Math. Res. Lett.
Volume 30, Number 1, 267–294, 2023

Non-isogenous elliptic curves and hyperelliptic jacobians

Yuri G. Zarhin

To the memory of Yuri Ivanovich Manin

Let K be a field of characteristic different from 2, $\bar{K}$ its algebraic closure. Let $n \geq 3$ be an odd prime such that 2 is a primitive root modulo n. 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 reducible. We prove that if $J(C_f)$ and $J(C_h)$ are isogenous over $\bar{K}$ then both jacobians are abelian varieties of CM type with multiplication by the field of nth roots of 1.

We also discuss the case when both polynomials are irreducible while their splitting fields are linearly disjoint. In particular, we prove that if $\mathrm{char}(K) = 0$, the Galois group of one of the polynomials is doubly transitive and the Galois group of the other is a cyclic group of order n, then $J(C_f)$ and $J(C_h)$ are not isogenous over $\bar{K}$.

1. Definitions, notations, statements

Let K be a field, $\bar{K}$ its algebraic closure, and $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ the group of all automorpisms of the field extension $\bar{K}/K$. If $K_s \subset \bar{K}$ is the separable closure of K in $\bar{K}$ then $\mathrm{Gal}(K)$ coincides with the Galois group of the (possibly infinite) Galois extension K_s/K.

If X is an abelian variety over K then we write $\mathrm{End}(X)$ for the ring of its $\bar{K}$-endomorphisms and $\mathrm{End}^0(X)$ for the corresponding $\mathbb{Q}$-algebra $\mathrm{End}(X) \otimes \mathbb{Q}$. If Y is (may be another) abelian variety over K then we write $\mathrm{Hom}(X, Y)$ for the group of all $\bar{K}$-homomorphisms from X to Y, which is a free commutative group of finite rank. It is well known that $\mathrm{Hom}(X, Y) = 0$ if and only if $\mathrm{Hom}(Y, X) = 0$.

Let $f(x) \in K[x]$ be a nonconstant polynomial of degree n without repeated roots. We write $\mathfrak{R}_f \subset \bar{K}$ for the set of its roots, and $K(\mathfrak{R}_f) \subset \bar{K}$ for the splitting field of $f(x)$. Then $\mathfrak{R}_f$ consists of n elements and

$$\mathfrak{R}_f \subset K(\mathfrak{R}_f) \subset K_s \subset \bar{K}.$$

We write

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

for the Galois group of $f(x)$ over K. The group $\mathrm{Gal}(f/K)$ permutes elements of $\mathfrak{R}_f$ and therefore can be identified with a certain subgroup of the group $\mathrm{Perm}(\mathfrak{R}_f)$ of all permutations of $\mathfrak{R}_f$. (The action of $\mathrm{Gal}(f/K)$ on $\mathfrak{R}_f$ is *transitive* if and only if $f(x)$ is *irreducible* over K.) If we choose an order on the n-element set $\mathfrak{R}_f$ then we get a group isomorphism between $\mathrm{Perm}(\mathfrak{R}_f)$ and the full symmetric group $\mathbf{S}_n$, which makes $\mathrm{Gal}(f/K)$ a certain subgroup of $\mathbf{S}_n$. We write $\mathrm{Alt}(\mathfrak{R}_f)$ for the only index 2 subgroup of $\mathrm{Perm}(\mathfrak{R}_f)$, which corresponds to the alternating (sub)group $\mathbf{A}_n$ of $\mathbf{S}_n$ under any isomorphism between $\mathrm{Perm}(\mathfrak{R}_f)$ and $\mathbf{S}_n$. Slightly abusing notation, we say that $\mathrm{Gal}(f)$ is $\mathbf{S}_n$ (resp. $\mathbf{A}_n$) if it coincides with $\mathrm{Perm}(\mathfrak{R}_f)$ (resp. $\mathrm{Alt}(\mathfrak{R}_f)$).

Throughout the paper (unless otherwise stated) we assume that $\mathrm{char}(K) \neq 2$.

1.1. Elliptic curves

Let us assume that $n = 3$ (i.e., $f(x)$ is a cubic polynomial) and consider the elliptic curve

$$C_f : y^2 = f(x)$$

viewed as a one-dimensional abelian variety defined over K with the infinite point taken as the zero of group law. As usual, $j(C_f) \in K$ denotes the *j-invariant* of the elliptic curve C_f.

Let $h(x) \in K[x]$ be another cubic polynomial without repeated roots and

$$C_h : y^2 = h(x)$$

be the corresponding elliptic curve (one-dimensional abelian variety) over K. It is well known that $j(C_f) = j(C_h)$ if and only if the elliptic curves C_f and C_h are isomorphic over $\bar{K}$ [27, Chapter III, Prop. 1.4b].

The aim of this paper is to discuss when C_f and C_h are *not* isogenous over $\bar{K}$. There are several known criteria for elliptic curves over number fields not

to be isogenous that are based on their arithmetic properties (reductions, arithmetic properties of the corresponding j-invariants) [11, p. 645]. See also [32, Th. 1.2] and [34, Sect. 2]. There are also recent results describing the "asymptotic behavior" of the number of elliptic curves with j-invariant in certain countable sets of complex numbers (e.g., the set $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers) that are not isogenous to elliptic curves whose j-invariants lie on a given real algebraic curve in $\mathbb{C} = \mathbb{R}^2$ [11, Th. 1.7 and Sect. 3]).

Here we discuss criteria that use the properties of $f(x)$ and $h(x)$ over arbitrary K only. Our main results are the following two assertions.

Theorem 1.1. *Let K be a field of characteristic different from 2. Let $f(x)$ and $h(x)$ be cubic polynomials over K without repeated roots. Suppose that exactly one of the two polynomials is irreducible.*

Let us assume that C_f and C_h are isogenous over $\bar{K}$. Then:

(i) *Both $\mathbb{Q}$-algebras $\mathrm{End}^0(C_f)$ and $\mathrm{End}^0(C_h)$ contain a subfield isomorphic to $\mathbb{Q}(\sqrt{-3})$.*

(ii) *If $\mathrm{char}(K) = 0$ then both C_f and C_h are isogenous over $\bar{K}$ to the elliptic curve $y^2 = x^3 - 1$.*

Theorem 1.2. *Let K be a field of characteristic different from 2. Let $f(x), h(x) \in K[x]$ be cubic polynomials without repeated roots that enjoy the following properties.*

(i) *The splitting fields of $f(x)$ and $h(x)$ are linearly disjoint over K.*

(ii) *$h(x)$ is irreducible over K.*

(iii) *$\mathrm{Gal}(f/K) = \mathbf{S}_3$, i.e., $K(\mathfrak{R}_f)$ has degree 6 over K.*

If C_f and C_h are isogenous over $\bar{K}$ then $p = \mathrm{char}(K)$ is a prime that is not congruent to 1 modulo 3, and both C_f and C_h are supersingular elliptic curves.

Remark 1.3. If $\mathrm{char}(K) = 0$ then it follows from Theorem 1.2 that if cubic polynomials $f(x)$ and $h(x)$ enjoy properties (i), (ii), (iii) of Theorem 1.2 then C_f and C_h are not isogenous over $\bar{K}$. This assertion is a special case (with $m = n = 3$) of [32, Th. 1.2].

Example 1.4. Let $K = \mathbb{Q}$, $f(x) = x^3 - 5$, $h(x) = x^3 - 15x + 22$. Clearly, $K(\mathfrak{R}_f) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{5})$ is a sextic number field, i.e. $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$, and $h(x) = (x-2)(x^2+2x-11)$ is reducible over $\mathbb{Q}$. So, $f(x)$ and $h(x)$ satisfy the conditions of Theorem 1.1. It is well known that the endomorphism

ring $\mathrm{End}(C_f)$ is $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$. It is also known [28, Appendix A, p. 483] that $\mathrm{End}(C_h)$ is

$$\mathbb{Z} + 2 \cdot \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] = \mathbb{Z}\left[\sqrt{-3}\right].$$

Anyway, both C_f and C_h are CM elliptic curves whose endomorphism algebras (over an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$) are isomorphic to $\mathbb{Q}(\sqrt{-3})$. Hence, C_f and C_h are isogenous to each other over $\bar{\mathbb{Q}}$ and to $y^2 = x^3 - 1$. (Actually, C_f is even isomorphic to $y^2 = x^3 - 1$ over $\bar{\mathbb{Q}}$).

Remark 1.5. Let $\tilde{K}$ be an overfield of K_s. If X and Y are abelian varieties over K then, by a theorem of Chow ([9, Ch. 2, Th. 5], [3, Th. 3.19]), all their $\tilde{K}$-homomorphisms (and $\tilde{K}$-endomorphisms) are defined over K_s. In particular, X and Y are isogenous over $\tilde{K}$ if and only if they are isogenous over K.

Corollary 1.6. *Let $K = \mathbb{Q}$. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic polynomial and $h(x) \in \mathbb{Q}[x]$ a reducible cubic polynomial.*

Then precisely one of the following two conditions holds.

(i) *The elliptic curves C_f and C_h are not isogenous over $\bar{\mathbb{Q}}$ (and even over $\mathbb{C}$).*

(ii) *Both $j(C_f)$ and $j(C_h)$ lie in a 3-element set*

$$S = \{0,\ 2^4 3^3 5^3,\ -2^{15} 3 \cdot 5^3\} \subset \mathbb{Q}.$$

Proof of Corollary 1.6 (modulo Theorem 1.1). Let us consider an elliptic curve C that is defined over $\mathbb{Q}$. Then $\mathrm{End}^0(C)$ contains $\mathbb{Q}(\sqrt{-3})$ (actually coincides with it) if and only if the j-invariant of C lies in S ([22, Sect. 2, p. 295], [28, Appendix A, Sect. 3]). Now the desired result follows from Theorem 1.1 combined with Remark 1.5. □

Corollary 1.7. *Let k be an algebraically closed field of characteristic 0 and K an overfield of k. Let $f(x) \in K[x]$ be an irreducible cubic polynomial with $\mathrm{Gal}(f/K) = \mathbf{S}_3$. (E.g., $K = k(t)$ is the field of rational functions in one variable t over k and $f(x) = x^3 - x - t$). Let $h(x) \in K[x]$ be a reducible cubic polynomial without repeated roots.*

Then the elliptic curves C_f and C_h are not isogenous over $\bar{K}$.

Proof of Corollary 1.7 (modulo Theorem 1.1). Clearly, the field k contains $\bar{\mathbb{Q}}$. By Lemma 2.4 on p. 366 of [34], $j(C_f) \notin k$. In particular, $j(C_f) \notin \bar{\mathbb{Q}}$. In

light of [28, Ch. II, Sect. 6, Th. 6.1], C_f is *not* of CM type over $\bar{K}$, i.e.,

$$\mathrm{End}(C_f) = \mathbb{Z},\ \mathrm{End}^0(C_f) = \mathbb{Q}.$$

Now the desired result follows from Theorem 1.1. □

We will need the following elementary observation that will be proven in Section 4.

Proposition 1.8. *Let $n \geq 3$ be a prime, K a field. Let $f(x), h(x) \in K[x]$ be degree n irreducible polynomials without repeated roots. Suppose that $\mathrm{Gal}(h/K)$ is a cyclic group of order n, i.e., the Galois extension $K(\mathfrak{R}_h)/K$ is cyclic of degree n. Then precisely one of the following two conditions holds.*

(i) *The fields $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ are linearly disjoint over K.*

(ii) *The field $K(\mathfrak{R}_f)$ contains $K(\mathfrak{R}_h)$ and the cyclic group $\mathbb{Z}/n\mathbb{Z}$ of order n is isomorphic to a quotient of $\mathrm{Gal}(f/K)$. In addition, the permutation group $\mathrm{Gal}(f/K)$ is not doubly transitive.*

Corollary 1.9. *Let K be a field of characteristic different from 2. Let $f(x), h(x) \in K[x]$ be irreducible cubic polynomials without repeated roots such that*

$$\mathrm{Gal}(f/K) = \mathbf{S}_3,\ \mathrm{Gal}(h/K) = \mathbf{A}_3.$$

If C_f and C_h are isogenous over $\bar{K}$ then $p = \mathrm{char}(K)$ is a prime that is congruent to 2 modulo 3, and both C_f and C_h are supersingular elliptic curves.

Proof of Corollary 1.9 (modulo Theorem 1.2). Since the order of the group $\mathbf{A}_3$ is 3, the degree $[K(\mathfrak{R}_h) : K] = 3$. Notice that $n = 3$ is a prime, the permutation group $\mathrm{Gal}(\mathfrak{R}_f) = \mathbf{S}_3$ is *doubly transitive* and $\mathrm{Gal}(h) = \mathbf{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$. Applying Proposition 1.8, we conclude that $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ are linearly disjoint over K. Now the desired result follows from Theorem 1.2. □

Corollary 1.10. *Suppose that $K = \mathbb{Q}$ and $h(x) \in \mathbb{Q}[x]$ is an irreducible cubic polynomial such that $\mathbb{Q}(\mathfrak{R}_h)$ is a cyclic cubic field, i.e., $\mathrm{Gal}(h/\mathbb{Q}) = \mathbf{A}_3$. Then the elliptic curve C_h enjoys the following properties.*

(i) *C_h is not isogenous to $y^2 = x^3 - 1$ over $\bar{\mathbb{Q}}$, i.e., $\mathrm{End}^0(C_h)$ is not isomorphic to $\mathbb{Q}(\sqrt{-3})$. In other words,*

$$j(C_h) \neq 0,\ 2^4 3^3 5^3,\ -2^{15} 3 \cdot 5^3.$$

(ii) *Let $u(x)$ be an an irreducible cubic polynomial such that $K(\mathfrak{R}_u)$ is a cyclic cubic field, i.e.,* $\mathrm{Gal}(u/\mathbb{Q}) = \mathbf{A}_3$. *If the cubic fields $\mathbb{Q}(\mathfrak{R}_h)$ and $\mathbb{Q}(\mathfrak{R}_u)$ are not isomorphic then the elliptic curves C_h and C_u are not isogenous over $\bar{\mathbb{Q}}$.*

Proof of Corollary 1.10 (modulo Theorems 1.2 and 1.1). In order to prove (i), let us put

$$f(x) = x^3 - 5 \in \mathbb{Q}[x].$$

We have seen (Example 1.4) that $\mathrm{Gal}(f/\mathbb{Q}) = \mathbf{S}_3$. It follows from Corollary 1.9 that the elliptic curves $C_f : y^2 = x^3 - 5$ and C_h are *not* isogenous over $\bar{\mathbb{Q}}$ and even over $\mathbb{C}$, thanks to Remark 1.5. Since $\mathrm{End}^0(C_f) \cong \mathbb{Q}(\sqrt{-3})$, it follows from [24, Ch. 4, Sect. 4.4, Prop. 4.9] combined with Remark 1.5. that $\mathrm{End}^0(C_h)$ is *not* isomorphic to $\mathbb{Q}(\sqrt{-3})$. On the other hand, it is well known (see the proof of Corollary 1.6) that if C is an elliptic curve over $\mathbb{Q}$ then

$$j(C) \in \{0,\ 2^4 3^3 5^3,\ -2^{15} 3 \cdot 5^3\}$$

if and only if $\mathrm{End}^0(C)$ is isomorphic to $\mathbb{Q}(\sqrt{-3})$. This ends the proof of (i).

In order to prove (ii), notice that $\mathbb{Q}(\mathfrak{R}_h) \ne \mathbb{Q}(\mathfrak{R}_u)$ (they both are subfields of $\bar{\mathbb{Q}}$). Since they both have the same degree over $\mathbb{Q}$ (namely, 3, which is a prime), $\mathbb{Q}(\mathfrak{R}_h)$ does *not* contain $\mathbb{Q}(\mathfrak{R}_u)$. Applying Proposition 1.8, we conclude that the fields $\mathbb{Q}(\mathfrak{R}_h)$ and $\mathbb{Q}(\mathfrak{R}_u)$ are *linearly disjoint* over $\mathbb{Q}$. The linear disjointness implies that $u(x)$ remains irreducible over $K_1 = \mathbb{Q}(\mathfrak{R}_h)$ while $h(x)$ is reducible (actually splits into a product of linear factors) over K_1. Notice that $\bar{\mathbb{Q}}$ is an algebraic closure of K_1.

Applying Theorem 1.1 to irreducible $u(x)$ and reducible $h(x)$ over K_1, we conclude that if C_h and C_u are isogenous over $\bar{\mathbb{Q}}$ then C_h is isogenous over $\bar{\mathbb{Q}}$ to $y^2 = x^3 - 1$, which is not the case, in light of already proven (i). Hence, C_h and C_u are *not* isogenous over $\bar{\mathbb{Q}}$. □

Example 1.11. (i) Let us put

$$K = \mathbb{Q},\ a \in \mathbb{Z},\quad h_a(z) := x^3 - ax^2 - (a+3)x - 1 \in \mathbb{Q}[x].$$

It is known [23, p. 1137–1138] that for every integer a the splitting field $\mathbb{Q}(\mathfrak{R}_{h_a})$ of the cubic polynomial $h_a(z)$ is a *cyclic* cubic field, i.e. $\mathrm{Gal}(h_a/\mathbb{Q}) = \mathbf{A}_3$. If $f(x) \in \mathbb{Q}[x]$ is any irreducible cubic polynomial with $\mathrm{Gal}(f) = \mathbf{S}_3$ (e.g., $f(x) = x^3 - x - 1$ or $x^3 - 5$) then it follows from Corollary 1.9 that the elliptic curves C_f and $C_{h_a} : y^2 = h_a(x)$ are *not* isogenous over $\bar{\mathbb{Q}}$ (and even over $\mathbb{C}$) for all $a \in \mathbb{Z}$.

(ii) Suppose that $a \ge -1$ and a^2+3a+9 is a *prime*, e.g.,

$$a = -1, 1, 2, 4, 7, 8, 10, 11, 16, 17, \dots, 410, \ \dots$$

[23, Table 1 on p. 1140]. Then the discriminant of $\mathbb{Q}(\mathfrak{R}_{h_a})$ is $(a^2+3a+9)^2$ [23, p. 1138]. This implies that if b is an integer such that $b > a$ and b^2+3b+9 is also a prime then $(b^2+3b+9)^2$ is the discriminant of $\mathbb{Q}(\mathfrak{R}_{h_b})$ and

$$(a^2+3a+9)^2 < (b^2+3b+9)^2.$$

Hence, the cubic fields $\mathbb{Q}(\mathfrak{R}_{h_a})$ and $\mathbb{Q}(\mathfrak{R}_{h_b})$ have *distinct* discriminants and therefore are *not* isomorphic. In light of Corollary 1.10, the elliptic curves C_{h_a} and C_{h_b} are *not* isogenous over $\bar{\mathbb{Q}}$.

We deduce Theorems 1.1 and 1.2 from more general results about non-isogenous hyperelliptic jacobians (Theorems 1.12 and 1.14 below) that will be stated in Subsection 1.2 and proven in Section 3.

1.2. Non-isogenous hyperelliptic jacobians

Throughout this subsection, $n \ge 3$ 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.

Theorem 1.12. *Suppose that $n \ge 3$ is an odd prime such that 2 is a primitive root* mod *n. 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 reducible.*

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

Remark 1.13. See [5, Th. 1.1] where the possible structure of the endomorphism algebra $\mathrm{End}^0(J(C_f))$ is described when K is a number field, $f(x)$ is a prime (odd) degree n irreducible polynomial over K and 2 is a primitive root mod n. (See also [30, 31].)

Theorem 1.14. *Suppose that $n \ge 3$ is an odd prime such that 2 is a primitive root* mod n. *Let K be a field of characteristic different from 2. Suppose that $f(x), h(x) \in K[x]$ are degree n polynomials without repeated roots that enjoy the following properties.*

(i) *$f(x)$ is irreducible over K and its Galois group* $\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$ *is doubly transitive.*

(ii) *$h(x)$ is irreducible over K.*

(iii) *The splitting fields $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ of $f(x)$ and $h(x)$ are linearly disjoint over K.*

Then the hyperelliptic jacobians $J(C_f)$ and $J(C_h)$ enjoy precisely one of the following properties.

(1) *The abelian varieties $J(C_f)$ and $J(C_h)$ are not isogenous over $\bar{K}$. Even better,*

$$\mathrm{Hom}(J(C_f), J(C_h)) = \{0\},\ \mathrm{Hom}(J(C_h), J(C_f)) = \{0\}.$$

(2) *$p = \mathrm{char}(K) > 0$ and both $J(C_f)$ and $J(C_h)$ are supersingular abelian varieties. In addition, n does not divide $p - 1$. More precisely, if $p \ne n$ and $\mathfrak{f}_p$ is the order of p* mod n *in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ then $\mathfrak{f}_p$ is even.*

Remark 1.15. If $n = 3$ then C_f and C_h are elliptic curves that are canonically isomorphic to their jacobians. Clearly, $\mathbf{S}_3$ is a *doubly transitive* permutation group while 2 is a *primitive root* mod 3. Hence, Theorem 1.1(i) and Theorem 1.2 are special cases of Theorems 1.12 and 1.14, respectively. Now Theorem 1.1(ii) follows from Theorem 1.1(i) combined with [24, Ch. 4, Sect. 4.4, Prop. 4.9] and Remark 1.5.

Example 1.16. Let $K = \mathbb{Q}$ and $n \ge 3$ is an odd prime. Let

$$f(x) = x^n - x - 1, h(x) = x^n - 1.$$

By a theorem of Nart and Vila [16, Th. 1] (see also [17, Cor. 3 on p. 233]), $\mathrm{Gal}(f) = \mathbf{S}_n$, which is doubly transitive. (The irreducibility of $f(x)$ was proven by Selmer [20, Th. 1].) On the other hand, $h(x)$ is obviously reducible over $\mathbb{Q}$. It is well known that $J(C_h)$ is an abelian variety of CM type with multiplication by the nth cyclotomic field $\mathbb{Q}(\zeta_n)$. It was proven in [30, Examples 2.2] that $J(C_f)$ is absolutely simple (and even $\mathrm{End}(J(C_f)) = \mathbb{Z}$).

Hence, $J(C_f)$ and $J(C_h)$ are not isogenous over $\bar{\mathbb{Q}}$ (and even over $\mathbb{C}$), and

$$\mathrm{Hom}(J(C_f), J(C_h)) = \{0\},\ \mathrm{Hom}(J(C_h), J(C_f)) = \{0\}.$$

Example 1.17. Let $K = \mathbb{Q}$ and $n \geq 3$ is an odd integer. Let

$$f(x) = x^n - 2,\ h(x) = x^n - 1.$$

By Eisenstein's criterion, the polynomial $f(x)$ is irreducible over the field $\mathbb{Q}_2$ of 2-adic numbers and therefore is irreducible also over $\mathbb{Q}$ (see also [10, Ch. VI, Sect. 9, Th. 9.1]). Obviously, $h(x)$ is reducible over $\mathbb{Q}$. However, $J(C_f)$ and $J(C_h)$ are not only isogenous over $\bar{\mathbb{Q}}$ but actually become isomorphic over $\bar{\mathbb{Q}}$. On the other hand, both $J(C_f)$ and $J(C_h)$ are abelian varieties of CM type with multiplication by $\mathbb{Q}(\zeta_n)$.

The following assertion may be viewed as a generalization of Corollary 1.9.

Corollary 1.18. *Suppose that $n \geq 3$ is an odd prime such that 2 is a primitive root* mod n. *Let K be a field of characteristic different from 2. Suppose that $f(x), h(x) \in K[x]$ are degree n polynomials without repeated roots that enjoy the following properties.*

(i) *$f(x)$ is irreducible over K and its Galois group* $\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$ *is doubly transitive.*

(ii) *$h(x)$ is irreducible over K and $K(\mathfrak{R}_h)/K$ is a degree n cyclic field extension, i.e.,* $\mathrm{Gal}(h) \cong \mathbb{Z}/n\mathbb{Z}$.

Then the hyperelliptic jacobians $J(C_f)$ and $J(C_h)$ enjoy precisely one of the following properties.

(1) $\mathrm{Hom}(J(C_f), J(C_h)) = \{0\},\ \mathrm{Hom}(J(C_h), J(C_f)) = \{0\}$.

(2) *$p = \mathrm{char}(K) > 0$ and both $J(C_f)$ and $J(C_h)$ are supersingular abelian varieties. In addition, n does not divide $p - 1$. More precisely, if $p \neq n$ then the residue p* mod n *has even multiplicative order in $(\mathbb{Z}/n\mathbb{Z})^*$.*

Proof of Corollary 1.18 (modulo Theorem 1.14). Applying Proposition 1.8, we conclude that the fields $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ are linearly disjoint over K. Now the desired result follows from Theorem 1.14. □

Example 1.19. Let us put $K = \mathbb{Q}, n = 5$, and

$$f_1(x) = x^5 - x - 1,\ f_2(x) = x^5 + 15x + 12 \in \mathbb{Q}[x];$$

$$h(x) = x^5 - 110x^3 - 55x^2 + 2310x + 979 \in \mathbb{Q}[x].$$

Notice that 2 is a *primitive root* mod 5. We have seen (Example 1.16) that $f_1(x)$ is irreducible with the doubly transitive Galois group $\mathbf{S}_5$. It is known [4, Sect. 5, p. 398] that $f_2(x)$ is irreducible, whose Galois group is the *doubly transitive Frobenius group* $\mathbf{F}_{20}$ of order 20 [4, p. 388]. It is also known [4, p. 400] that $h(x)$ is irreducible, whose Galois group is a cyclic group of order 5. Applying Corollary 1.18 to the pair of polynomials $f_1(x)$ and $h(x)$, and to the pair of polynomials $f_2(x)$ and $h(x)$, we conclude that

$$\mathrm{Hom}(J(C_{f_1}), J(C_h)) = \{0\},\ \mathrm{Hom}(J(C_h), J(C_{f_1})) = \{0\};$$

$$\mathrm{Hom}(J(C_{f_2}), J(C_h)) = \{0\},\ \mathrm{Hom}(J(C_h), J(C_{f_2})) = \{0\}.$$

I claim that

$$\mathrm{Hom}(J(C_{f_1}), J(C_{f_2})) = \{0\},\ \mathrm{Hom}(J(C_{f_2}), J(C_{f_1})) = \{0\}.$$

Indeed, in light of Theorem 1.14, it suffices to check that the splitting fields $\mathbb{Q}(\mathfrak{R}_{f_1})$ and $\mathbb{Q}(\mathfrak{R}_{f_2})$ are *linearly disjoint* over $\mathbb{Q}$, i.e., their *intersection* $F = \mathbb{Q}(\mathfrak{R}_{f_1}) \cap \mathbb{Q}(\mathfrak{R}_{f_2})$ coincides with $\mathbb{Q}$. Suppose that this is not the case, i.e. $[F : \mathbb{Q}] > 1$. Clearly, $F/\mathbb{Q}$ is a Galois extension. It is also clear that

$$[\mathbb{Q}(\mathfrak{R}_{f_1}) : \mathbb{Q}] > [\mathbb{Q}(\mathfrak{R}_{f_2}) : \mathbb{Q}]$$

and the Frobenius group $\mathrm{Gal}(f_2)$ is *not* isomorphic to a quotient of $\mathrm{Gal}(f_1) = \mathbf{S}_5$. Hence, none of $\mathbb{Q}(\mathfrak{R}_{f_1})$ and $\mathbb{Q}(\mathfrak{R}_{f_2})$ is a subfield of the other one, and therefore F is a *proper subfield* of both $\mathbb{Q}(\mathfrak{R}_{f_1})$ and $\mathbb{Q}(\mathfrak{R}_{f_2})$. In particular, the natural *surjective* homomorphism

$$\mathbf{S}_5 = \mathrm{Gal}(f_1) \twoheadrightarrow \mathrm{Gal}(F/\mathbb{Q})$$

has a *nontrivial* kernel and therefore $\mathrm{Gal}(F/\mathbb{Q})$ is a cyclic group of order 2, i.e., F is a quadratic field. Since F is a subfield of $\mathbb{Q}(\mathfrak{R}_{f_1})$ and the only index 2 subgroup of $\mathbf{S}_5$ is $\mathbf{A}_5$, the field $F = \mathbb{Q}(\sqrt{D_1})$ where D_1 is the discriminant of $f_1(x)$, which equals $19 \cdot 151$. On the other hand, $\mathbb{Q}(\mathfrak{R}_{f_2})$ contains the quadratic subfield $\mathbb{Q}(\sqrt{D_2})$ where D_2 is the discriminant of $f_1(x)$, which equals $2^{10}3^45^5$ [4] and therefore $\mathbb{Q}(\mathfrak{R}_{f_2})$ contains the quadratic field $F_2 :=$

$\mathbb{Q}(\sqrt{5})$. This implies that $\mathbb{Q}(\mathfrak{R}_{f_2})$ contains two *distinct* quadratic fields F and F_2 and therefore there is a surjective group homomorphism

$$\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_{f_2})/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(F_2F/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

However, the Sylow 2-subgroup of the Frobenius group $\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_{f_2})/\mathbb{Q})$ is cyclic. Hence, $\mathrm{Gal}(\mathbb{Q}(\mathfrak{R}_{f_2})/\mathbb{Q})$ does not have a quotient that is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The obtained contradiction proves the desired result.

The paper is organized as follows. In Section 2 we discuss Galois properties of points of order 2 on hyperelliptic jacobians and abelian varieties. Notice that Proposition 2.4 is central to the results of the paper and may be of certain independent interest. We also formulate there several useful auxiliary results about matrix algebras of skew-fields and splitting fields of polynomials. Section 3 contains the proofs of Theorems 1.12 and 1.14. In Sections 4 and 5 we prove Proposition 1.8 and auxiliary results from Section 2.

This paper may be viewed as a follow-up of [32, 33].

2. Order 2 points on hyperelliptic jacobians

Recall that $\mathrm{char}(K) \neq 2$. We start with an arbitrary positive-dimensional abelian variety X over K. If d is a positive integer that is not divisible by $\mathrm{char}(K)$ then we write $X[d]$ for the kernel of multiplication by d in $X(\bar{K})$. It is well known that

$$X[d] \subset X(K_s) \subset X(\bar{K});$$

in addition, $X[d]$ is a $\mathrm{Gal}(K)$-submodule of $X(K_s)$; this submodule is isomorphic as a commutative group to $(\mathbb{Z}/d\mathbb{Z})^{2\dim(X)}$ ([15, Sect. 6], [12, Sect. 8, Remark 8.4]). We denote by

$$\tilde{\rho}_{d,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}/d\mathbb{Z}}(X[d])$$

the corresponding (continuous) homomorphism defining the action of $\mathrm{Gal}(K)$ on $X[d]$ and put

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

Let us consider

$$G(d) := \ker(\tilde{\rho}_{d,X}) \subset \mathrm{Gal}(K),$$

which is a closed *normal subgroup* of finite index (and therefore also open) in $\mathrm{Gal}(K)$. Since $G(d)$ is open normal, the subfield of $G(d)$-invariants in K_s

$$K(X[d]) := K_s^{G(d)}$$

is a finite Galois extension of K. Hence, $\tilde{G}_{d,X} = \mathrm{Gal}(K)/G(d)$ coincides with the Galois group of $K(X[d])/K$. By definition, $K(X[d])$ coincides with the *field of definition* of all torsion points of order dividing d on X. For example, $X[2]$ is a $2\dim(X)$-dimensional vector space over the 2 elements 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 $X[2]$.

Remark 2.1. The surjectiveness of $\mathrm{Gal}(K) \twoheadrightarrow \tilde{G}_{2,X}$ implies that the $\mathrm{Gal}(K)$-module $X[2]$ is simple (resp. absolutely simple) if and only if the $\tilde{G}_{2,X}$-module $X[2]$ is absolutely simple.

Remark 2.2. (i) Let $K(X[4])$ be the field of definition of all points of order dividing 4 on X. Recall that $K(X[4])/K$ is a finite Galois field extension. Clearly,

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

It is known that the Galois group $\mathrm{Gal}(K(X[4])/K(X[2]))$ is a finite commutative group of exponent 2 or 1. For reader's convenience, let us give a short proof. Let

$$\sigma \in \mathrm{Gal}(K(X[4])/K(X[2])) \subset \mathrm{Gal}(K(X[4])/K) = \tilde{G}_{4,X}.$$

Then for each $x \in X[4]$ we have $2x \in X[2]$ and therefore $\sigma(2x) = 2x$. This implies that $2(\sigma(x) - x) = \sigma(2x) - 2x = 0$, i.e., $y = \sigma(x) - x \in X[2]$ and therefore $\sigma(y) = y$. Thus

$$\sigma^2(x) = \sigma(x + y) = \sigma(x) + y = (x + y) + y = x + 2y = x.$$

This proves that each $\sigma \in \mathrm{Gal}(K(X[4])/K(X[2]))$ has order dividing 2 and therefore $\mathrm{Gal}(K(X[4])/K(X[2]))$ is a (finite) commutative group of exponent 2 or 1.

(ii) All the endomorphisms of X are defined over $K(X[4])$ (a special case of Theorem 2.4 of A. Silverberg [26]). See [5, 6, 19] for further results about the field of definition of endomorphisms of abelian varieties.

The following two assertions will be used in the proof of Theorems 1.12 and 1.14.

Lemma 2.3. [1] *Let n be an odd prime such that 2 is a primitive root* mod n *of 1. Let $g = (n-1)/2$. Suppose that* $\dim(X) = g$ *and the degree* $[K(X[2]) : K]$ *is divisible by n.*

Then the $\mathrm{Gal}(K)$*-module* $X[2]$ *is simple.*

Proposition 2.4. *Let n be an odd prime such that 2 is a primitive root* mod n*. Let $g = (n-1)/2$. Let X and Y be g-dimensional abelian varieties defined over K that are isogenous over $\bar{K}$. Suppose that $K(Y[2]) = K$ and the degree $[K(X[2]) : K]$ is divisible by n.*

Then both X and Y are abelian varieties of CM type over $\bar{K}$ with multiplication by $\mathbb{Q}(\zeta_n)$.

We will prove Lemma 2.3 and Proposition 2.4 in Section 4.

Now let us turn to hyperelliptic jacobians. The following assertion will play a crucial role in the proof of Theorems 1.12 and 1.14.

Proposition 2.5. *Suppose that $n \geq 3$ is an odd prime and 2 is a primitive root* mod n*. Let $f(x) \in K[x]$ be a degree n polynomial without repeated roots.*

Then the jacobian $J(C_f)$ enjoys the following properties.

(0) *There is a canonical isomorphism of finite groups*

$$\tilde{G}_{2,J(C_f)} \cong \mathrm{Gal}(f/K).$$

In addition, $K(\mathfrak{R}_f)$ coincides with the field $K(J(C_f)[2])$ of definition of all points of order 2 on $J(C_f)$.

(1) *If $f(x)$ is irreducible over K then* $\mathrm{Gal}(f)$ *contains a cyclic subgroup H of order n and the* $\mathrm{Gal}(K)$*-module $J(C_f)[2]$ is simple.*

(2) *If $f(x)$ is irreducible over K and its Galois group* $\mathrm{Gal}(\mathfrak{R}_f) \subset \mathrm{Perm}(\mathfrak{R}_f)$ *is doubly transitive then the* $\mathrm{Gal}(K)$*-module $J(C_f)[2]$ is absolutely simple.*

(3) *Suppose that $f(x)$ is irreducible over K and its Galois group* $\mathrm{Gal}(\mathfrak{R}_f) \subset \mathrm{Perm}(\mathfrak{R}_f)$ *is doubly transitive. Let $h(x) \in K[x]$ be a degree n polynomial without repeated roots that is irreducible over K.*

[1] Actually, the statement and proof of Lemma 2.3 below may be extracted from [5, p. 4644–4645].

If the splitting fields $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ of $f(x)$ and $h(x)$ are linearly disjoint over K then either

$$\mathrm{Hom}(J(C_f), J(C_h)) = \{0\},\ \mathrm{Hom}(J(C_h), J(C_f)) = \{0\}$$

or $\mathrm{char}(K) > 0$ *and both $J(C_f)$ and $J(C_h)$ are supersingular abelian varieties.*

We prove Proposition 2.5 in Section 4.

2.1. Galois module $J(C_f)[2]$

In this subsection we discuss a well known explicit description of the Galois module $J(C_f)[2]$ for arbitrary (separable) $f(x)$ and (odd) n. This description will be used in the proof of Proposition 2.5. 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 $\mathfrak{R}_f \subset K_s$. The action of $\mathrm{Perm}(\mathfrak{R}_f)$ on $\mathfrak{R}_f$ provides $\mathbb{F}_2^{\mathfrak{R}_f}$ with the structure of a faithful $\mathrm{Perm}(\mathfrak{R}_f)$-module, which splits into a direct sum

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

of the one-dimensional subspace of constant functions $\mathbb{F}_2 \cdot \mathbf{1}_{\mathfrak{R}_f}$ and the $(n-1)$-dimensional *heart* [8, 14]

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

(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 $\mathrm{Gal}(f)$-module.

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

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

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

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

The surjectiveness implies that the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}_f}$ is simple (resp. absolutely simple) if and only if it is simple (resp. absolutely simple) as the $\mathrm{Gal}(K)$-module.

It is well known (see, e.g., [13, 31]) 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 $K(J(C_f)[2])$. In addition, the $\mathrm{Gal}(K)$-module $J(C_f)[2]$ is simple (resp. absolutely simple) if and only if the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}_f}$ is simple (resp. absolutely simple).

2.2. Useful algebraic results

We finish this section by stating two auxiliary elementary results that will be used in the proofs of Theorems 1.12 and 1.14.

Lemma 2.6. *Let n be a prime, K an arbitrary field, and $h(x) \in K[x]$ a polynomial without repeated roots with $\deg(h) \le n$. If $h(x)$ is reducible over K then the degree $[K(\mathfrak{R}_h) : K]$ is not divisible by n. More precisely, if l is a prime divisor of $[K(\mathfrak{R}_h) : K]$ then $l < n$.*

Lemma 2.7. *Let n and p be distinct primes. Assume that n is odd, i.e., $m := (n-1)/2$ a positive integer. Let D be a quaternion algebra over $\mathbb{Q}$ that is ramified at p, i.e., $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra over the field $\mathbb{Q}_p$ of p-adic numbers. Let E be a commutative $\mathbb{Q}$-subalgebra of $\mathrm{Mat}_m(D)$ (with the same 1) that is isomorphic to the nth cyclotomic field $\mathbb{Q}(\zeta_n)$.*

Then $p \bmod n$ has even multiplicative order in $(\mathbb{Z}/n\mathbb{Z})^*$. In particular, n does not divide $p-1$.

Remark 2.8. Keeping the notation and assumptions of Lemma 2.7, assume additionally that $n = 3$. (This is exactly the case that we need for elliptic curves.) Then

$$p \ne 3,\ \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}),\ m = 1, \mathrm{Mat}_m(D) = D.$$

Hence, $\mathbb{Q}(\sqrt{-3}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is isomorphic to a subalgebra of the division algebra $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$. This implies that $\mathbb{Q}(\zeta_3) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ has no zero divisors, i.e., p is *inert* in $\mathbb{Q}(\sqrt{-3})$, which means that $p-1$ is *not* divisible by 3. Hence, $p \equiv 2 \bmod 3$ and therefore has multiplicative order 2 in $(\mathbb{Z}/3\mathbb{Z})^*$. This proves Lemma 2.7 for $n = 3$.

We will prove Lemmas 2.6 and 2.7 in Sections 4 and 5 respectively.

3. Non-isogenous hyperelliptic jacobians: proofs

Proof of Theorem 1.12. We may assume that $f(x)$ is irreducible over K and $h(x)$ is reducible over K.

By Proposition 2.5(1),

$$\mathrm{Gal}(K(J(C_f)[2]))/K) = \mathrm{Gal}(K(\mathfrak{R}_f)/K)$$

contains a cyclic subgroup H of order n. Replacing K by its overfield $K(\mathfrak{R}_f)^H$ (of H-invariants in $K(\mathfrak{R}_f)$), we may and will assume that

$$\mathrm{Gal}(K(J(C_f)[2])/K) = \mathrm{Gal}(K(\mathfrak{R}_f)/K) = H$$

is a cyclic group of (prime odd) order n. By Lemma 2.6, the degree of Galois extension $K(\mathfrak{R}_h)/K$ is not divisible by n. This implies that the fields $K(J(C_f)[2])$ and $K(\mathfrak{R}_h)$ are linearly disjoint over K. Replacing K by its overfield $K(\mathfrak{R}_h)$, we may and will assume that

$$K(J(C_h)[2]) = K(\mathfrak{R}_h) = K$$

and $\mathrm{Gal}(K(J(C_f)[2])/K)$ is a cyclic group of order n. In particular,

$$[K(J(C_f)[2]) : K] = n.$$

Now the desired result follows from Proposition 2.4 applied to $X = J(C_f)$ and $Y = J(C_h)$. □

Proof of Theorem 1.14. In light of Proposition 2.5(3), we may and will assume that $p = \mathrm{char}(K) > 0$ and both $J(C_f)$ and $J(C_h)$ are $(n-1)/2$-dimensional supersingular abelian varieties, which are isogenous. We may also assume that $p \neq n$.

The linear disjointness of the splitting fields (property (iii)) means that

$$\mathrm{Gal}(f/K(\mathfrak{R}_h)) = \mathrm{Gal}(f/K) \subset \mathrm{Perm}(\mathfrak{R}_f).$$

In particular, $f(x)$ remains irreducible over $K(\mathfrak{R}_h)$. So, replacing K by its overfield $K(\mathfrak{R}_h)$, we may and will assume that $f(x)$ is irreducible over K and $h(x)$ splits into a product of linear factors, i.e., the $\mathrm{Gal}(K)$-module $J(C_f)[2]$

is simple (thanks to Proposition 2.5(1)) while

$$K = K(\mathfrak{R}_h) = K(J(C_h)[2]).$$

The irreducibility of $f(x)$ implies that $[K(\mathfrak{R}_f) : K]$ is divisible by $\deg(f) = n$. Applying Proposition 2.4 to $X = J(C_f), Y = J(C_h)$, we conclude that $\mathrm{End}^0(J(C_h))$ contains an invertible element, say, c, of multiplicative order n such that the $\mathbb{Q}$-subalgebra $\mathbb{Q}[c] \cong \mathbb{Q}(\zeta_n)$. The supersingularity of $J(C_h)$ implies that $\mathrm{End}^0(J(C_h))$ is isomorphic to the matrix algebra $\mathrm{Mat}_m(D_{p,\infty})$ of size $m := (n-1)/2$ over a definite quaternion $\mathbb{Q}$-algebra $D_{p,\infty}$ such that $D_{p,\infty}$ is ramified precisely at p and ∞ [29, Th. 2d]. We obtain that $\mathrm{Mat}_m(D_{p,\infty})$ contains a subfield (with the same 1) that is isomorphic to $\mathbb{Q}(\zeta_n)$.

Now the desired result follows from Lemma 2.7 applied to $D = D_{p,\infty}$. □

4. Proofs of auxiliary results

Proof of Proposition 1.8. Suppose that the Galois extensions $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ of K are *not* linearly disjoint over K. In light of [2, A.V.71, Th. 5] (see also [10, Ch. VI, Th. 1.14]), this means that the field

$$L := K(\mathfrak{R}_f) \cap K(\mathfrak{R}_h) \neq K.$$

Clearly,

$$K \subset L \subset K(\mathfrak{R}_h).$$

Since the degree $[K(\mathfrak{R}_h) : K] = n$ is a prime, $L = K(\mathfrak{R}_h)$, i.e.,

$$K(\mathfrak{R}_f) \cap K(\mathfrak{R}_h) = L = K(\mathfrak{R}_h),$$

which means that $K(\mathfrak{R}_h) \subset K(\mathfrak{R}_f)$. This implies that $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(h)$ is isomorphic to a quotient of $\mathrm{Gal}(f)$, i.e., there exists a surjective group homomorphism

$$\psi : G := \mathrm{Gal}(f) \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}.$$

Suppose that $\mathrm{Gal}(f)$ is *doubly transitive*. We need to arrive to a contradiction. Let us choose a root $\alpha \in \mathfrak{R}_f$ of $f(x)$ and let G_α be the *stabilizer* of α in G. Since G is transitive, G_α is a subgroup of index n in G. Since n is a

prime and the permutation group

$$G = \mathrm{Gal}(\mathfrak{R}_f/K) \subset \mathrm{Perm}(\mathfrak{R}_f)$$

is isomorphic to a subgroup of $\mathbf{S}_n$, the order of G is *not* divisible by n^2. This implies that the order of G_α is not divisible by n, i.e., is prime to n. It follows that the order of the image $\psi(G_\alpha)$ is prime to n as well. Since $\psi(G_\alpha)$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$, we get $\psi(G_\alpha) = \{0\}$, i.e.,

$$G_\alpha \subset \ker(\psi)\ \forall \alpha \in \mathfrak{R}_f.$$

The surjectiveness of ψ implies that the index of $\ker(\psi)$ in G is also n. Hence, both G_α and $\ker(\psi)$ have the same order. Now, the inclusion $G_\alpha \subset \ker(\psi)$ implies that

$$G_\alpha = \ker(\psi)\ \forall \alpha \in \mathfrak{R}_f.$$

It follows that $\ker(\psi)$ lies in all the stabilizers G_α, i.e., $\ker(\psi)$ consists only of the trivial permutation, which sends every $\alpha \in \mathfrak{R}_f$ to α. Hence, the surjective homomorphism ψ is an isomorphism, i.e., $\mathrm{Gal}(f) \cong \mathbb{Z}/n\mathbb{Z}$. In particular, the order of $\mathrm{Gal}(f)$ is n. However, $\mathrm{Gal}(f)$ is a *doubly transitive* permutation group of the n-element set $\mathfrak{R}_f$. Hence, the order of $\mathrm{Gal}(f)$ is at least $n(n-1)$, which is strictly greater than n, because $n \geq 3$. The obtained contradiction proves the desired result. □

Proof of Lemma 2.3. First,

$$\dim_{\mathbb{F}_2}(X[2]) = 2g = 2 \cdot \frac{n-1}{2} = n-1.$$

Second, since $[K(X[2]) : K]$ is divisible by the prime n, the Galois group $\tilde{G}_{2,X} = \mathrm{Gal}(K(X[2])/K)$ contains a cyclic subgroup H_2 of order n. Our assumptions on n imply that the faithful representation of $H_2 \cong \mathbb{Z}/n\mathbb{Z}$ on the $(n-1)$-dimensional $\mathbb{F}_2$-vector space $X[2]$ is irreducible, see [5, Lemma 2.8]. Since H_2 is a subgroup of $\tilde{G}_{2,X}$, the $\tilde{G}_{2,X}$-module $X[2]$ is also simple, which means that the $\mathrm{Gal}(K)$-module $X[2]$ is simple as well. □

Proof of Proposition 2.4. There are field inclusions

$$K \subset K(X[2]) \subset K(X[4]). \tag{1}$$

Since $[K(X[2]) : K]$ is divisible by n, the degree $[K(X[4]) : K]$ is also divisible by n. Hence, the Galois group $\mathrm{Gal}(K(X[4])/K)$ contains a cyclic subgroup H of order n. Replacing K by its overfield $K(X[4])^H$ (of H-invariants),

we may and will assume that $K(X[4])/K$ is a degree n cyclic extension, i.e., a Galois extension with Galois group $\mathrm{Gal}(K(X[4])/K) \cong \mathbb{Z}/n\mathbb{Z}$. On the other hand, the field inclusions (1) give rise to the short exact sequence of Galois groups

$$\{1\} \to \mathrm{Gal}(K(X[4])/K(X[2]) \to \mathrm{Gal}(K(X[4])])/K) \\ \to \mathrm{Gal}(K(X[2])])/K) \to \{1\}.$$

In particular, $\mathrm{Gal}(K(X[4])/K(X[2]))$ is a subgroup of $\mathrm{Gal}(K(X[4])/K)$ and therefore the order of $\mathrm{Gal}(K(X[4])/K(X[2]))$ divides the order of $\mathrm{Gal}(K(X[4])])/K)$, which is *odd* n. We know that $\mathrm{Gal}(K(X[4])/K(X[2]))$ is a finite 2-group (see Remark 2.2). This implies that the order of $\mathrm{Gal}(K(X[4])/K(X[2]))$ is 1. In light of the exact sequence, we get that $K(X[4]) = K(X[2])$; in particular, $\mathrm{Gal}(K(X[2])])/K)$ is a cyclic group of order n and therefore $[K(X[2])] : K] = n$.

Recall (Remark 2.2) that $K(Y[4])/K(Y[2])$ is a finite Galois extension, whose degree is a power of 2. Since $K(Y[2]) = K$ and n is an odd prime, the fields $K(Y[4])$ and $K(X[4])$ are linearly disjoint over K. Replacing K by its overfield $K(Y[4])$, we may and will assume that $K = K(Y[4])$ and $K(X[4]) = K(X[2])$ is still a cyclic degree n extension of K. In light of already proven Lemma 2.3, the $\mathrm{Gal}(K)$-module $X[2]$ is simple.

It follows from the theorem of Silverberg (see Remark 2.2 above) applied to X, Y and $X \times Y$ that all the endomorphisms of Y are defined over K and all the homomorphisms from X to Y are defined over $K(X[4]) = K(X[2])$.

Suppose that X and Y are isogenous over $\bar{K}$. Let $\phi : X \to Y$ be an isogeny, which, as we know, is defined over $K(X[4])$. We may assume that ϕ has the smallest possible degree; in particular, ϕ is *not* divisible by 2 in $\mathrm{Hom}(X, Y)$. If ϕ is defined over K then it induces a *nonzero* homomorphism of $\mathrm{Gal}(K)$-modules $X[2] \to Y[2]$, which is nonzero, because ϕ is *not* divisible by 2. However, the module $X[2]$ is simple while the module $Y[2]$ is trivial (as a Galois representation), because $K(Y[2]) = K$. Hence, a nonzero homomorphism of these Galois modules does *not* exist and therefore ϕ is *not* defined over K. Since both X and Y are defined over K, to each $\sigma \in \mathrm{Gal}(K(X[4])/K) \cong \mathbb{Z}/nZ$ corresponds the isogeny $\sigma(\phi) : X \to Y$, which does *not* coincide with ϕ if σ is *not* the identity element of $\mathrm{Gal}(K(X[4])/K)$. Since both ϕ and $\sigma(\phi)$ are isogenies from X to Y, there exists precisely one $a_\sigma \in \mathrm{End}^0(Y)^*$ such that

$$\sigma(\phi) = a_\sigma \phi \text{ in } \mathrm{Hom}(X, Y) \otimes \mathbb{Q}.$$

If $\tau \in \mathrm{Gal}(K(X[4])/K)$ then

$$a_{\sigma\tau}(\phi) = (\sigma\tau)\phi = \sigma(\tau(\phi)) = \sigma(a_\tau\phi) = \sigma(a_\tau)\sigma(\phi).$$

Since all the endomorphisms of Y are defined over K, we have $\sigma(a_\tau) = a_\tau$ and therefore

$$a_{\sigma\tau}(\phi) = a_\tau\sigma(\phi) = a_\tau(a_\sigma\phi) = (a_\tau a_\sigma)\phi$$

for all $\sigma, \tau \in \mathrm{Gal}(K(X[4])/K)$. Since $\mathrm{Gal}(K(X[4])/K)$ is commutative,

$$a_{\tau\sigma}\phi = a_{\sigma\tau}\phi = (a_\tau a_\sigma)\phi.$$

Since ϕ is an isogeny, we get

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

In other words, the map

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

is a group homomorphism, which, as we know, is nontrivial. Take any non-identity element $\sigma \in \mathrm{Gal}(K(X[4])/K)$ and put

$$c = a_\sigma \in \mathrm{End}^0(Y)^*.$$

Then c is a non-identity element of $\mathrm{End}^0(Y)^*$. In addition, $c^n = 1$, because the order of σ is n. Since n is a prime, the quotient-algebra $\mathbb{Q}[T]/(T^n - 1)$ of the ring of polynomials $\mathbb{Q}[T]$ is isomorphic to the direct sum $\mathbb{Q}(\zeta_n) \oplus \mathbb{Q}$. Hence, the $\mathbb{Q}$-subalgebra $\mathbb{Q}[c]$ of $\mathrm{End}^0(Y)$ is isomorphic to a quotient of $\mathbb{Q}(\zeta_n) \oplus \mathbb{Q}$; in particular, it is a *semisimple commutative* $\mathbb{Q}$-(sub)algebra. Notice that

$$2\dim(Y) = n - 1 < (n-1) + 1 = \dim_{\mathbb{Q}}\left(\mathbb{Q}(\zeta_n) \oplus \mathbb{Q}\right).$$

It follows from [25, Ch. II, Prop. 1 on p. 36] that

$$\dim_{\mathbb{Q}}(\mathbb{Q}[c]) \le 2\dim(Y) = n - 1 < \dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_n) \oplus \mathbb{Q});$$

in particular, $\mathbb{Q}[c]$ is not isomorphic to $\mathbb{Q}(\zeta_n) \oplus \mathbb{Q}$. Since c has odd multiplicative order $n > 2$, $\mathbb{Q}[c]$ is not isomorphic to $\mathbb{Q}$. The only remaining

possibility is that there there is an isomorphism of $\mathbb{Q}$-algebras $\mathbb{Q}[c] \cong \mathbb{Q}(\zeta_n)$. This gives as a $\mathbb{Q}$-algebra embedding

$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[c] \subset \mathrm{End}^0(Y).$$

Since

$$2\dim(Y) = n-1 = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)),$$

Y is an abelian variety of CM type over $\bar{K}$ with multiplication by $\mathbb{Q}(\zeta_n)$. Since X is $\bar{K}$-isogenous to Y, it is also of CM type with multiplication by $\mathbb{Q}(\zeta_n)$. □

Proof of Proposition 2.5. Assertion (0) is already proven in Subsection 2.1. In order to prove (1), notice that the irreducibility of $f(x)$ means the transitivity of the permutation group

$$\mathrm{Gal}(f) = \mathrm{Gal}(f/K) \subset \mathrm{Perm}(\mathfrak{R}_f).$$

Since $n = \#(\mathfrak{R}_f)$, the transitivity implies that n divides the order of $\mathrm{Gal}(f)$. Let

$$H \subset \mathrm{Gal}(f/K) \subset \mathrm{Perm}(\mathfrak{R}_f)$$

be a cyclic subgroup of prime order n in $\mathrm{Gal}(f/K)$ and $K_1 = K(\mathfrak{R}_f)^H$ the subfield of H-invariants in $K(\mathfrak{R}_f)$. Then

$$K \subset K_1 \subset K(\mathfrak{R}_f),\ K_1(\mathfrak{R}_f) = K(\mathfrak{R}_f);$$

$$\mathrm{Gal}(f/K_1) = H \subset \mathrm{Gal}(f/K) \subset \mathrm{Perm}(\mathfrak{R}_f).$$

Recall that n is a *prime* and 2 is a *primitive root* mod n, i.e., 2 mod n has order $n-1$ in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. Since

$$\mathrm{Gal}(f/K_1) \cong \mathbb{Z}/n\mathbb{Z} \ \text{ and } \ n-1 = \dim_{\mathbb{F}_2}(Q_{\mathfrak{R}_f}),$$

the $\mathrm{Gal}(f/K_1)$-module $Q_{\mathfrak{R}_f}$ is simple, thanks to [5, Lemma 2.8] (applied to $n = 2, p = n, s = n-1$). Since $\mathrm{Gal}(f/K_1) \subset \mathrm{Gal}(f/K)$, the $\mathrm{Gal}(f/K)$-module $Q_{\mathfrak{R}_f}$ is also simple and therefore the $\mathrm{Gal}(K)$-module $Q_{\mathfrak{R}_f}$ is simple as well. This implies that the $\mathrm{Gal}(K)$-module $J(C_f)[2]$ is also simple, thanks to the arguments at the end of Subsection 2.1.

Let us prove (2). We are given that $\mathrm{Gal}(f)$ is *doubly transitive*. Since n is *odd*, the centralizer $\mathrm{End}_{\mathrm{Gal}(f)}(Q_{\mathfrak{R}_f})$ coincides with $\mathbb{F}_2$, thanks to [8, Satz 4a] (see also [13, p. 108]). This implies that the simple $\mathrm{Gal}(f)$-module

$Q_{\mathfrak{R}_f}$ is absolutely simple and therefore the $\mathrm{Gal}(K)$-module $J(C_f)[2]$ is also absolutely simple, thanks to the arguments at the end of Subsection 2.1.

Let us prove (3). We are given that the fields $K(J(C_f)[2]) = K(\mathfrak{R}_f)$ and $K(J(C_h)[2]) = K(\mathfrak{R}_h)$ are linearly disjoint over K. By already proven assertions (1) and (2) combined with Remark 2.1, the $\mathrm{Gal}(K)$-module $J(C_f)[2]$ is absolutely simple while the $\mathrm{Gal}(K)$-module $J(C_h)[2]$ is simple. Now the desired result follows from Theorem 2.1 of [32] (applied to $n = 2$ and $X = J(C_f), Y = J(C_h)$). □

Proof of Lemma 2.6. We may view $\mathrm{Gal}(\mathfrak{R}_h)$ as the certain subgroup of $\mathrm{Perm}(\mathfrak{R}_h)$. If the order N of $\mathrm{Gal}(\mathfrak{R}_h)$ is divisible by n then $\mathrm{Gal}(\mathfrak{R}_h)$ contains an element of order n (recall that n is a prime), which is a n-cycle. This implies that $\mathrm{Gal}(\mathfrak{R}_h)$ acts transitively on $\mathfrak{R}_h$, which contradicts the reducibility of $h(x)$. Hence, N is *not* divisible by n. On the other hand, N obviously divides $n!$. This implies that all prime divisors of N are strictly less than n. It remains to notice that $N = [K(\mathfrak{R}_h) : K]$.

□

5. Central simple algebras and cyclotomic fields

The aim of this section is to prove Lemma 2.7. We start with some basic facts related to cyclotomic fields.

Remark 5.1. Suppose that p and n are *distinct* primes. Let $\mathcal{O}$ be the ring of integers in the nth cyclotomic field $L := \mathbb{Q}(\zeta_n)$ and $\mathfrak{P}$ a maximal ideal of $\mathcal{O}$ that contains $p\mathcal{O}$. Let $L_{\mathfrak{P}}$ be the completion of L with respect to the $\mathfrak{P}$-adic topology.

(i) By definition, $L_{\mathfrak{P}}$ contains the fields L and $\mathbb{Q}_p$ (which coincides with the completion of $\mathbb{Q}$ with respect to the $\mathfrak{P}$-adic topology). Since n is a prime, the field extension $L/\mathbb{Q} = \mathbb{Q}(\zeta_n)/\mathbb{Q}$ is cyclic and therefore the field extension $L_{\mathfrak{P}}/\mathbb{Q}_p$ is also cyclic.

(ii) Since the primes p and n are distinct, the field extension $L_{\mathfrak{P}}/\mathbb{Q}_p$ is *unramified* and therefore the degrees of the field extensions $L_{\mathfrak{P}}/\mathbb{Q}_p$ and $(\mathcal{O}/\mathfrak{P}) \,/\, (\mathbb{Z}/p\mathbb{Z})$ do coincide.

(iii) In light of [1, Sect. 1, Lemma 4 and its proof], the residual degree $[\mathcal{O}/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}]$ coincides with the multiplicative order $\mathfrak{f}_p$ of $p \bmod n \in (\mathbb{Z}/n\mathbb{Z})^*$. This implies that

$$\mathfrak{f}_p = [L_{\mathfrak{P}} : \mathbb{Q}_p]\,. \tag{2}$$

5.2. We also need to recall basic facts about central simple algebras [18, Sect. 13.1 and 15.1]. Let $\mathcal{K}$ be a field. If $\mathcal{A}$ is a central simple algebra over $\mathcal{K}$ then we write $[\mathcal{A}]$ for the similarity class of $\mathcal{A}$ in the *Brauer group* $\mathrm{Br}(\mathcal{K})$. If $\phi : \mathcal{K} \hookrightarrow \mathcal{L}$ is an *embedding of fields* then there is the natural group homomorphism [18, Sect. 12.5]

$$\phi_* : \mathrm{Br}(\mathcal{K}) \to \mathrm{Br}(\mathcal{L}),\ [\mathcal{A}] \to [\mathcal{A} \otimes_{\mathcal{K}} \mathcal{L}]. \tag{3}$$

Recall that the correspondences

$$\mathcal{K} \mapsto \mathrm{Br}(\mathcal{K}),\ \phi \mapsto \phi_*$$

define a *functor* from the category of fields to the category of commutative groups [18, Sect. 12.5, Proposition **c**]. In particular, if $\psi : \mathcal{L} \hookrightarrow \mathcal{F}$ is a *field embedding* then the group homomorphism $(\psi\phi)_* : \mathrm{Br}(\mathcal{K}) \to \mathrm{Br}(\mathcal{F})$ coincides with the *composition*

$$\psi_* \circ \phi_* : \mathrm{Br}(\mathcal{K}) \to \mathrm{Br}(\mathcal{L}) \to \mathrm{Br}(\mathcal{F}). \tag{4}$$

In addition, if ψ is a *field isomorphism* then ψ_* is a *group isomorphism*.

If $\mathcal{L}$ is an *overfield* of $\mathcal{K}$ then we write

$$i(\mathcal{K}, \mathcal{L}) : \mathcal{K} \subset \mathcal{L}$$

for the *inclusion map*. We write $\mathbf{B}(\mathcal{L}/\mathcal{K})$ for the *relative Brauer group* of $\mathcal{L}/\mathcal{K}$, i.e., for the *kernel* of the group homomorphism

$$i(\mathcal{K}, \mathcal{L})_* : \mathrm{Br}(\mathcal{K}) \to \mathrm{Br}(\mathcal{L}).$$

[18, Sect. 13.2]. If $\mathcal{F}$ is an *overfield* of $\mathcal{L}$ then, by functoriality (4),

$$i(\mathcal{K}, \mathcal{F})_* = i(\mathcal{L}, \mathcal{F})_* \circ i(\mathcal{K}, \mathcal{L})_*. \tag{5}$$

If $\mathcal{L}_1$ and $\mathcal{L}_2$ are *overfields* of $\mathcal{K}$ and there is a field isomorphism $\psi : \mathcal{L}_1 \to \mathcal{L}_2$, whose restriction to $\mathcal{K}$ coincides with the *identity map* then

$$i(\mathcal{K}, \mathcal{L}_2) = \psi \circ i(\mathcal{K}, \mathcal{L}_1)$$

and therefore

$$i(\mathcal{K}, \mathcal{L}_2)_* = \psi_* \circ i(\mathcal{K}, \mathcal{L}_1)_*.$$

Since $\psi_* : \mathrm{Br}(\mathcal{L}_1) \to \mathrm{Br}(\mathcal{L}_2)$ is a group isomorphism, the kernels of $i(\mathcal{K}, \mathcal{L}_2)_*$ and $i(\mathcal{K}, \mathcal{L}_1)_*$ do coincide, i.e.

$$\mathbf{B}(\mathcal{L}_1/\mathcal{K}) = \mathbf{B}(\mathcal{L}_2/\mathcal{K}). \tag{6}$$

Definition 5.3. Let $\mathcal{A}$ be a central simple algebra over $\mathcal{K}$ of finite dimension d^2 where d is a positive integer. A $\mathcal{K}$-subalgebra E of $\mathcal{A}$ with the same 1 that is a subfield is called a *strictly maximal subfield* if $[E : \mathcal{K}] = d$. (See [18, Sect. 13.1].)

Remark 5.4. It is known [18, Sect. 13.3] that if E is a strictly maximal subfield of a central simple $\mathcal{K}$-algebra $\mathcal{A}$ then E *splits* $\mathcal{A}$, i.e., the E-algebra $\mathcal{A} \otimes_{\mathcal{K}} E$ is isomorphic to a matrix algebra over E. In other words, $[\mathcal{A}] \in \mathbf{B}(E/\mathcal{K})$.

Proof of Lemma 2.7. We keep the notation and conventions of Remark 5.1. Let us put $\mathcal{A} := \mathrm{Mat}_m(D)$. Then $\mathcal{A}$ is a central simple $\mathbb{Q}$-algebra of dimension

$$4 \cdot m^2 = (2m)^2 = (n-1)^2$$

and therefore E is a *strictly maximal subfield* of the central simple $\mathbb{Q}$-algebra $\mathcal{A}$, because

$$[E : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = n - 1 = \sqrt{\dim_{\mathbb{Q}}(\mathcal{A})}.$$

This implies that $[\mathcal{A}] \in \mathbf{B}(E/\mathbb{Q})$. In light of (6), $[\mathcal{A}] \in \mathbf{B}(L/\mathbb{Q})$, because the fields E and L are isomorphic (recall that $L = \mathbb{Q}(\zeta_n)$). In other words,

$$i(\mathbb{Q}, L)_*[\mathcal{A}] = 0. \tag{7}$$

Now let us consider the central simple $\mathbb{Q}_p$-algebra

$$\mathcal{A}_p := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p = \mathrm{Mat}_m(D) \otimes_{\mathbb{Q}} \mathbb{Q}_p = \mathrm{Mat}_m(D_p)$$

where $D_p := D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a quaternion (division) algebra over $\mathbb{Q}_p$. This implies that $\mathcal{A}_p$ is *not* isomorphic to a matrix algebra over $\mathbb{Q}_p$ but $\mathcal{A}_p \otimes_{\mathbb{Q}_p} \mathcal{A}_p$ is isomorphic to a matrix algebra over $\mathbb{Q}_p$. In other words,

$$[\mathcal{A}_p] = i(\mathbb{Q}, \mathbb{Q}_p)_*[\mathcal{A}]$$

is an element of order 2 in $\mathrm{Br}(\mathbb{Q}_p)$. Let us prove that

$$[\mathcal{A}_p] \in \mathbf{B}(L_{\mathfrak{P}}/\mathbb{Q}_p) \tag{8}$$

where the field $L_{\mathfrak{P}}$ is defined in Remark 5.1. Indeed, recall that $L_{\mathfrak{P}}$ contains both fields $\mathbb{Q}_p$ and $L = \mathbb{Q}(\zeta_n)$, whose intersection contains $\mathbb{Q}$. By functoriality of Brauer groups (5),

$$i(\mathbb{Q}_p, L_{\mathfrak{P}})_* \circ i(\mathbb{Q}, \mathbb{Q}_p)_* = i(\mathbb{Q}, L_{\mathfrak{P}})_* = i(L, L_{\mathfrak{P}})_* \circ i(\mathbb{Q}, L)_*. \tag{9}$$

This implies that

$$i(\mathbb{Q}_p, L_{\mathfrak{P}})_*[\mathcal{A}_p] = i(\mathbb{Q}_p, L_{\mathfrak{P}})_* \circ (i(\mathbb{Q}, \mathbb{Q}_p)_*[\mathcal{A}]) = i(L, L_{\mathfrak{P}})_* \circ (i(\mathbb{Q}, L)_*[\mathcal{A}]) \,. \tag{10}$$

In light of (7), $i(\mathbb{Q}, L)[\mathcal{A}] = 0$. In light of (10), $i(\mathbb{Q}_p, L_{\mathfrak{P}})[\mathcal{A}_p] = 0$, which proves (8).

It follows that $\mathbf{B}(L_{\mathfrak{P}}/\mathbb{Q}_p)$ contains an element of order 2, namely $[\mathcal{A}_p]$. Since $L_{\mathfrak{P}}/\mathbb{Q}_p$ is a *cyclic* field extension (see Remark 5.1), the group $\mathbf{B}(L_{\mathfrak{P}}/\mathbb{Q}_p)$ is isomorphic to the quotient $\mathbb{Q}_p^*/\mathrm{N}_{L_{\mathfrak{P}}/\mathbb{Q}_p}(L^*)$ where

$$\mathrm{N}_{L_{\mathfrak{P}}/\mathbb{Q}_p} : L_{\mathfrak{P}}^* \to \mathbb{Q}_p^*$$

is the *norm map* attached to $L/\mathbb{Q}_p$ and $\mathrm{N}_{L_{\mathfrak{P}}/\mathbb{Q}_p}(L_{\mathfrak{P}}^*)$ is its image in $\mathbb{Q}_p^*$ [18, Sect. 15.1, Proposition **b**]. On the other hand, according to the *fundamental equality* in local class field theory [7, Sect. 7.1, p. 98], the index $\left[\mathbb{Q}_p^* : \mathrm{N}_{L_{\mathfrak{P}}/\mathbb{Q}_p}(L_{\mathfrak{P}}^*)\right]$ coincides with the degree $[L_{\mathfrak{P}} : \mathbb{Q}_p]$. [2] This means that the quotient $\mathbb{Q}_p^*/\mathrm{N}_{L_{\mathfrak{P}}/\mathbb{Q}_p}(L_{\mathfrak{P}}^*)$ is a finite group of order $[L_{\mathfrak{P}} : \mathbb{Q}_p]$. Since $\mathbb{Q}_p^*/\mathrm{N}_{L_{\mathfrak{P}}/\mathbb{Q}_p}(L_{\mathfrak{P}}^*)$ contains an element of order 2, the degree $[L_{\mathfrak{P}} : \mathbb{Q}_p]$ is an *even integer*. On the other hand, (2) tells us that $[L_{\mathfrak{P}} : \mathbb{Q}_p]$ coincides with the multiplicative order $\mathfrak{f}_p$ of the residue $p \bmod n \in (\mathbb{Z}/n\mathbb{Z})^*$. Hence, $\mathfrak{f}_p$ is even. This ends the proof. □

Acknowledgements

I am grateful to Alexei Skorobogatov and Umberto Zannier for their interest in this topic. My special thanks go to Ken Ribet and both referees for useful comments that helped to improve the exposition and simplify the arguments. I am grateful to Boris Kunyavskiĭ for help with references.

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

[2] Actually, we need only a special "elementary" case of the fundamental equality that deals with *unramified* extensions and is discussed in detail in [21, Ch. V, §2].

References

[1] B.J. Birch, *Cyclotomic Fields and Kummer Extensions*, Chapter III, p. 85–93. In: Algebraic Number Theory (J.W.S. Cassels and A. Frölich, eds), 2nd edition. London Mathematical Society, 2010.

[2] N. Bourbaki, Algebra II, Chapters 4–7. Springer-Verlag, Berlin Heidelberg New York, 2003.

[3] B. Conrad, *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem*. Enseign. Math. **52** (2006), 37–108.

[4] D.S. Dummit, *Solving solvable quintics*. Mathematics of Computation **57** (1991), 387–401.

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

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

[7] K. Iwasawa, Local class field theory. Oxford University Press, 1986.

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

[9] S. Lang, Abelian varieties, 2nd edition. Springer-Verlag, New York, 1983.

[10] S. Lang, Algebra, Revised Third Edition. Springer Science, New York, 2002.

[11] D. Masser and U. Zannier, *Abelian varieties isogenous to no Jacobians*. Ann. Math. **191** (2020), 635–674.

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

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

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

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

[16] E. Nart and N. Vila, *Equations of the type $X^n + aX + b$ with absolute Galois group S_n*. Rev. Univ. Santander No **2**, part 2 (1979), 821–825.

[17] H. Osada, *The Galois groups of the polynomials $X^n + aX^l + b$*. J. Number Theory **25** (1987), no. 2, 230–238.

[18] R. Pierce, Associative algebras. Graduate Texts in Mathematics **88**, Springer-Verlag, New York Heidelberg Berlin, 1982.

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

[20] E.S. Selmer, *On the irreducibility of certain trinomials*. Math. Scand. **4** (1956), 287–302.

[21] J.-P. Serre, Corps Locaux, troisiéme edition, corrigée. Hermann, Paris, 1968.

[22] J.-P. Serre, *Complex multiplication*, Chapter XIII, p. 292–296. In Algebraic Number Theory (J.W.S. Cassels, A. Fröhlich, eds.), 2nd edition. London Mathematical Society, London, 2010.

[23] D. Shanks, *The simplest cubic fields*. Mathematics of Computation **28** (1974), 1137–1152.

[24] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions. Princeton University Press, Princeton, NJ, 1994.

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

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

[27] J.H. Silverman, The Arithmetic of Elliptic Curves, 2nd edition. Springer Science, New York, 2009.

[28] J.H. Silverman, Advanced topics in the Arithmetic of Elliptic Curves. Springer-Verlag, New York, 1994.

[29] J.T. Tate, *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2** (1966), 134–144.

[30] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132.

[31] 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.

[32] Yu. G. Zarhin, *Homomorphisms of hyperelliptic jacobians*. Trudy Math. Inst. Steklova **241** (2003), 79–92; Proc. Steklov Institute of Mathematics **241** (2003), 90–104.

[33] Yu. G. Zarhin, *Non-isogenous superelliptic jacobians*. Math. Z. **253** (2006), 537–554.

[34] Yu. G. Zarhin, *Superelliptic jacobians*, p. 363–390. In: Diophantine Geometry proceedings (U. Zannier, ed). Edizioni Della Normale, Pisa 2007.

Department of Mathematics, Pennsylvania State University
University Park, PA 16802, USA
Current address:
Max-Planck Institut für Mathematik
Vivatgasse 7, 53111 Bonn, Germany
E-mail address: zarhin@math.psu.edu

Received May 7, 2021
Accepted February 15, 2022