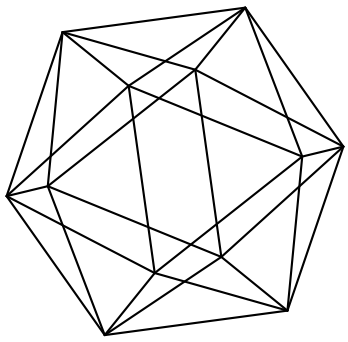
Max-Planck-Institut für Mathematik
Bonn

Non-isogenous elliptic curves and hyperelliptic jacobians II

by

Yuri G. Zarhin



Max-Planck-Institut für Mathematik
Preprint Series 2022 (29)

Date of submission: April 22, 2022

Non-isogenous elliptic curves and hyperelliptic jacobians II

by

Yuri G. Zarhin

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

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

MPIM 22-29

NON-ISOGENOUS ELLIPTIC CURVES AND HYPERELLIPTIC JACOBIANS II

YURI G. ZARHIN

To Yuri Ivanovich Manin on the occasion of his 85th birthday

ABSTRACT. Let K be a field of characteristic different from 2, $\bar{K}$ its algebraic closure. Let $n \ge 3$ be an odd integer. Let $f(x)$ and $h(x)$ be degree n polynomials with coefficients in K and without repeated roots. Let us consider genus $(n-1)/2$ hyperelliptic curves $C_f : y^2 = f(x)$ and $C_h : y^2 = h(x)$, and their jacobians $J(C_f)$ and $J(C_h)$, which are $(n-1)/2$-dimensional abelian varieties defined over K.

Suppose that one of the polynomials is irreducible and the other splits completely over K. We prove that if $J(C_f)$ and $J(C_h)$ are isogenous over $\bar{K}$ then there is an (odd) prime ℓ dividing n such that the endomorphism algebras of both $J(C_f)$ and $J(C_h)$ contain a subfield that is isomorphic to the field of ℓth roots of 1.

1. Definitions, notations, statements

This paper is a follow up of [15] and we use its notation. (See also [13, 14].) In particular, if $f(x) \in K[x]$ is a polynomial of odd degree $n = 2g + 1$ without repeated roots and with coefficients in a field K, and with $\mathrm{char}(K) \ne 2$, then we write C_f for the smooth projective model of the plane curve $y^2 = f(x)$ and $J(C_f)$ for its jacobian, which is a g-dimensional abelian variety over K. We fix an algebraic closure $\bar{K}$ of K and write $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ for the group of its K-linear automorpisms. We write $\mathfrak{R}_f \subset \bar{K}$ for the n-element set of roots of $f(x)$, $K(\mathfrak{R}_f)$ for the splitting field of $f(x)$ and $\mathrm{Gal}(f/K)$ for the Galois group

$$\mathrm{Gal}(K(\mathfrak{R}_f)/K) = \mathrm{Aut}(K(\mathfrak{R}_f)/K)$$

2010 *Mathematics Subject Classification.* 14H40, 14K05, 11G30, 11G10.

Key words and phrases. hyperelliptic curves, jacobians, isogenies of abelian varieties.

The author was partially supported by Simons Foundation Collaboration grant # 585711. This work was done during his stay in 2022 at the Max-Planck Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

of $f(x)$. As usual, one may view $\mathrm{Gal}(f/K)$ as the certain permutation subgroup of the group $\mathrm{Perm}(\mathfrak{R}_f)$ of all permutations of $\mathfrak{R}_f$.

Throughout this paper, $n \ge 3$ is an odd integer, $f(x)$ and $h(x)$ are degree n polynomials with coefficients in K and without repeated roots,

$$C_f : y^2 = f(x),\ C_h : y^2 = h(x)$$

are the corresponding genus $(n-1)/2$ hyperelliptic curves over K, whose jacobians we denote by $J(C_f)$ and $J(C_h)$, respectively. These jacobians are $(n-1)/2$-dimensional abelian varieties defined over K.

The main result of this paper is the following assertion.

Theorem 1.1. *Suppose that $n \ge 3$ is an odd prime. Let K be a field of characteristic different from 2. Let $f(x), h(x) \in K[x]$ be degree n polynomials without repeated roots. Suppose that one of the polynomials is irreducible and the other is reducible.*

If the corresponding hyperelliptic jacobians $J(C_f)$ and $J(C_h)$ are isogenous over $\bar{K}$ then they both are abelian varieties of CM type over $\bar{K}$ with multiplication by the nth cyclotomic field $\mathbb{Q}(\zeta_n)$.

Remark 1.2. Theorem 1.1 was proven in [15] under an additional assumption that 2 is a primitive root modulo n.

The next assertion may be viewed as a a partial generalization of Theorem 1.1 to the case of arbitrary odd n.

Theorem 1.3. *Suppose that $n \ge 3$ is an odd integer. Let K be a field of characteristic different from 2. Let $f(x), h(x) \in K[x]$ be degree n polynomials without repeated roots. Suppose that $f(x)$ is irreducible over K.*

Assume additionally that the order of the Galois group $\mathrm{Gal}(h/K)$ of $h(x)$ is prime to n. (E.g., each irreducible factor of $h(x)$ over K has degree 1 or 2.)

If the corresponding hyperelliptic jacobians $J(C_f)$ and $J(C_h)$ are isogenous over $\bar{K}$ then there is a prime divisor ℓ of n such that both endomorphism algebras $\mathrm{End}^0(J(C_f))$ and $\mathrm{End}^0(J(C_h))$ contain an invertible element of multiplicative order ℓ.

Remark 1.4. Assume that the conditions of Theorem 1.3 hold. Then $h(x)$ is reducible over K. Indeed, if $h(x)$ is irreducible then $\mathrm{Gal}(h/K)$ acts *transitively* on the n-element set $\mathcal{R}_h$ of roots of $h(x)$. Therefore its order $\#(\mathrm{Gal}(h/K))$ is divisible by n, which gives us a desired contradiction.

The paper is organized as follows. In Section 2 we remind basic facts about Galois properties of points of order 2 and 4 on abelian

varieties and hyperelliptic jacobians. We also state Theorem 2.2 that is a stronger (but a more technical) variant of Theorem 1.3. Section 3 contains the proof of Theorem 2.2. (Notice that Lemma 3.3 plays a crucial role in the proof and may be of certain independent interest.) We prove Theorem 1.1 in Section 4.

2. Points of order 2 and 4 on hyperelliptic jacobians

Let $K_s \subset \bar{K}$ be the separable algebraic closure of K. Let X be a positive-dimensional abelian variety over K. If d is a positive integer then we write $X[d]$ for the kernel of multiplication by d in $X(\bar{K})$. Recall ([7, Sect. 6], [4, Sect. 8, Remark 8.4]) that if d is *not* divisible by $\mathrm{char}(K)$ then is a $\mathrm{Gal}(K)$-submodule of $X(K_s)$; in addition, $X[d]$ is isomorphic as a commutative group to $(\mathbb{Z}/d\mathbb{Z})^{2\dim(X)}$.

Let $K(X[d])$ be the *field of definition* of all torsion points of order dividing d on X. It is well known [4, Remark 8.4]) that $K(X[d])$ lies in K_s and is a finite Galois extension of K. Let us put

$$\tilde{G}_{d,X} := \mathrm{Gal}(K(X[d])/K).$$

One may view $\tilde{G}_{d,X}$ as the certain subgroup of $\mathrm{Aut}_{\mathbb{Z}/d\mathbb{Z}}(X[d])$ and $X[d]$ as the faithful $\tilde{G}_{d,X}$-module. In addition, the structure of the $\mathrm{Gal}(K)$-module on $X[d]$ is induced by the canonical (continuous) *surjective* group homomorphism

$$\tilde{\rho}_{d,X} : \mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K(X[d])/K) = \tilde{G}_{d,X}.$$

For example, if $d = 2 \neq \mathrm{char}(K)$ then $X[2]$ is a $2\dim(X)$-dimensional vector space over the 2-element prime field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and the inclusion $\tilde{G}_{2,X} \subset \mathrm{Aut}_{\mathbb{F}_2}(X[2])$ defines a *faithful* linear representation of the group $\tilde{G}_{2,X}$ in the vector space $X[2]$ over $\mathbb{F}_2$.

Remark 2.1.

(i) Let $K(X[4])$ be the field of definition of all points of order dividing 4 on X. It is well known that $K(X[4])/K$ is a finite Galois field extension,

$$K \subset K(X[2]) \subset K(X[4]) \subset K_s$$

and the Galois group $\mathrm{Gal}(K(X[4])/K(X[2]))$ is a finite commutative group of exponent 2 or 1 (e.g., see [15, Remark 2.2(i)]).

(ii) Let $d \geq 3$ be an integer that is *not* divisible by $\mathrm{char}(K)$. By a result of A. Silverberg, [11, Th. 2.4] all the endomorphisms of X are defined over $K(X[d])$. (See [2, 9, 1] for further results concerning the field of definition of all endomorphisms of an abelian variety.)

The following assertion contains Theorem 1.3 as a special case (when $Y = J(C_h)$).

Theorem 2.2. *Let K a field with characteristic $\ne 2$. Let g be a positive unteger, $n := 2g+1$, and $f(x) \in K[x]$ a degree n irreducible polynomial without repeated roots. Let us put $X = J(C_f)$.*

Let Y be a g-dimensional abelian variety over K such that the order of $\tilde{G}_{2,Y}$ is prime to n. (E.g., $K(Y[2]) = K$.)

Suppose that X and Y are isogenous over $\bar{K}$.

Then there is an odd prime ℓ dividing n such that both endomorphism algebras $\mathrm{End}^0(X)$ and $\mathrm{End}^0(Y)$ contan an invertible element of multiplicative order ℓ.

In addition, if $n = 2g+1$ is a prime then both X and Y are abelian varieties of CM type over $\bar{K}$ with multiplication by the nth cyclotomic field $\mathbb{Q}(\zeta_n)$.

We will prove Theorem 2.2 in Section 3. Our proof is based on the Galois properties of points of order 2 on hyperelliptic jacobians that will be discussed in the next subsection.

2.1. **Galois properties.** In this subsection we recall a well known explicit description of the Galois module $J(C_f)[2]$ [5, 12] for arbitrary separable $f(x)$ and odd n. Let us start with the n-dimensional $\mathbb{F}_2$-vector space

$$\mathbb{F}_2^{\mathfrak{R}_f} = \{\phi : \mathfrak{R}_f \to \mathbb{F}_2\}$$

of all $\mathbb{F}_2$-valued functions on $\mathfrak{R}_f$. The action of $\mathrm{Perm}(\mathfrak{R}_f)$ on $\mathfrak{R}_f$ provides $\mathbb{F}_2^{\mathfrak{R}_f}$ with the structure of faithful $\mathrm{Perm}(\mathfrak{R}_f)$-module, which splits into a direct sum

$$\mathbb{F}_2^{\mathfrak{R}_f} = \mathbb{F}_2 \cdot \mathbf{1}_{\mathfrak{R}_f} \oplus Q_{\mathfrak{R}_f} \tag{1}$$

of the one-dimensional subspace $\mathbb{F}_2 \cdot \mathbf{1}_{\mathfrak{R}_f}$ of constant functions and the $(n-1)$-dimensional *heart* [3, 6]

$$Q_{\mathfrak{R}_f} := \{\phi : \mathfrak{R}_f \to \mathbb{F}_2 \mid \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = 0\}$$

(here we use that n is odd). Clearly, the $\mathrm{Perm}(\mathfrak{R}_f)$-module is faithful. It remains faithful if we view it as the $\mathrm{Gal}(f/K)$-module. There is a $\mathrm{Perm}(\mathfrak{R}_f)$-invariant $\mathbb{F}_2$-bilinear pairing

$$\Psi : \mathbb{F}_2^{\mathfrak{R}_f} \times \mathbb{F}_2^{\mathfrak{R}_f} \to \mathbb{F}_2,\ \phi, \psi \mapsto \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha)\psi(\alpha)$$

and the splitting (1) is an orthogonal (with respect to Ψ) direct sum. Clearly, the restriction of Ψ to $\mathbb{F}_2 \cdot \mathbf{1}_{\mathfrak{R}_f}$ is nondegenerate and therefore the restriction of Ψ to $Q_{\mathfrak{R}_f}$ is nondegenerate as well. This implies that

the $\mathrm{Gal}(f/K)$-modules $Q_{\mathfrak{R}_f}$ and its *dual* $\mathrm{Hom}_{\mathbb{F}_2}(Q_{\mathfrak{R}_f}, \mathbb{F}_2)$ are *isomorphic*.

The field inclusion $K(\mathfrak{R}_f) \subset K_s$ induces the *surjective* continuous homomorphism

$$\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K) \twoheadrightarrow \mathrm{Gal}(K(\mathfrak{R}_f)/K) = \mathrm{Gal}(f/K),$$

which gives rise to the natural structure of the $\mathrm{Gal}(K)$-module on $Q_{\mathfrak{R}_f}$ such that the image of $\mathrm{Gal}(K)$ in $\mathrm{Aut}_{\mathbb{F}_2}(Q_{\mathfrak{R}_f})$ coincides with

$$\mathrm{Gal}(f/K) \subset \mathrm{Perm}(\mathfrak{R}_f) \hookrightarrow \mathrm{Aut}_{\mathbb{F}_2}(Q_{\mathfrak{R}_f}).$$

This implies that the *Galois modules* $Q_{\mathfrak{R}_f}$ *and* $\mathrm{Hom}_{\mathbb{F}_2}(Q_{\mathfrak{R}_f}, \mathbb{F}_2)$ *are isomorphic*.

It is well known (see, e.g., [5, 12]) that the $\mathrm{Gal}(K)$-module $J(C_f)[2]$ and $Q_{\mathfrak{R}_f}$ are canonically isomorphic. This implies that the groups $\tilde{G}_{2,J(C_f)}$ and $\mathrm{Gal}(f)$ are canonically isomorphic. It is also clear that $K(\mathfrak{R}_f)$ coincides with $K(J(C_f)[2])$. We will need the following assertion.

Lemma 2.3. *Suppose that $f(x)$ is irreducible over K. Then:*

(i) *$Q_{\mathfrak{R}_f}$ does not contain nonzero Galois-invariants.*
(ii) *Every Galois-invariant linear functional $Q_{\mathfrak{R}_f} \to \mathbb{F}_2$ is zero.*
(iii) *Let W be a $\mathbb{F}_2$-vector space provided with the trivial action of $\mathrm{Gal}(K)$. Then every homomorphism of the Galois modules $Q_{\mathfrak{R}_f} \to W$ is zero and every homomorphism of the Galois modules $J(C_f)[2] \to W$ is zero as well.*

Proof. Recall that the irreducibility means that the Galois group acts transitively on $\mathfrak{R}_f$. Let $\phi \in Q_{\mathfrak{R}_f}$ be a Galois-invariant function on $\mathfrak{R}_f$. The transitivity implies that ϕ is constant. If ϕ is not (identically) zero then $\phi(\alpha) = 1$ for all $\alpha \in \mathfrak{R}_f$ and therefore (since $\phi \in Q_{\mathfrak{R}_f}$)

$$0 = \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = n \cdot 1 = 1 \in \mathbb{F}_2,$$

i.e., $0 = 1$, which is absurd. The obtained contradiction proves that $\phi \equiv 0$. In order to prove the second assertion of Lemma, recall that the Galois modules $Q_{\mathfrak{R}_f}$ and $\mathrm{Hom}_{\mathbb{F}_2}(Q_{\mathfrak{R}_f}, \mathbb{F}_2)$ are isomorphic. Now the second assertion of our Lemma follows from the already proven first one. On the other hand, the third assertion is an immmediate corollary of the second one: one has only to choose a basis of W and recall that the Galois modules $Q_{\mathfrak{R}_f}$ and $J(C_f)[2]$ are isomorphic. □

3. Isogenous hyperelliptic jacobians

We will deduce Theorem 2.2 from the following auxiliary statements.

Lemma 3.1. *Let G be a transitive permutation group of a finite nonempty set $\mathfrak{R}$, and H a normal subgroup of G. Then the number of H-orbits in $\mathfrak{R}$ divides both $\#(\mathfrak{R})$ and the index $(G:H)$. In particular, if $\#(\mathfrak{R})$ and $(G:H)$ are relatively prime then H acts transitively on $\mathfrak{R}$.*

Lemma 3.2. *Let $f(x)$ be a degree n irreducible polynomial over a field K and without repeated roots. Let K_1/K be a finite Galois extension of fields, whose degree is prime to n. Then $f(x)$ remains irreducible over K. In particular, the order of Galois group $\mathrm{Gal}(f/K_1)$ is divisible by n.*

Lemma 3.3. *Suppose that $K = K(Y[4])$. Then there is a nontrivial group homomorphism*

$$\chi : \mathrm{Gal}(K(X[4])/K) \to \mathrm{End}^0(Y)^*,$$

whose image

$$\Gamma := \mathrm{Im}(\chi) \subset \mathrm{End}^0(Y)^*$$

is a finite group that enjoys the following property.

The integers n and $\#(\Gamma)$ are not relatively prime. In other words, there is an odd prime ℓ that divides both n and $\#(\Gamma)$.

Proof of Theorem 2.2 (modulo Lemmas 3.2 and 3.3). The degree

$$[K(Y[4] : K] = [K(Y[4]) : K(Y[2])] \cdot [K(Y[2]) : K].$$

We know that $[K(Y[2]) : K] = \#(\tilde{G}_{2,Y})$ is prime to n. Thanks to Remark 2.1(i), $[K(Y[4]) : K(Y[2])]$ is either 1 or a power of 2. This implies that the product $[K(Y[4]) : K]$ is also prime to the odd integer n. In light of Lemma 3.2, $f(x)$ remains irreducible over the field $K_1 = K(Y[4])$. Replacing K by K_1, we may assume that $K = K(Y[4])$.

By Lemma 3.3, there is a nontrivial finite subgroup $\Gamma \subset \mathrm{End}^0(Y)^*$, whose order is divisible by a certain prime divisor ℓ of n. Then H contains an element of order ℓ that is an invertible element u in $\mathrm{End}^0(Y)$ of multiplicative order ℓ. Hence, the $\mathbb{Q}$-subalgebra $\mathbb{Q}[u]$ of $\mathrm{End}^0(Y)$ generated by u is isomorphic to a quotient of the direct sum $\mathbb{Q} \oplus \mathbb{Q}(\zeta_\ell)$. Since ℓ is odd, $\mathbb{Q}[u]$ is isomorphic either to $\mathbb{Q}(\zeta_\ell)$ or to $\mathbb{Q} \oplus \mathbb{Q}(\zeta_\ell)$.

If n is a prime then $\ell = n = 2g+1$ and the same arguments as in [15, Sect. 4, proof of Prop. 2.4] (based on [10, Ch. II, Prop. 1]) show that the $\mathbb{Q}$-subalgebra $\mathbb{Q}[u]$ of $\mathrm{End}^0(Y)$ is isomorphic to $\mathbb{Q}(\zeta_n)$ and therefore Y (and also X) is an abelian variety of CM type with multiplication by $\mathbb{Q}(\zeta_n)$.

□

Proof of Lemma 3.1. Let us put

$$n = \#(\mathfrak{R}),\ h = (G : H).$$

Since G acts transitively on the n-element set $\mathfrak{R}$, all the orbits of normal H have the same cardinality, say, r [8, Prop. 4.4 on p. 22]. This implies that m=n/r is the *number of H-orbits* in $\mathfrak{R}$. In particular, both m and r divide n.

Let B be an r-element orbit of H in $\mathfrak{R}$. Then B is a *subset of imprimitivity* for G [8, Proof of Prop. 4.4 on p. 22]. Let O be the the m-element set of H-orbits in $\mathfrak{R}$. Now the transitivity of the action of G on $\mathfrak{R}$ and the normality of H implies that G acts transitively on O and this action factors through the *transitive* action of the *quotient* G/H on O. This implies that $m = \#(O)$ divides $\#(G/H) = (G : H) = h$. So, m divides both n and h, which ends the proof. □

Proof of Lemma 3.2. Since K_1/K is Galois, the group $\mathrm{Gal}(f/K_1)$ is a *normal* subgroup of $\mathrm{Gal}(f/K)$, whose index h divides $[K_1 : K]$ and therefore is also prime to n. It follows from Lemma 3.1 applied to

$$\mathfrak{R} = \mathfrak{R}_f,\ G = \mathrm{Gal}(f/K),\ H = \mathrm{Gal}(f/K_1)$$

that $\mathrm{Gal}(f/K_1)$ acts transitively on $\mathfrak{R}_f$, i.e., $f(x)$ is irreducible over K_1. □

Proof of Lemma 3.3. In light of the theorem of Silverberg (Remark 2.1(ii)), all endomorphisms of Y are defined over K. Applying the theorem of Silverberg (see Remark 2.1(ii) above) to $X \times Y$, we conclude that all the homomorphisms from X to Y are defined over $K(X[4])$.

Let $\mu : X \to Y$ be an isogeny. Dividing, if necessary, μ by a suitable power of 2, we may and will assume that

$$\mu(X[2]) \neq \{0\}. \tag{2}$$

Let us put

$$G_4 := \mathrm{Gal}(K(X[4])/K),\ G = \mathrm{Gal}(K(X[2])/K) = \mathrm{Gal}(f/K).$$

We know that μ is defined over $K(X[4])$. This allows us to define for each $\sigma \in G_4$ the isogeny $\sigma(\mu) : X \to Y$, which is the Galois-conjugate of μ (recall that both X and Y are defined over K). Then the same construction as in [15, Sect. 4, proof of Prop. 2.4] allows us to define a map

$$c : G_4 \to \mathrm{End}^0(Y)^*,\ \sigma \mapsto c(\sigma)$$

where $c(\sigma)$ is determined by

$$\sigma(\mu) = c(\sigma)\mu\ \forall \sigma \in G_4 = \mathrm{Gal}(K(X[4])/K).$$

We have for each $\sigma, \tau \in G_4$

$$c(\sigma\tau)\mu = \sigma\tau(\mu)) = \sigma(\tau(\mu)) = \sigma(c(\tau)\mu)) = c(\tau)\sigma(\mu) = c(\tau)c(\sigma)\mu$$

(here we use that all elements of $\mathrm{End}(Y)$ are defined over K, i.e., are G-invariant) and therefore

$$c(\sigma\tau) = c(\tau)c(\sigma)\ \forall \sigma, \tau \in G = \mathrm{Gal}(K(X[4])/K).$$

This means that the map

$$\chi : G_4 = \mathrm{Gal}(K(X[4])/K) \to \mathrm{End}^0(Y)^*,\ \sigma \mapsto \chi(\sigma) = c(\sigma)^{-1}$$

is a *group homomorphism*. Let $\Gamma \subset \mathrm{End}^0(Y)^*$ be the image of χ, which is a finite subgroup of $\mathrm{End}^0(Y)^*$. We need to check that there is a prime divisor ℓ of n that divides $\#(\Gamma)$.

Let H_4 be the kernel of χ, i.e.,

$$H_4 = \{\sigma \in G_4 \mid \sigma(\mu) = \mu\}. \tag{3}$$

By definition, H_4 is a normal subgroup of G_4. Let H be the image of H_4 under the *surjective* group homomorphism

$$G_4 = \mathrm{Gal}(K(X[4])/K) \twoheadrightarrow \mathrm{Gal}(K(X[2])/K) = \mathrm{Gal}(f/K) = G.$$

The surjectiveness implies that H is a normal subgroup of G and the index $(G : H)$ divides

$$(G_4 : H_4) = \#(\Gamma).$$

In order to finish the proof, we need the following assertion that will be proven at the end of this section.

Proposition 3.4. *The subgroup H of G is not transitive on $\mathfrak{R}_f$.*

End of Proof of Lemma 3.3 (modulo Proposition 3.4) Combining Proposition 3.4 with Lemma 3.1, we conclude that $(G : H)$ is *not* prime to n. Hence, there is a prime ℓ that divides both $(G : H)$ and n (recall that n is odd). Since $(G : H)$ divides $(G_4 : H_4)$, we conclude thast ℓ divides $(G_4 : H_4) = \#(\Gamma)$, which ends the proof.

□

Proof of Proposition 3.4. Suppose that H is transitive. Then $f(x)$ remains *irreducible* over the (sub)field $K(X[4])^H$ of H-invariants. Replacing K by its overfield $K(X[4])^{H_4}$, we may and will assume that

$$H_4 = \mathrm{Gal}(K(X[4])/K),\ H = \mathrm{Gal}(K(X[2])/K) = \mathrm{Gal}(f/K).$$

In particular,

$$\sigma(\mu) = \mu\ \forall \sigma \in H = \mathrm{Gal}(K(X[4])/K). \tag{4}$$

Combining (2) with (4), we obtain that μ induces a *nonzero* homomorphism of Galois modules

$$X[2] \to Y[2].$$

Notice that the Galois module $Y[2]$ is *trivial*, because

$$K \subset K(Y[2]) \subset K(Y[4]) = K,$$

i.e., $K[Y[2]) = K$. On the other hand, the irreducibility of $f(x)$ over K implies (thanks to Lemma 2.3(iii)) that every homomorphism of the Galois module $X[2]$ to the trivial Galois module $Y[2]$ is zero. The obtained contradiction proves that H is not transitive. □

4. Proof of Theorem 1.1

So, n is an odd prime, both $f(x)$ and $h(x) \in K[x]$ are degree n polynomials without repeated roots, $f(x)$ is irreducible and $h(x)$ is reducible. Since n is a prime, the reducibility of $h(x)$ implies that the order of $\mathrm{Gal}(h/K)$ is prime to n (see [15, Lemma 2.6]). This implies that if we put $Y = J(C_h)$ then the group $\tilde{G}_{2,Y} = \mathrm{Gal}(h/K)$ has order that is prime to n. Now the desired result follows readily from Theorem 2.2.

References

[1] P. Goodman, *Restrictions on endomorphism rings of jacobians and their minimal fields of definition*. Trans. Amer. Math. Soc. **374** (2021), 4639–4654.

[2] R. Guralnick and K.S. Kedlaya, *Endomorphism fields of abelian varieties*. Research in Number Theory **3** (2017), Paper No. 22, 10.

[3] M. Klemm, *Über die Reduktion von Permutationsmoduln*. Math. Z. **143** (1975), 113–117.

[4] J.S. Milne, *Abelian varieties*, p. 103–150. In: Arithmetic Geometry (G. Cornell, J.H. Silverman, eds.), Springer-Verlag, New York, 1986.

[5] Sh. Mori, *The endomorphism rings of some abelian varieties*. II, Japanese J. Math, **3** (1977), 105–109.

[6] B. Mortimer, The modular permutation representations of the known doubly transitive groups. *Proc. London Math. Soc.* (3) **41** (1980), 1–20.

[7] D. Mumford, Abelian varieties, Second edition, Oxford University Press, London, 1974.

[8] D.S. Passman, Permutation Groups. W.A. Benjamin, Inc., New York Amsterdam, 1968.

[9] G. Rémond, *Degré de définition des endomorphisms d'une variété abélienne*. J. European Math. Soc. **22** (2020), 3059–3099.

[10] G. Shimura, Abelian varieties with complex multiplication and modular functions. Princeton University Press, Princeton, NJ, 1998.

[11] A. Silverberg, *Fields of definitions for homomorphisms of abelian varieties*. J. Pure Applied Algebra **77** (1992), 253–262.

[12] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (C. Faber, G. van der Geer, F. Oort, eds.), pp. 473–490, Progress in Math., Vol. **195**, Birkhäuser, Basel–Boston–Berlin, 2001.
[13] Yu. G. Zarhin, *Homomorphisms of hyperelliptic jacobians*. Trudy Math. Inst. Steklova **241** (2003), 79–92; Proc. Steklov Institute of Mathematics **241** (2003), 90–104.
[14] Yu. G. Zarhin, *Non-isogenous superelliptic jacobians*. Math. Z. **253** (2006), 537–554.
[15] Yu. G. Zarhin, *Non-isogenous elliptic curves and hyperelliptic jacobians*. Math. Research Letters, to appear; arXiv:2105.03783 [math.NT].

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
Email address: zarhin@math.psu.edu