} \) and \( L \) is 2-balanced with respect to \( X \).

The following assertion (and its proof) is (are) inspired by Theorem 1.6 of [38] (and its proof).

Theorem 2.4. Suppose that \( E := \text{End}^0_K(X) \) is a field that contains the center \( C \) of \( \text{End}^0_K(X) \). Let \( C_{X,K} \) be the centralizer of \( \text{End}^0_K(X) \) in \( \text{End}^0(X) \). Then:

(i) \( C_{X,K} \) is a central simple \( E \)-subalgebra in \( \text{End}^0(X) \). In addition, the centralizer of \( C_{X,K} \) in \( \text{End}^0(X) \) coincides with \( E = \text{End}^0_K(X) \) and

\[
\dim_E(C_{X,K}) = \frac{\dim_C(\text{End}^0(X))}{[E : C]^2}.
\]

(ii) Assume that \( K \) is 2-balanced with respect to \( X \) and \( \tilde{G}_{2,X,K} \) is a non-abelian simple group. If \( \text{End}^0(X) \neq E \) (i.e., not all endomorphisms of \( X \) are defined over \( K \)) then there exist a finite perfect group \( \Pi \subset C_{X,K}^* \) and a surjective homomorphism \( \Pi \rightarrow \tilde{G}_{2,X,K} \) that is a minimal cover. In addition, the induced homomorphism

\[
E[\Pi] \rightarrow C_{X,K}
\]

is surjective, i.e., \( C_{X,K} \) is isomorphic to a direct summand of the group algebra \( E[\Pi] \).

Proof. Since \( E \) is a field, \( C \) is a subfield of \( E \) and therefore \( \text{End}^0(X) \) is a central simple \( C \)-algebra. Now the assertion (i) follows from Theorem 2 of Sect. 10.2 in Chapter VIII of [5].

Now let us prove the assertion (ii).

Recall that there is the homomorphism

\[
k_{X,4} : \tilde{G}_{4,X,K} \rightarrow \text{Aut}(\text{End}^0(X))
\]

such that

\[
\text{End}^0(X)\tilde{G}_{4,X,K} = \text{End}^0_K(X) = E \subset C.
\]

This implies that

\[
k_{X,4}(\tilde{G}_{4,X,K}) \subset \text{Aut}_E(\text{End}^0(X)) \subset \text{Aut}_C(\text{End}^0(X))
\]

and we get a homomorphism

\[
k_E : \tilde{G}_{4,X,K} \rightarrow \text{Aut}_E(C_{X,K})
\]

such that

\[
C_{X,K}^{\tilde{G}_{4,X,K}} = E.
\]
Assume that \( E = C_{X,K} \), i.e., \( E \) coincides with its own centralizer in \( \text{End}^0(X) \). It follows from the Skolem-Noether theorem that \( \text{Aut}_C(\text{End}^0(X)) = \text{End}^0(X)^*/C^* \). This implies that the group
\[
\text{Aut}_E(\text{End}^0(X)) = C_{X,K}^*/C^* = E^*/C^*
\]
is commutative. It follows that \( \kappa_{X,4}(\hat{G}_{4,X,K}) \) is commutative. Since \( \hat{G}_{4,X,K} \) is perfect, \( \kappa_{X,4}(\hat{G}_{4,X,K}) \) is perfect commutative and therefore trivial, i.e., \( \text{End}^0(X) = \text{End}^0_K(X) \).

Assume that \( E \neq C_{X,K} \). This means that the group \( \Gamma := \kappa_E(\hat{G}_{4,X,K}) \) is not \( \{1\} \), i.e., \( \ker(\kappa_E) \neq \hat{G}_{4,X,K} \). Clearly, \( \Gamma \) is a finite perfect subgroup of \( \text{Aut}_E(C_{X,K}) \).

The minimality of \( \tau_{2,X} \) and the simplicity of \( \hat{G}_{2,X,K} \) imply the existence of a minimal cover
\[
\Gamma \to \hat{G}_{2,X,K},
\]
thanks to Remark 2.1.

Since \( C_{X,K} \) is a central simple \( E \)-algebra, all its automorphisms are inner, i.e., \( \text{Aut}_E(C_{X,K}) = C_{X,K}^*/E^* \). Let \( \Delta \to \Gamma \) be the universal central extension of \( \Gamma \). It is well-known [30, Ch. 2, Sect. 9] that \( \Delta \) is a finite perfect group. The universality property implies that \( \Delta \to \Gamma \) is a minimal cover and the inclusion map \( \Gamma \subseteq C_{X,K}^*/E^* \) lifts (uniquely) to a homomorphism \( \pi : \Delta \to C_{X,K}^* \). Clearly, \( \ker(\pi) \) lies in the kernel of \( \Delta \to \Gamma \) and we get a minimal cover
\[
\pi(\Delta) \cong \Delta/\ker(\pi) \to \Gamma,
\]
thanks to Remark 2.1. Taking the compositions of minimal covers \( \pi(\Delta) \to \Gamma \) and \( \Gamma \to \hat{G}_{2,X,K} \), we obtain a minimal cover \( \pi(\Delta) \to \hat{G}_{2,X,K} \). If we put
\[
\Pi := \pi(\Delta) \subseteq C_{X,K}^*,
\]
then we get a minimal cover
\[
\Pi \to \hat{G}_{2,X,K}.
\]
The equality (1) means that the centralizer of \( \pi(\Delta) = \Pi \) in \( C_{X,K} \) coincides with \( E \). It follows that if \( E[\Pi] \) is the group \( E \)-algebra of \( \Pi \) then the inclusion \( \Pi \subseteq C_{X,K}^* \) induces the \( E \)-algebra homomorphism \( \omega : E[\Pi] \to C_{X,K} \) such that the centralizer of its image in \( C_{X,K} \) coincides with \( E \).

We claim that \( \omega(E[\Pi]) = C_{X,K} \) and therefore \( C_{X,K} \) is isomorphic to a direct summand of \( E[\Pi] \). This claim follows easily from the next lemma that was proven in [38, Lemma 1.7]

**Lemma 2.5.** Let \( F \) be a field of characteristic zero, \( T \) a semisimple finite-dimensional \( F \)-algebra, \( S \) a finite-dimensional central simple \( F \)-algebra, \( \beta : T \to S \) an \( F \)-algebra homomorphism that sends 1 to 1. Suppose that the centralizer of the image \( \beta(T) \) in \( S \) coincides with the center \( F \). Then \( \beta \) is surjective, i.e., \( \beta(T) = S \).

\[ \square \]

**Theorem 2.6.** Suppose that \( \text{End}^0(X) \) is a simple \( \mathbb{Q} \)-algebra, \( \hat{G}_{2,X,K} \) is a simple non-abelian group, whose order is not a divisor of \( 2 \dim(X) \) and \( \text{End}_K \hat{G}_{2,X,K}(X_2) \cong \mathbb{F}_4 \).

Then the center \( C \) of \( \text{End}^0(X) \) is either \( \mathbb{Q} \) or a quadratic field. In addition, there exists a finite separable field extension \( L/K \) such that \( \hat{G}_{2,X,L} = \hat{G}_{2,X,K} \), the map \( \tau_{2,X} : \hat{G}_{4,X,L} \to \hat{G}_{2,X,L} \) is surjective and a minimal cover, the \( \mathbb{Q} \)-algebra
Definition 2.7. We say that a group is trivially, i.e., $C \subseteq L$. Theorem 2.4 (to follow): Suppose also that $\tilde{G}_{2,X,K}$ is a minimal cover. In addition, the induced homomorphism

$$E[\Pi] \rightarrow C_{X,L}$$

is surjective, i.e., $C_{X,L}$ is isomorphic to a direct summand of the group algebra $E[\Pi]$.

Proof. Choose a field $L$ as in Remark 2.3. Then $\tilde{G}_{2,X,L} = \tilde{G}_{2,X,K}$, the map

$$\tau_{2,X} : \tilde{G}_{4,X,L} \rightarrow \tilde{G}_{2,X,L} = \tilde{G}_{2,X,K}$$

is surjective and a minimal cover. We have

$$\text{End}_{L}(X) \otimes \mathbb{Z}/2\mathbb{Z} \hookrightarrow \text{End}_{\text{Gal}(L)}(X_2) = \text{End}_{\tilde{G}_{2,X,L}}(X_2) = \mathbb{F}_4.$$ 

It follows that the rank of the free $\mathbb{Z}$-module $\text{End}_{L}(X)$ is 1 or 2; Lemma 1.3 of [38] implies that $\text{End}_{L}(X)$ has no zero divisors. This implies that $\text{End}^0_{L}(X) = \text{End}_{L}(X) \otimes \mathbb{Q}$ is a division algebra of $\mathbb{Q}$-dimension 1 or 2. This means that $E = \text{End}^0_{L}(X)$ is either $\mathbb{Q}$ or a quadratic field.

Recall that the center $C$ of $\text{End}^0_{L}(X)$ is a number field, whose degree $|C : \mathbb{Q}|$ divides $2\text{dim}(X)$. The group $\tilde{G}_{4,X,L}$ acts via automorphisms on $C$ and

$$C^{\tilde{G}_{4,X,L}} = C \cap \text{End}^0_{L}(X)$$

is either $\mathbb{Q}$ or a quadratic field. Since $\tilde{G}_{2,X,L} = \tilde{G}_{2,X,K}$ has no normal subgroups of index dividing $2\text{dim}(X)$, the same is true for $\tilde{G}_{4,X,L}$ and therefore $\tilde{G}_{4,X,L}$ acts on $C$ trivially, i.e., $C \subseteq \text{End}^0_{L}(X)$. In order to finish the proof, one has only to apply Theorem 2.4 (to $L$ instead of $K$).

THEOREM 2.8. Let us assume that $\text{char}(K) = 0$. Suppose that $\text{End}^0_{L}(X)$ is a simple $\mathbb{Q}$-algebra with the center $C$. Suppose that $\tilde{G}_{2,X,K}$ is a simple non-abelian group, whose order is not a divisor of $2\text{dim}(X)$ and $\text{End}_{\tilde{G}_{2,X,K}}(X_2) \cong \mathbb{F}_4$. Assume, in addition, that $\tilde{G}_{2,X,K}$ is a known simple group that is not FTKL-exceptional. Suppose also that $\text{dim}(X)$ coincides with the smallest positive integers $d$ such that $\tilde{G}_{2,X,K}$ is isomorphic to a subgroup of $\text{PGL}(d, \mathbb{C})$. Then:

(i) The center $C$ of $\text{End}^0_{L}(X)$ is either $\mathbb{Q}$ or quadratic field.

(ii) Either $\text{End}^0_{L}(X) = C$ or the following conditions hold:
(1) There exists a finite algebraic field extension \( L/K \) such that \( \tilde{G}_{2,X,L} = \tilde{G}_{2,X,K} \); the overfield \( L \) is 2-balanced with respect to \( X \), the algebra \( E := \text{End}_{k}^{0}(X) \) is either \( \mathbb{Q} \) or a quadratic field, \( C = E \) and the following conditions hold.

There exist a finite perfect group \( \Pi \subset \text{End}^{0}(X)^{+} \) and a surjective homomorphism \( \Pi \to \tilde{G}_{2,X,K} \) that is a minimal cover and a central extension. In addition, the induced homomorphism

\[
E[\Pi] \to \text{End}^{0}(X)
\]

is surjective, i.e., \( \text{End}^{0}(X) \) is isomorphic to a direct summand of the group algebra \( E[\Pi] \).

(2) If \( C = \mathbb{Q} \) then \( X \) enjoys one of the following two properties:

(a) \( X \) is isogenous over \( K_{a} \) to a self-product of an elliptic curve without complex multiplication.

(b) \( \dim(X) \) is even and \( X \) is isogenous over \( K_{a} \) to a self-product of an abelian surface \( Y \) such that \( \text{End}^{0}(Y) \) is an indefinite quaternion \( \mathbb{Q} \)-algebra.

(3) If \( C \neq \mathbb{Q} \) then \( C \) is an imaginary quadratic field and \( X \) is isogenous over \( K_{a} \) to a self-product of an elliptic curve with complex multiplication by \( C \).

Proof. Using Theorem 2.6 and replacing if necessary \( K \) by its suitable extension, we may assume that \( K \) is 2-balanced with respect to \( X \), the algebra \( E := \text{End}_{k}^{0}(X) \) is either \( \mathbb{Q} \) or a quadratic field, \( C \subset E \) and the following conditions hold.

Either \( \text{End}^{0}(X) = E \) or there exist a finite perfect group \( \Pi \subset C_{X,K}^{2} \) and a surjective homomorphism \( \Pi \to \tilde{G}_{2,X,K} \) that is a minimal cover and such that the induced homomorphism

\[
E[\Pi] \to C_{X,K}
\]

is surjective, i.e., \( C_{X,K} \) is isomorphic to a direct summand of the group algebra \( E[\Pi] \). (Here as above \( C_{X,K} \) is the centralizer of \( E \) in \( \text{End}^{0}(X) \)).

Assume that \( \text{End}^{0}(X) \neq E \). We are going to prove that \( \Pi \to \tilde{G}_{2,X,K} \) is a central extension, using results of Feit-Tits and Kleidman-Liebeck [8, 15]. Without loss of generality we may assume that there is a field embedding \( K_{a} \to \mathbb{C} \) and consider \( X \) as complex abelian variety. Let \( t_{X} \) be the Lie algebra of \( X \) that is a \( \dim(X) \)-dimensional complex vector space. By functoriality, this gives us the embeddings

\[
j : \text{End}^{0}(X) \to \text{End}_{\mathbb{C}}(t_{X}) \cong M_{\dim(X)}(\mathbb{C}),
\]

\[
j : \text{End}^{0}(X)^{*} \to \text{Aut}_{\mathbb{C}}(t_{X}) \cong \text{GL}(\dim(X), \mathbb{C}).
\]

Clearly, only central elements of \( \Pi \) go to scalars under \( j \). It follow that there exists a central subgroup \( Z \) in \( \Pi \) such that \( j(Z) \) consists of scalars and \( \Pi/Z \to \text{PGL}(\dim(X), \mathbb{C}) \). The simplicity of \( \tilde{G}_{2,X,K} \) implies that \( Z \) lies in the kernel of \( \Pi \to \tilde{G}_{2,X,K} \) and the induced map \( \Pi/Z \to \tilde{G}_{2,X,K} \) is a central extension of \( \tilde{G}_{2,X,K} \). Since \( \Pi \) is a central extension of \( \Pi/Z \), it follows from Theorem on p. 1092 of [8] and Theorem 3 on p. 316 of [15] that \( \Pi/Z \to \tilde{G}_{2,X,K} \) is a central extension of \( \tilde{G}_{2,X,K} \). Since \( \Pi \) is a central extension of \( \Pi/Z \), it follows [30] that \( \Pi \) is a central extension of \( \tilde{G}_{2,X,K} \).

Now notice that \( t_{X} \) carries a natural structure of \( E \otimes_{\mathbb{Q}} \mathbb{C} \)-module. Assume that \( E \neq \mathbb{Q} \); i.e., \( E \) is a quadratic field. Let \( \sigma, \tau : E \to \mathbb{C} \) be the two different embeddings
of $E$ into $\mathbb{C}$. Then

$$E \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}_\sigma \oplus \mathbb{C}_\tau$$

with

$$\mathbb{C}_\sigma = E \otimes_{E, \sigma} \mathbb{C} = \mathbb{C}, \quad \mathbb{C}_\tau = E \otimes_{E, \tau} \mathbb{C} = \mathbb{C}$$

and $t_X$ splits into a direct sum

$$t_X = \mathbb{C}_\sigma t_X \oplus \mathbb{C}_\tau t_X.$$ 

Suppose that both $\mathbb{C}_\sigma t_X$ and $\mathbb{C}_\tau t_X$ do not vanish. Then the $\mathbb{C}$-dimension $d_\sigma$ of non-zero $\mathbb{C}_\sigma t_X$ is strictly less than $\dim(X)$. Clearly, $\mathbb{C}_\sigma t_X$ is $C_{X,K}$-stable and we get a nontrivial homomorphism

$$C_{X,K} \to \text{End}_\mathbb{C}(\mathbb{C}_\sigma t_X) \cong M_{d_\sigma}(\mathbb{C})$$

that must be an embedding in light of the simplicity of $C_{X,K}$. This gives us an embedding

$$C_{X,K}^* \to \text{Aut}_\mathbb{C}(\mathbb{C}_\sigma t_X) \cong \text{GL}(d_\sigma, \mathbb{C}).$$

One may easily check that all the elements of $\Pi$ that go to scalars in $\text{Aut}_\mathbb{C}(\mathbb{C}_\sigma t_X)$ constitute a central subgroup $Z_\sigma$ that lies in the kernel of $\Pi \to \tilde{G}_{2,X,K}$. This gives us a central extension $\Pi/Z_\sigma \to \tilde{G}_{2,X,K}$ that is a minimal cover and an embedding $\Pi/Z_\sigma \hookrightarrow \text{Aut}_\mathbb{C}(\mathbb{C}_\sigma t_X) \cong \text{GL}(d_\sigma, \mathbb{C})$. Since $d_\sigma < \dim(X)$, Theorem on p. 1092 of [8] and Theorem 3 on p. 316 of [15] provide us with a contradiction. It follows that either $\mathbb{C}_\sigma t_X$ or $\mathbb{C}_\tau t_X$ does vanish. We may assume that $\mathbb{C}_\tau t_X = 0$. This means that each $e \in E$ acts on $t_X$ as multiplication by complex number $\sigma(e)$, i.e., $j(E)$ consists of scalars. Recall that the exponential map identifies $X(\mathbb{C})$ with the complex torus $t_X/\Lambda$ where $\Lambda$ is a discrete lattice of rank $2\dim(X)$. In addition, $\Lambda$ is $j(\text{End}_K(X))$-stable where $\text{End}_K(X)$ is an order in the quadratic field $\text{End}_K(X)$. Now the discreteness of $\Lambda$ implies that $E$ cannot be real and therefore is an imaginary quadratic field. It follows easily that $X$ is isogenous over $\mathbb{C}$ to a self-product of an elliptic curve with complex multiplication by $E$. In particular, $E = \mathbb{C}$ and $C_{X,K} = \text{End}^0(X)$.

Now let us assume that $E = \mathbb{Q}$. Then $C_{X,K} = \text{End}^0(X)$. Let $Y$ be an absolutely simple abelian variety such that $X$ is isogenous to a self-product $Y^r$ for some positive integer $r$ with $r \mid \dim(X)$. Then $\text{End}^0(Y) \cong M_r(\text{End}^0(Y))$. In particular, the center of the division algebra $\text{End}^0(Y)$ is $\mathbb{Q}$. It follows from Albert’s classification [21] that $\text{End}^0(Y)$ is either $\mathbb{Q}$ or a quaternion $\mathbb{Q}$-algebra.

If $\text{End}^0(Y) = \mathbb{Q}$ then $\text{End}^0(X) \cong M_r(\mathbb{Q})$ and $\Pi/Z \hookrightarrow \text{PGL}(r, \mathbb{Q}) \subset \text{PGL}(r, \mathbb{C})$. It follows that $r = \dim(X)$, i.e. $Y$ is an elliptic curve without complex multiplication.

Suppose that $\text{End}^0(Y)$ is a quaternion $\mathbb{Q}$-algebra. Since $\dim(Y) = \dim(X)/r$ and we live in characteristic zero, $2r$ divides $\dim(X)$. Clearly,

$$\text{End}^0(Y) \subset \text{End}^0(Y) \otimes_{\mathbb{Q}} \mathbb{C} \cong M_2(\mathbb{C})$$

and therefore

$$\text{End}^0(X) \cong M_r(\text{End}^0(Y)) \hookrightarrow M_{2r}(\mathbb{C}).$$

This implies that $\Pi \hookrightarrow \text{GL}(2r, \mathbb{C})$. It follows that $2r = \dim(X)$, i.e., $\dim(Y) = 2$. It follows from the classification of endomorphism algebras of abelian surfaces [22, Sect. 6] that $\text{End}^0(Y)$ is an indefinite quaternion $\mathbb{Q}$-algebra. $\square$
Let us assume that \( \text{char}(K) = 0 \). Suppose that \( \text{End}^0(X) \) is a simple \( \mathbb{Q} \)-algebra. Suppose that \( d := \dim(X) = (q - 1)/2 \) where \( q \geq 5 \) is an odd prime power. Suppose that \( \widetilde{G}_{2, X, K} \cong \text{PSL}_2(\mathbb{F}_q) \) and \( \text{End}_{\widetilde{G}_{2, X, K}}(X_2) \cong \mathbb{F}_4 \). Then one of the following two conditions holds:

(i) \( \text{End}^0(X) = \mathbb{Q} \) or a quadratic field. In particular, \( X \) is an absolutely simple abelian variety.

(ii) \( q \) is congruent to 3 modulo 4 and \( X \) is \( K \)-isogenous to a self-product of an elliptic curve with complex multiplication by \( \mathbb{Q}(\sqrt{-1}) \).

Proof. It is well-known [10, Sect. 4.15] that \( \text{SL}_2(\mathbb{F}_q) \) is the universal central extension of \( \text{PSL}_2(\mathbb{F}_q) \) and therefore every projective representation of \( \text{PSL}_2(\mathbb{F}_q) \) lifts to a linear representation of \( \text{SL}_2(\mathbb{F}_q) \). The well-known list of irreducible representations of \( \text{SL}_2(\mathbb{F}_q) \) over complex numbers [6, Sect. 38] tells us that the smallest degree of a nontrivial representation of \( \text{SL}_2(\mathbb{F}_q) \) is \( (q - 1)/2 = d \). This implies that we are in position to apply Theorem 2.8. In particular, \( C \) is either \( \mathbb{Q} \) or a quadratic field.

We may and will assume that \( \text{End}^0(X) \neq C \).

We need to rule out the following possibilities:

1. \( \dim(X) \) is even and \( X \) is isogenous over \( K \) to a self-product of an abelian surface \( Y \) such that \( \text{End}^0(Y) \) is an indefinite quaternion \( \mathbb{Q} \)-algebra. In particular, \( \text{End}^0(X) \) is a \( d^2 \)-dimensional central simple \( \mathbb{Q} \)-algebra.

2. \( q \) is congruent to 1 modulo 4 and \( X \) is isogenous over \( K \) to a self-product of an elliptic curve with complex multiplication. In particular, \( \text{End}^0(X) \) is a \( d^2 \)-dimensional central simple algebra over the imaginary quadratic field \( C \) unramified at \( \infty \).

3. \( X \) is isogenous over \( K \) to a self-product of an elliptic curve without complex multiplication. In particular, \( \text{End}^0(X) \) is a \( d^2 \)-dimensional central simple \( \mathbb{Q} \)-algebra.

By Theorem 2.8, there exist a finite perfect group \( \Pi \) and a minimal central cover \( \Pi \to \text{PSL}_2(\mathbb{F}_q) \) such that \( \text{End}^0(X) \) is a quotient of the group algebra \( E[\Pi] \) where \( E = C \) is either \( \mathbb{Q} \) or an imaginary quadratic field. It follows easily that \( \Pi = \text{PSL}_2(\mathbb{F}_q) \) or \( \text{SL}_2(\mathbb{F}_q) \), so we may always view \( \text{End}^0(X) \) as a simple quotient (direct summand) \( D \) of \( E[\text{SL}_2(\mathbb{F}_q)] \). By Theorem 2.8, \( \text{End}^0(X) \) is a central simple \( E \)-algebra of dimension \( d^2 \).

Let us consider the composition

\[
\mathbb{Q}[\text{SL}_2(\mathbb{F}_q)] \subset E[\text{SL}_2(\mathbb{F}_q)] \twoheadrightarrow \text{End}^0(X).
\]

Let \( D \) be the simple direct summand of \( \mathbb{Q}[\text{SL}_2(\mathbb{F}_q)] \), whose image in the simple \( \mathbb{Q} \)-algebra \( \text{End}^0(X) \) is not zero. We write \( B \subset \text{End}^0(X) \) for the image of \( D \): it is a \( \mathbb{Q} \)-subalgebra isomorphic to \( D \). The induced map \( D \to \text{End}^0(X) \) is injective, because \( D \) is a simple \( \mathbb{Q} \)-algebra. On the other hand, \( D_E = D \otimes \mathbb{Q} E \) is a direct summand of \( E[\text{SL}_2(\mathbb{F}_q)] \) and the image of \( D_E \to \text{End}^0(X) \) is a non-zero ideal of \( \text{End}^0(X) \). Since \( \text{End}^0(X) \) is simple, \( D_E \to \text{End}^0(X) \) is surjective. In particular, \( B \) generates \( \text{End}^0(X) \) as \( E \)-vector space and the center of \( D \) embeds into the center \( E \) of \( \text{End}^0(X) \). This implies that the center of \( D \) is either \( \mathbb{Q} \) or isomorphic to \( E \).

In addition, if the center of \( D \) is isomorphic to \( E \) then \( B \) contains \( E \), i.e., \( B \) is a \( E \)-vector subspace of \( \text{End}^0(X) \) and therefore coincides with \( \text{End}^0(X) \): this implies that \( \text{End}^0(X) \cong D \).
Assume that the center of \( D \) is isomorphic to \( E \). Then \( \text{End}^0(X) \cong D \) and therefore \( D \) is a central simple \( \mathbb{E} \)-algebra of dimension \( d^2 \). This means that the simple direct summand \( D \) of \( \mathbb{R}[\text{SL}_2(\mathbb{F}_{q})] \) corresponds to an irreducible (complex) character of \( \text{SL}_2(\mathbb{F}_{q}) \) of degree \( d \) as in Lemma 24.7 of [6]. These simple direct summands are described explicitly in [13, 9]. In particular, if \( q \) is congruent to 1 modulo 4 but is not a square then the center of \( D \) is a real quadratic field \( \mathbb{Q}(\sqrt{q}) \), which is not the case. This implies that \( q \) is congruent to 3 modulo 4: in this case the center of \( D \) is an imaginary quadratic field \( \mathbb{Q}(\sqrt{-q}) \) and therefore \( E = \mathbb{Q}(\sqrt{-q}) \). It follows from Theorem 2.8 that \( X \) is \( K_{\alpha} \)-isogenous to a self-product of an elliptic curve with complex multiplication by \( \mathbb{Q}(\sqrt{-q}) \).

Now assume that the center of \( D \) is not isomorphic to \( E \). Then it must be \( \mathbb{Q} \), i.e., \( D \) is a central simple \( \mathbb{Q} \)-algebra. It follows that \( D_E \) is a central simple \( \mathbb{E} \)-algebra and therefore the surjective homomorphism \( D_E \rightarrow \text{End}^0(X) \) is injective. It follows that \( D_E \cong \text{End}^0(X) \); in particular, the central simple \( \mathbb{Q} \)-algebra \( D \) has \( \mathbb{Q} \)-dimension \( d^2 \). As above, this means that the simple direct summand \( D \) corresponds to an irreducible (complex) character of \( \text{SL}_2(\mathbb{F}_{q}) \) of degree \( d \). Since the center of \( D \) is \( \mathbb{Q} \), it follows from results of [13, 9] that \( q \) is a square, which is not the case. This ends the proof.

3. Hyperelliptic Jacobians

Suppose that \( f(x) \in K[x] \) is a polynomial of degree \( n \geq 5 \) without multiple roots. Let \( \mathfrak{R}_f \subset K_a \) be the set of roots of \( f \). Clearly, \( \mathfrak{R}_f \) consists of \( n \) elements. Let \( K(\mathfrak{R}_f) \subset K_a \) be the splitting field of \( f \). Clearly, \( K(\mathfrak{R}_f)/K \) is a Galois extension and we write \( \text{Gal}(f) \) for its Galois group \( \text{Gal}(K(\mathfrak{R}_f)/K) \). By definition, \( \text{Gal}(K(\mathfrak{R}_f)/K) \) permutes elements of \( \mathfrak{R}_f \); further we identify \( \text{Gal}(f) \) with the corresponding subgroup of \( \text{Perm}(\mathfrak{R}_f) \), where \( \text{Perm}(\mathfrak{R}_f) \) is the group of permutations of \( \mathfrak{R}_f \).

We write \( \mathbb{F}_{2}^{\mathfrak{R}_f} \) for the \( n \)-dimensional \( \mathbb{F}_2 \)-vector space of maps \( h : \mathfrak{R}_f \rightarrow \mathbb{F}_2 \). The space \( \mathbb{F}_{2}^{\mathfrak{R}_f} \) is provided with a natural action of \( \text{Perm}(\mathfrak{R}_f) \) defined as follows. Each \( s \in \text{Perm}(\mathfrak{R}_f) \) sends a map \( h : \mathfrak{R}_f \rightarrow \mathbb{F}_2 \) to \( sh : \alpha \mapsto h(s^{-1}(\alpha)) \). The permutation module \( \mathbb{F}_{2}^{\mathfrak{R}_f} \) contains the \( \text{Perm}(\mathfrak{R}_f) \)-stable hyperplane

\[
(\mathbb{F}_{2}^{\mathfrak{R}_f})^0 = \{ h : \mathfrak{R}_f \rightarrow \mathbb{F}_2 \mid \sum_{\alpha \in \mathfrak{R}_f} h(\alpha) = 0 \}
\]

and the \( \text{Perm}(\mathfrak{R}_f) \)-invariant line \( \mathbb{F}_2 \cdot 1_{\mathfrak{R}_f} \) where \( 1_{\mathfrak{R}_f} \) is the constant function 1. Clearly, \( (\mathbb{F}_{2}^{\mathfrak{R}_f})^0 \) contains \( \mathbb{F}_2 \cdot 1_{\mathfrak{R}_f} \) if and only if \( n \) is even.

If \( n \) is even then let us define the \( \text{Gal}(f) \) module \( Q_{\mathfrak{R}_f} := (\mathbb{F}_{2}^{\mathfrak{R}_f})^0/(\mathbb{F}_{2} \cdot 1_{\mathfrak{R}_f}) \). If \( n \) is odd then let us put \( Q_{\mathfrak{R}_f} := (\mathbb{F}_{2}^{\mathfrak{R}_f})^0 \). If \( n \neq 4 \) the natural representation of \( \text{Gal}(f) \) is faithful, because in this case the natural homomorphism \( \text{Perm}(\mathfrak{R}_f) \rightarrow \text{Aut}_{\mathbb{F}_2}(Q_{\mathfrak{R}_f}) \) is injective.

The canonical surjection \( \text{Gal}(K) \twoheadrightarrow \text{Gal}(K(\mathfrak{R}_f)/K) = \text{Gal}(f) \) provides \( Q_{\mathfrak{R}_f} \) with a natural structure of \( \text{Gal}(K) \)-module. It is well-known that the \( \text{Gal}(K) \) modules \( J(C_f)_2 \) and \( Q_{\mathfrak{R}_f} \) are isomorphic (see for instance [23, 24, 33]). It follows easily that \( K(J(C_f)_2) = K(\mathfrak{R}_f) \) and \( G_{2,J(C_f)_2,K} = \text{Gal}(f) \).

Let us put \( X = J(C_f) \) and \( G := G_{2,X,K} \). Then \( G \cong \text{Gal}(f) \), and the \( G \)-modules \( X_2 \) and \( Q_{\mathfrak{R}_f} \) are isomorphic. We freely interchange these two modules throughout this section.
Example 3.1. Suppose that $n = q + 1$ where $q \geq 5$ is a power of an odd prime $p$. Suppose that $\text{Gal}(f) = \text{PSL}_2(\mathbb{F}_q)$. Assume that that $f(x)$ is irreducible, i.e., $\text{Gal}(f) = \text{PSL}_2(\mathbb{F}_q)$ acts transitively on the $(q + 1)$-element set $\mathcal{R}_f$. If $\beta \in \mathcal{R}_f$, then its stabilizer $\text{Gal}(\beta)$ is a subgroup of index $q + 1$ and therefore contains a Sylow $p$-subgroup of $\text{PSL}_2(\mathbb{F}_q)$. It follows from the classification of subgroups of $\text{PSL}_2(\mathbb{F}_q)$ [30, Theorem 6.25 on page 412] and explicit description of its Sylow $p$-subgroup and their normalizers [12, p. 191–192] that $\text{Gal}(\beta)$ is isomorphic to a power of an absolutely simple abelian variety.

Assume, in addition that $q$ is congruent to $±3$ modulo $8$. Then it is known [20] that

$$\text{End}_{\text{Gal}(f)}(Q_{\mathcal{R}_f}) = \mathbb{F}_4.$$  

Theorem 3.2. Suppose that $\text{char}(K) \neq 2$ and $n = q + 1$ where $q \geq 5$ is a prime power that is congruent to $±3$ modulo $8$. Suppose that $\text{Gal}(f) = \text{PSL}_2(\mathbb{F}_q)$ acts doubly transitively on $\mathcal{R}_f$ (where $\mathcal{R}_f$ is identified with the projective line $\mathbb{P}^1(\mathbb{F}_q)$). Then $\text{End}^0(J(C_f))$ is a simple $\mathbb{Q}$-algebra, i.e., $J(C_f)$ is either absolutely simple or isogenous to a power of an absolutely simple abelian variety.

Proof. See [38, Theorem 3.10].

Proof of Theorem 1.1. The result follows from Theorem 2.9 combined with Example 3.1 and Theorem 3.2. □

4. Criteria for Absolute Simplicity

Sometimes, it is possible to rule out the second outcome of Theorem 1.1. First, recall Goursat’s lemma [16, p. 75]:

Lemma 4.1. Let $G_1$ and $G_2$ be finite groups, and $H$ a subgroup of $G_1 \times G_2$ such that the restrictions $p_1 : H \to G_1$ and $p_2 : H \to G_2$ of the projection maps are surjective. Let $H_1$ and $H_2$ be the normal subgroups of $G_1$ and $G_2$, respectively, such the groups $H_1 \times \{1\}$ and $\{1\} \times H_2$ are kernels of $p_2$ and $p_1$, respectively. Then there exist an isomorphism $\gamma : G_1/H_1 \cong G_1/H_2$ such that $H$ coincides with the preimage in $G_1 \times G_2$ of the graph of $\gamma$ in $G_1/H_1 \times G_2/H_2$.

Example 4.2. Let $G_1$ be a finite simple group and $G_2$ be a finite group that does not admit $G_1$ as a quotient. If $H$ is a subgroup of $G_1 \times G_2$ that satisfies the conditions of Goursat’s lemma, then $H = G_1 \times G_2$.

Indeed, since $G_1$ is simple, $H_1 = \{1\}$ or $G_1$. We have $H_1 \neq \{1\}$, since otherwise $G_1/H_1 \cong G_1$ and no quotient of $G_2$ is isomorphic to $G_1$. Therefore, $H_1 = G_1$, $G_1/H_1 \cong G_2/H_2 = \{1\}$, and $H_2 = G_2$. Since $G_1/H_1 \times G_2/H_2$ is a trivial group, the graph of $\gamma$ coincides with $G_1/H_1 \times G_2/H_2$, and its preimage $H$ coincides with $G_1 \times G_2$.

Theorem 4.3. Let $K$ be a field of characteristic zero. Suppose that $f(x) \in K[x]$ is a polynomial of degree $n \geq 5$ without multiple roots. Let us consider the hyperelliptic curve $C_f : y^2 = f(x)$ and its jacobian $J(C_f)$. Suppose that $h(x) \in K[x]$ is an irreducible cubic polynomial and let us consider the elliptic curve $Y : y^2 = h(x)$.

Let us assume that $f(x)$ and $h(x)$ enjoy the following properties:
(1) \( \text{Gal}(K(\mathfrak{R}_f)/K) = \text{PSL}_2(\mathbb{F}_q) \) for some odd prime \( q \equiv 3 \mod 8 \) with \( n = q + 1 \), and \( \text{Gal}(K(\mathfrak{R}_f)/K) \) acts doubly transitively on \( \mathfrak{R}_f \) (where \( \mathfrak{R}_f \) is identified with the projective line \( \mathbb{P}^1(\mathbb{F}_q) \));

(2) \( \text{Gal}(K(\mathfrak{R}_h)/K) = S_3 \).

Then \( \text{Hom}(J(C_f), Y) = 0 \) and \( \text{Hom}(Y, J(C_f)) = 0 \). In particular, \( J(C_f) \) is not \( K_a \)-isogenous to a self-product of \( Y \).

Proof. First, we prove that \( K(\mathfrak{R}_f) \) and \( K(\mathfrak{R}_h) \) are linearly disjoint over \( K \). Let us put \( G_1 := \text{Gal}(K(\mathfrak{R}_f)/K) \), \( G_2 := \text{Gal}(K(\mathfrak{R}_h)/K) \), and \( H := \text{Gal}(K(\mathfrak{R}_f, \mathfrak{R}_h)/K) \), the Galois group of the compositum of \( K(\mathfrak{R}_f) \) and \( K(\mathfrak{R}_h) \) over \( K \). By Theorem 1.14 of [16], \( H \) can be considered to be a subgroup of \( G_1 \times G_2 \), where the Galois restriction maps coincide with restrictions of projection maps \( p_i : G_1 \times G_2 \to G_i \), with \( i = 1, 2 \), to \( H \). It follows from Example 4.2 that \( H \cong G_1 \times G_2 \), and \( K(\mathfrak{R}_f) \) and \( K(\mathfrak{R}_h) \) are linearly disjoint over \( K \). The equalities \( \text{Hom}(J(C_f), Y) = 0 \) and \( \text{Hom}(Y, J(C_f)) = 0 \) follow from the definitions (s) and (p3) and Theorem 2.5 of [36]. Since for any positive integer \( r \) we have \( \text{Hom}(J(C_f), Y^r) = \prod_{i=1}^r \text{Hom}(J(C_f), Y) \), we conclude that \( \text{Hom}(J(C_f), Y^r) = 0 \). \( \square \)

The following assertion will be proven in Section 5.

**Theorem 4.4.** Let \( p > 3 \) be a prime such that \( p \equiv 3 \mod 8 \). Let us put \( \omega = \frac{-1 + \sqrt{-p}}{2} \) and let \( \mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega \) be the ring of integers in \( \mathbb{Q}(\sqrt{-p}) \). Let \( \mathcal{O}_2 = \mathbb{Z} + 2\mathcal{O} \) be the order of conductor 2 in \( \mathbb{Q}(\sqrt{-p}) \).

(i) The principal ideal (2) is prime in \( \mathcal{O} \).

(ii) Let \( b \) be a proper fractional \( \mathcal{O}_2 \)-ideal in \( \mathbb{Q}(\sqrt{-p}) \) and \( a = \mathcal{O}b \) be the \( \mathcal{O} \)-ideal generated by \( b \). Then \( b \) contains \( 2a \) as a subgroup of index 2 and \( a \) contains \( b \) as a subgroup of index 2.

(iii) Let \( a \) be a fractional \( \mathcal{O} \)-ideal in \( \mathbb{Q}(\sqrt{-p}) \). If \( b \) is a subgroup of index 2 in \( a \) then it is a proper \( \mathcal{O}_2 \)-ideal in \( \mathbb{Q}(\sqrt{-p}) \), i.e.,

\[ \mathcal{O}_2 = \{ z \in \mathbb{Q}(\sqrt{-p}) \mid zb \subset b \} \]

in addition, \( a = \mathcal{O}b \). There are exactly three index 2 subgroups in \( a \); they are mutually non-isomorphic as \( \mathcal{O}_2 \)-ideals.

(iv) If \( h \) is the class number of \( \mathbb{Q}(\sqrt{-p}) \) then \( 3h \) is the number of classes of proper \( \mathcal{O}_2 \)-ideals.

We write \( j \) for the classical modular function [17, Ch. 3, Sect. 3].

**Corollary 4.5.** Let \( p \) be a prime such that \( p \equiv 3 \mod 8 \). Let \( q \geq 11 \) be an odd power of \( p \). (In particular, \( q \equiv p \equiv 3 \mod 8 \).) Let us put

\[ \omega := \frac{-1 + \sqrt{-p}}{2}, \ \alpha := j(\omega) \in \mathbb{C}, \ K := \mathbb{Q}(j(\omega)) \subset \mathbb{C}. \]

Suppose that \( f(x) \in K[x] \) is an irreducible polynomial of degree \( q + 1 \) such that \( \text{Gal}(f/K) = \text{PSL}_2(\mathbb{F}_q) \) acts doubly transitively on \( \mathfrak{R}_f \) (where \( \mathfrak{R}_f \) is identified with the projective line \( \mathbb{P}^1(\mathbb{F}_q) \)).

Then \( J(C_f) \) is an absolutely simple abelian variety, and \( \text{End}^0(J(C_f)) = \mathbb{Q} \) or a quadratic field.
Theorem 4.8. Let \( p \) be a prime such that \( p \equiv 3 \mod 8 \). Let \( q \geq 11 \) be an odd power of \( p \). (In particular, \( q \equiv p \equiv 3 \mod 8 \).) Suppose that \( f(x) \in \mathbb{Q}[x] \) is an irreducible polynomial of degree \( q + 1 \) such that \( \text{Gal}(f/\mathbb{Q}) = \text{PSL}_2(\mathbb{F}_q) \) acts doubly transitively on \( \mathcal{R}_f \) (where \( \mathcal{R}_f \) is identified with the projective line \( \mathbb{P}^1(\mathbb{F}_q) \)).

Then \( J(C_f) \) is an absolutely simple abelian variety, and \( \text{End}^0(J(C_f)) = \mathbb{Q} \) or a quadratic field.
Proof. Let us put
\[ \omega := \frac{-1 + \sqrt{-p}}{2}, \quad \alpha := j(\omega) \in \mathbb{C}, \quad K := \mathbb{Q}(j(\omega)) \subset \mathbb{C}. \]
Since simple non-abelian \( \text{PSL}_2(\mathbb{F}_q) \) does not have a subgroup of index 2,
\[ \text{Gal}(f/\mathbb{Q}) = \text{PSL}_2(\mathbb{F}_q) = \text{Gal}(f/\mathbb{Q}(\sqrt{-p})). \]
Since \( \text{PSL}_2(\mathbb{F}_q) \) is perfect and \( K\mathbb{Q}(\sqrt{-p}) = \mathbb{Q}(\sqrt{-p})(j(\omega)) \) is abelian over \( \mathbb{Q}(\sqrt{-p}) \),
\[ \text{Gal}(f/\mathbb{Q}) = \text{PSL}_2(\mathbb{F}_q) = \text{Gal}(f/K\mathbb{Q}(\sqrt{-p})). \]
Since \( \text{Gal}(f/K\mathbb{Q}(\sqrt{-p})) \subset \text{Gal}(f/K) \subset \text{Gal}(f/\mathbb{Q}) \),
we conclude that
\[ \text{Gal}(f/K) = \text{Gal}(f/\mathbb{Q}) = \text{PSL}_2(\mathbb{F}_q) \]
aracts doubly transitively on \( \mathfrak{A}_f \). In order to finish the proof, one has only to apply Corollary 4.5. □

5. Proof of Theorem 4.4

There is a positive integer \( k \) such that \( p = 8k+3 \). It follows that \( \omega^2 + \omega + (2k+1) = 0 \). This implies that the 4-element algebra \( O/2O \) contains a subalgebra isomorphic to the finite field \( \mathbb{F}_4 \) and therefore coincides with \( \mathbb{F}_4 \). This means that (2) is prime in \( O \). So, this proves (i).

Suppose that \( b \) is a proper \( O_2 \)-ideal in \( \mathbb{Q}(\sqrt{-p}) \) and \( a := O_b \). Clearly, \( 2a \subset b \subset a \). Since \( a \) and \( 2a \) are \( O \)-ideals, \( b \) does coincide neither with \( a \) nor with \( 2a \). Since \( 2a \) has index 4 in \( a \), the group \( b \) has index 2 in \( a \) and \( 2a \) has index 2 in \( b \). This proves (ii).

Now, suppose that \( a \) is a fractional \( O \)-ideal in \( \mathbb{Q}(\sqrt{-p}) \) and a subgroup \( b \subset \mathbb{Q}(\sqrt{-p}) \) satisfies \( 2a \subset b \subset a \). If \( b \) is an \( O \)-ideal then the unique factorization of \( O \)-ideals and the fact that (2) is prime imply that either \( b = a \) or \( b = 2a \). So, if \( b \) has index 2 in \( a \), it is neither \( a \) nor \( 2a \) and therefore is not an \( O \)-ideal.

On the other hand, it is clear that \( O_b \subset a \) and \( 2O_b \subset 2a \subset b \) and therefore \( b \) is a proper \( O_2 \)-ideal. This proves the first assertion of (iii). We have \( b \subset O_b \subset Oa = a \) but \( b \neq O_b \). Since the index of \( b \) in \( a \) is 2, we conclude that \( O_b = a \). This proves the second assertion of (iii).

Since \( a \) is a free commutative group of rank 2, it contains exactly three subgroups of index 2. Let \( b_1 \) and \( b_2 \) be two distinct subgroups of index 2 in \( a \). We have
\[ O_{b_1} = a = O_{b_2}. \]
Suppose that \( b_1 \) and \( b_2 \) are isomorphic as \( O_2 \)-ideals. This means that there exists a non-zero \( \lambda \in \mathbb{Q}(\sqrt{-p}) \) such that \( \lambda b_1 = b_2 \). It follows that \( \lambda a = a \) and therefore \( \lambda \) is a unit in \( O \). Since \( p > 3 \), we have \( \lambda = \pm 1 \) and therefore \( b_2 = b_1 \). This proves the last assertion of (iii).

The assertion (iv) follows easily from (ii) and (iii). (It is also a special case of Exercise 11 in Sect. 7 of Ch. II in [2] and of Exercise 4.12 in Section 4.4 of [27]).
6. Examples

Example 6.1. Let $S$ be a transcendental over $\mathbb{Q}$, $T = 2^83^5/(11S^2 + 1)$, and put

$$f_{11,S}(x) := (x^3 - 66x - 108)^4$$

$$- 9T(11x^5 - 44x^4 - 1573x^3 + 1892x^2 + 57358x + 103763)$$

$$- 3T^2(x - 11).$$

According to Table 10 of the Appendix in [19], $\text{Gal}(f_{11,S}/\mathbb{Q}(S)) = \text{PSL}_2(\mathbb{F}_{11})$. It can be verified using MAGMA [3] that when $s = m/n$ for any nonzero integers $-5 \leq m, n \leq 5$, then $\text{Gal}(f_{11,s}/\mathbb{Q}) = \text{PSL}_2(\mathbb{F}_{11})$. Consider the hyperelliptic curve

$$C_{11,s} : y^2 = f_{11,s}(x)$$

over $\mathbb{Q}$ by any one of these $s$. By Theorem 4.8 the 5-dimensional abelian variety $J(C_{11,s})$ is absolutely simple. For example, if we put $s = 1$, then we obtain a hyperelliptic curve

$$C_{11,1} : y^2 = x^{12} - 264x^{10} - 1232x^9 + 26136x^8 + 243936x^7 - 580800x^6$$

$$- 16612992x^5 - 54104688x^4 + 310712512x^3 + 2391092352x^2$$

$$+ 4956865152x + 504489216$$

over $\mathbb{Q}$ with $J(C_{11,1})$ absolutely simple.

Example 6.2. If we define

$$f_{13,S}(x) := (x^2 + 36)(x^3 - x^2 + 35x - 27)^4$$

$$- 4T(7x^2 - 2x + 247)(x^2 + 39)^6/27$$

with $T = 1/(39S^2 + 1)$ then again [19] we have $\text{Gal}(f_{13,S}/\mathbb{Q}(S)) = \text{PSL}_2(\mathbb{F}_{13})$. Similarly, we checked using MAGMA that when $s = m/n$ for any nonzero integers $-5 \leq m, n \leq 5$, then $\text{Gal}(f_{13,s}/\mathbb{Q}) = \text{PSL}_2(\mathbb{F}_{13})$. If we define

$$C_{13,s} : y^2 = f_{13,s}(x)$$

over $\mathbb{Q}$, then by Theorem 2.8 the 6-dimensional abelian variety $J(C_{13,s})$ is absolutely simple. As an example, take $s = -1$ to get the hyperelliptic curve

$$C_{13,-1} : y^2 = 263/270x^{14} - 539/135x^{13} + 9451/54x^{12} - 10114/15x^{11}$$

$$+ 376363/30x^{10} - 45487x^9 + 891605/2x^8 - 1533844x^7$$

$$+ 15279043/2x^6 - 25943931x^5 + 391472991/10x^4$$

$$- 896502438/5x^3 - 780396201/2x^2 - 365687757/5x$$

$$- 31998670461/10$$

defined over $\mathbb{Q}$ with $J(C_{13,-1})$ absolutely simple.

See [18] for other examples of irreducible polynomials over $\mathbb{Q}(T)$ of degrees $n = p + 1$ with $p = 11, 13, 19, 29, 37$, whose Galois groups are isomorphic to $\text{PSL}_2(\mathbb{F}_p)$. These polynomials can be used in a manner similar to that of Examples 6.1 and 6.2, in order to construct examples of absolutely simple abelian varieties over $\mathbb{Q}$ of dimensions 5, 6, 9, 14, 18 respectively, whose endomorphism algebra is either $\mathbb{Q}$ or a quadratic field.
References

[1] B. J. Birch, *Weber’s Class Invariants*. Mathematika 16 (1969), 283–294.
[2] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Third Edition, Moscow, Nauka, 1985.
[3] W. Bosma, J. Cannon, C. Playoust, *The Magma Algebra System I: The User Language*. J. Symb. Comp. 24 (1997), 235–265; http://magma.maths.usyd.edu.au/magma/.
[4] A. Brumer, *The Rank of \( J_0(N) \)*. Astérisque 228 (1995), 41–68.
[5] N. Bourbaki, *Algèbre*, Chapitre VIII, Hermann, Paris, 1958.
[6] L. Dornhoff, Group Representation Theory, Part A. Marcel Dekker, Inc., New York, 1972.
[7] A. Elkin, *Hyperelliptic jacobians with real multiplication*. J. Number Theory 117 (2006), 53–86.
[8] W. Feit, J. Tits, *Projective representations of minimum degree of group extensions*. Canad. J. Math. 30 (1978), 1092–1102.
[9] W. Feit, *The computations of some Schur indices*. Israel J. Math. 46 (1983), 274–300.
[10] D. Gorenstein, *Finite Simple Groups*, An Introduction to their classification, Plenum Press, New York and London, 1982.
[11] K. Hashimoto, *On Brumer’s family of RM-curves of genus two*. Tohoku Math. J. 52 (2000), 475–488.
[12] B. Huppert, *Endliche Gruppen I*. Springer-Verlag, Berlin Heidelberg New York, 1967.
[13] G. Janusz, *Simple components of \( \mathbb{Q}[SL(2,q)] \)*. Commun. Algebra 1 (1974), 1–22.
[14] T. Katsura, *On the structure of singular abelian varieties*. Proc. Japan Acad. 51 (1975), no. 4, 224–228.
[15] P. B. Kleidman, M. W. Liebeck, *On a theorem of Feit and Tits*. Proc. Amer. Math. Soc. 107 (1989), 315–322.
[16] S. Lang, *Algebra*, rev. 3rd ed., Springer-Verlag, New York, 2002.
[17] S. Lang, *Elliptic functions*, 2nd edition, Springer-Verlag, New York, 1987.
[18] G. Malle, *Polynome mit Galoisgruppen \( PGL_2(p) \) und \( PSL_2(p) \) über \( \mathbb{Q}(t) \).* Commun. Algebra 21 (1993), 511–526.
[19] G. Malle, B. H. Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin, 1999.
[20] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*. Proc. London Math. Soc. (3) 41 (1980), 1–20.
[21] D. Mumford, *Abelian varieties*, 2nd edn, Oxford University Press, 1974.
[22] F. Oort, *Endomorphism algebras of abelian varieties*. In: Algebraic Geometry and Commutative Algebra in Honor of M. Nagata (Ed. H. Hijikata et al), Kinokuniya Cy, Tokyo 1988; Vol. II, pp. 469–502.
[23] B. Poonen, E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*. J. reine angew. Math. 488 (1997), 141–188.
[24] E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*. Math. Ann. 310 (1998), 447–471.
[25] C. Schoen, *Produkte Abelscher Varietäten und Moduln über Ordnungen*. J. Reine Angew. Math. 429 (1992), 115–123.
[26] J.-P. Serre, *Complex Multiplication*. In: Algebraic Number Theory (J. Cassels, A. Fröhlich, eds.), Chapter XIII, pp. 292–296. Academic Press, 1967.
[27] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.
[28] T. Shioda, N. Mitani, *Singular abelian surfaces and binary quadratic forms*. In: Classification of Algebraic and Compact Complex Manifolds, Springer Lect. Notes in Math. 412 (1974), 259–287.
[29] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*. J. Pure Appl. Algebra 77 (1992), 253–262.
[30] M. Suzuki, *Group theory*. I. Springer-Verlag, Berlin-New York, 1982.
[31] J. Wilson, *Explicit moduli for curves of genus 2 with real multiplication by \( \mathbb{Q}(\sqrt{5}) \)*. Acta Arith. 93 (2000), 121–138.
[32] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters 7 (2000), 123–132.
[33] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (eds. C. Faber, G. van der Geer and F. Oort). Progress in Math., vol. 195 (2001), Birkhäuser, pp. 473–490.
Yu. G. Zarhin, *Hyperelliptic Jacobians without Complex Multiplication, Doubly Transitive Permutation Groups and Projective Representations*. In: Algebraic Number Theory and Algebraic Geometry (Parshin Festschrift), Contemp. Math. **300** (2002), 195–210.

Yu. G. Zarhin, *Very simple 2-adic representations and hyperelliptic jacobians*. Moscow Math. J. **2** (2002), issue 2, 403-431.

Yu. G. Zarhin, *Homomorphisms of hyperelliptic Jacobians*. In: Number Theory, Algebra and Algebraic Geometry (Shafarevich Festschrift), Tr. Mat. Inst. Steklova **241** (2003), 90–104; Proc. Steklov Inst. Math. **241** 2003, 79–92.

Yu. G. Zarhin, *Non-supersingular hyperelliptic jacobians*. Bull. Soc. Math. France **132** (2004), 617–634

Yu. G. Zarhin, *Homomorphisms of abelian varieties*. In: Y. Aubry, G. Lachaud (ed.) Arithmetic, Geometry and Coding Theory (AGCT 2003), Séminaires et Congrès **11**, 189–215 (2005).

Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication and Steinberg representations in positive characteristic*, arXiv:math.NT/0301177.

Institute of Mathematics, Hebrew University of Jerusalem, Givat Ram, Jerusalem, 91904, Israel

E-mail address: arsen@math.huji.ac.il

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

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