HOMOMORPHISMS OF HYPERELLIPTIC JACOBIANS

YU. G. ZARHIN

1. Definitions, notations, statements

Let K be a field. Let us fix its algebraic closure K_a and denote by $\mathrm{Gal}(K)$ the absolute Galois group $\mathrm{Aut}(K_a/K)$ of K. If X is an abelian variety over K_a then we write $\mathrm{End}(X)$ for the ring of all its K_a-endomorphisms. If Y is (may be another) abelian variety over K_a then we write $\mathrm{Hom}(X,Y)$ for the group of all K_a-homomorphisms from X to Y. It is well-known that $\mathrm{Hom}(X,Y) = 0$ if and only if $\mathrm{Hom}(Y,X) = 0$. One may easily check that if $\mathrm{End}(X) = \mathbf{Z}$ and $\dim(X) \geq \dim(Y)$ then $\mathrm{Hom}(X,Y) = 0$ if and only if X and Y are *not* isogenous over K_a.

Let $f(x) \in K[x]$ be a polynomial of degree $n \geq 3$ without multiple roots. We write $\mathfrak{R}_f \subset K_a$ for the set of its roots, $K(\mathfrak{R}_f) \subset K_a$ for the splitting field of f and $\mathrm{Gal}(f) = \mathrm{Aut}(K(\mathfrak{R}_f)/K) = \mathrm{Gal}(K(\mathfrak{R}_f)/K)$ for the Galois group of f. It is well-known that $\mathfrak{R}_f$ consists of $n = \deg(f)$ elements. The group $\mathrm{Gal}(f)$ 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 $\mathfrak{R}_f$. Clearly, every ordering of $\mathfrak{R}_f$ provides an isomorphism between $\mathrm{Perm}(\mathfrak{R}_f)$ and the full symmetric group $\mathbf{S}_n$ which makes $\mathrm{Gal}(f)$ a certain subgroup of $\mathbf{S}_n$. (It is well-known that this permutation subgroup is transitive if and only if f is irreducible over K.)

Let us assume that $\mathrm{char}(K) \neq 2$ and consider the hyperelliptic curve

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

defined over K. Its genus $g = g(C_f)$ equals $(n-1)/2$ if n is odd and $(n-2)/2$ if n is even. Let $J(C_f)$ be the jacobian of C_f; it is a g-dimensional abelian variety over K_a that is defined over K.

In his previous papers [20, 22, 23] the author proved the following assertion.

Theorem 1.1. *Let K be a field of characteristic different from 2. Let $n \geq 5$ be a positive integer. Let $f(x) \in K[x]$ be an irreducible polynomial of degree $n \geq 5$. Assume also that if $\mathrm{char}(K) > 0$ then $n \geq 9$ and $f(x)$ has no multiple roots. Suppose that the Galois group of $f(x)$ coincides either with the full symmetric group $\mathbf{S}_n$ or with the alternating group $\mathbf{A}_n$.*

Then $\mathrm{End}(J(C_f)) = \mathbf{Z}$.

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

Theorem 1.2 (Main Theorem)**.** *Let K be a field of characteristic different from 2 and K_a its algebraic closure. Let $f(x), h(x) \in K[x]$ be irreducible polynomials of degree $n \geq 3$ and $m \geq 3$ respectively. Suppose that the splitting fields of f and h are linearly disjoint over K. Assume also that if* $\mathrm{char}(K) > 0$ *then $n = \deg(f) \geq 9$ and $f(x)$ and $h(x)$ have no multiple roots.*
  Suppose that the following conditions hold:

  (i) $\mathrm{Gal}(h) = \mathbf{A}_m$ *or* SS_m.
  (ii) *Either* $\mathrm{Gal}(f) = \mathbf{S}_n$ *or* $\mathrm{Gal}(f) = \mathbf{A}_n$ *and* $n \geq 5$.

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

  We prove Theorem 1.2 in §2.

Example 1.3. Let $n \geq 3$ be a positive integer. It is well-known [16, p. 139] that the Galois group of the polynomial $x^n - x - t$ over the field of rational functions $\mathbf{Q}(t)$ coincides with the full symmetric group $\mathbf{S}_n$. It follows from Hilbert's irreducibility theorem that there exists an *infinite* set of rational numbers $S \subset \mathbf{Q}$ such that for each $r \in S$ the Galois group $\mathrm{Gal}(u_r)$ of the polynomial
$$u_r(x) = x^n - x - r \in \mathbf{Q}[x]$$
coincides with $\mathbf{S}_n$ and for *distinct* $r, k \in S$ the splitting fields of u_r and u_k are linearly disjoint over $\mathbf{Q}$. Let us consider the jacobians $J(C_{u_r})$ and $J(C_{u_k})$ of the hyperelliptic curves $C_{u_r} : y^2 = u_r(x)$ and $C_{u_k} : y^2 = u_k(x)$ defined over $\mathbf{Q}$. Notice that if $n < 5$ then $J(C_{u_r})$ and $J(C_{u_k})$ are elliptic curves. Applying Theorems 1.2 and 1.1 to u_r and u_k, we obtain that the jacobians $J(C_{u_r})$ are $J(C_{u_k})$ absolutely simple and mutually non-isogenous over $\bar{\mathbf{Q}}$ (and therefore over $\mathbf{C}$) for all $n \geq 3$. In particular, for each positive integer g the set of isogeny classes of absolutely simple g-dimensional abelian varieties over $\mathbf{Q}$ is infinite. (This assertion is well-known in the case of elliptic curves.) It also follows from Theorem 1.1 that for each positive integer $g > 1$ the set of isogeny classes of absolutely simple g-dimensional abelian varieties over $\mathbf{Q}$ without nontrivial endomorphisms over $\mathbf{C}$ is infinite. (The similar assertion for elliptic curves is also well-known: it suffices to take for each prime p an elliptic curve with j-invariant $1/p$.)

Corollary 1.4. *Let K be a field of characteristic different from 2 and K_a its algebraic closure. Let $f(x), h(x) \in K[x]$ be irreducible polynomials of degree $n \geq 5$ and $m \geq 3$ respectively. Assume also that if* $\mathrm{char}(K) > 0$ *then $n = \deg(f) \geq 9$ and both polynomials $f(x)$ and $h(x)$ have no multiple roots. Suppose that the following conditions hold:*

  (i) $\mathrm{Gal}(h) = \mathbf{A}_m$ *or* SS_m.
  (ii) $\mathrm{Gal}(f) = \mathbf{S}_n$ *or* $\mathrm{Gal}(f) = \mathbf{A}_n$.
  (iii) *Either* $n \neq m$ *or* $\mathrm{Gal}(f) = \mathbf{S}_n$ *and* $\mathrm{Gal}(h) = \mathbf{A}_m$.

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

Corollary 1.5. *Let K be a field of characteristic different from 2 and K_a its algebraic closure. Let $n \geq 5$ be a positive integer different from 6. Let $f(x), h(x) \in K[x]$ be irreducible polynomials of degree n. Assume also that if $\mathrm{char}(K) > 0$ then $n \geq 9$ and both polynomials $f(x)$ and $h(x)$ have no multiple roots. Suppose that the following conditions hold:*

(i) $\mathrm{Gal}(h) = \mathbf{A}_n$ *or* $\mathbf{S}_n$.
(ii) $\mathrm{Gal}(f) = \mathbf{S}_n$ *or* $\mathrm{Gal}(f) = \mathbf{A}_n$.
(iii) *Let us put $K_f := K[x]/fK[x], K_h := K[x]/hK[x]$. Then the field extensions K_f/K and K_h/K are not isomorphic.*

Then

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

We will prove Corollaries 1.4 and 1.5 in §4.

2. PROOF OF MAIN THEOREM

Let d be a positive integer that is not divisible by $\mathrm{char}(K)$. Let X be an abelian variety of positive dimension defined over K. We write X_d for the kernel of multiplication by d in $X(K_a)$. It is known [14] that the commutative group X_d is a free $\mathbf{Z}/d\mathbf{Z}$-module of rank $2\mathrm{dim}(X)$. Clearly, X_d is a Galois submodule in $X(K_a)$. We write

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

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

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

Clearly, $\tilde{G}_{d,X}$ coincides with the Galois group of the field extension $K(X_d)/K$ where $K(X_d)$ is the field of definition of all points of order dividing d on X. In particular, if $\ell \neq \mathrm{char}(K)$ is a prime then X_ℓ is a $2\mathrm{dim}(X)$-dimensional vector space over the prime field $\mathbf{F}_\ell = \mathbf{Z}/\ell\mathbf{Z}$ and the inclusion $\tilde{G}_{\ell,X} \subset \mathrm{Aut}_{\mathbf{F}_\ell}(X_\ell)$ defines a faithful linear representation of the group $\tilde{G}_{\ell,X}$ in the vector space X_ℓ. We will deduce Theorem 1.2 from the following auxiliary statement which is of some independent interest.

Theorem 2.1. *Let ℓ be a prime, K a field of characteristic different from ℓ, X and Y are abelian varieties of positive dimension defined over K. Suppose that the following conditions hold:*

(i) *The extensions $K(X_\ell)$ and $K(Y_\ell)$ are linearly disjoint over K.*
(ii) *The natural representation of the group $\tilde{G}_{\ell,X}$ in X_ℓ is absolutely irreducible.*
(iii) *The natural representation of the group $\tilde{G}_{\ell,Y}$ in Y_ℓ is irreducible.*

Then either

$$\mathrm{Hom}(X, Y) = 0, \quad \mathrm{Hom}(Y, X) = 0$$

or $\mathrm{char}(K) > 0$ and both abelian varieties X and Y are supersingular.

We will prove Theorem 2.1 in §3.

In fact, we are going to prove not Theorem 2.1 but its certain generalization. In order to state this generalization, we need to introduce definitions of *nice* and *very nice* polynomials. But first, let us recall some standard notations [3, §2.8]. Hereafter, $\mathbf{F}_q$ denotes the q-element finite field of characteristic p, $\mathrm{GL}(d,q) := \mathrm{GL}(d,\mathbf{F}_q)$ denotes the group of invertible linear transformations of the d-dimensional vector space $\mathbf{F}_q^d$, $\mathrm{SL}(d,q) := \mathrm{SL}(d,\mathbf{F}_q)$ its subgroup of all matrices with determinant 1 and $\mathrm{PGL}(d,q) = \mathrm{PGL}(d,\mathbf{F}_q)$ and $\mathrm{Ł}_d(q) = \mathrm{PSL}(d,q) = \mathrm{PSL}(d,\mathbf{F}_q)$ are the corresponding quotients with respect the subgroups of scalar matrices, viewed as transformation groups of the projective space $\mathbf{P}^{d-1}(\mathbf{F}_q)$. In addition, $\mathrm{AGL}(d,q) := \mathrm{AGL}(d,\mathbf{F}_q)$ is the group of all affine transformations of $\mathbf{F}_q^d$, which is a semi-direct product of $\mathrm{GL}(d,q)$ and the group $\mathbf{F}_q^d$ of all translations. We write $\mathrm{Fr} : \mathbf{F}_q^d \to \mathbf{F}_q^d$ for the Frobenius automorphism

$$(a_1, \cdots, a_d) \mapsto (a_1^p, \cdots, a_d^p).$$

We write $\mathrm{\Gamma L}(d,q)$, $\mathrm{\Sigma L}(d,q)$ and $\mathbf{A}\mathrm{\Sigma L}(d,q)$ for the transformation groups of $\mathbf{F}_q^d$, generated by Fr and $\mathrm{GL}(d,q), \mathrm{SL}(d,q)$ and $\mathrm{AGL}(d,q)$ respectively. We write $\mathbf{P\Gamma L}(d,q)$ and $\mathbf{P\Sigma L}(d,q)$ for the transformation groups of $\mathbf{P}^{d-1}(\mathbf{F}_q)$ induced by $\mathrm{\Gamma L}(d,q)$ and $\mathrm{\Sigma L}(d,q)$ respectively. (In other words, $\mathbf{P\Gamma L}(d,q)$ and $\mathbf{P\Sigma L}(d,q)$ are the quotients of $\mathrm{\Gamma L}(d,q)$ and $\mathrm{\Sigma L}(d,q)$ respectively with respect to the corresponding subgroups of scalar matrices.)

Let $f(x) \in K[x]$ be a separable irreducible polynomial of degree $n \geq 3$. We say that f is *very nice* if one of the following conditions holds:

- (s) $\mathrm{Gal}(f) = \mathbf{S}_n$.
- (a) $\mathrm{Gal}(f) = \mathbf{A}_n$ and $n \geq 5$.
- (m) $n = 11$ or 12 and $\mathrm{Gal}(f)$ is the corresponding small Mathieu group M_n acting 4(or 5-)transitivelyon $\mathfrak{R}_f$.
- (l11) $n = 11$ and $\mathrm{Gal}(f) = \mathrm{Ł}_2(11) = \mathrm{PSL}_2(\mathbf{F}_{11})$ acts doubly transitively on $\mathfrak{R}_f$.
- (m12) $n = 12$ and $\mathrm{Gal}(f) = \mathrm{M}_{11}$ acts 3-transitively on $\mathfrak{R}_f$.
- (aff) There exist an odd prime p, its positive integral power q and a positive integer d such that $n = p^d > 3$ and one may identify $\mathfrak{R}_f$ with $\mathbf{F}_q^d$ in such a way that $\mathrm{Gal}(f)$ becomes 2 *or* 3-*transitive* subgroup of $\mathrm{AGL}(d,q)$ that contains the subgroup $\mathbf{F}_q^d$ of all translations.
- (p) There exist an odd prime p, its positive integral power q and a positive integer $d \geq 3$ such that $n = \frac{q^d-1}{q-1}$ and one may identify $\mathfrak{R}_f$ with $\mathbf{P}^{d-1}(\mathbf{F}_q)$ in such a way that $\mathrm{Gal}(f)$ becomes a subgroup of $\mathbf{P\Gamma L}(d,q)$ that contains $\mathrm{PSL}(d,q)$.
- (p1) There exist an odd prime p and its positive integral power q such that $n = q+1$ and one may identify $\mathfrak{R}_f$ with the projective line $\mathbf{P}^1(\mathbf{F}_q)$ in such a way that $\mathrm{Gal}(f)$ becomes a 3-transitive subgroup of $\mathbf{P\Gamma L}(2,q)$.

(p2) There exists a positive integer $d \geq 2$ such that $q := 2^d, n = q + 1$ and one may identify $\mathfrak{R}_f$ with the projective line $\mathbf{P}^1(\mathbf{F}_q)$ in such a way that $\mathrm{Gal}(f)$ becomes a subgroup of $\mathbf{P\Gamma L}(d, q)$ that contains $\mathrm{PSL}(2, q)$.

(u3) There exists a positive integer $d \geq 2$ such that $q := 2^d, n = q^3 + 1$, and one may identify $\mathfrak{R}_f$ with the set of isotropic lines (Hermitian curve) in $\mathbf{F}_{q^2}^3$ with respect to a certain non-degenerate Hermitian form in such a way that $\mathrm{Gal}(f)$ becomes a group that contains the corresponding projective special unitary group $\mathrm{U}_3(q) := \mathrm{PSU}(3, q) = \mathrm{PSU}(3, \mathbf{F}_{q^2})$ and $\mathrm{U}_3(q)$ acts doubly transitively on $\mathfrak{R}_f$.

(sz) There exists a positive integer d such that $q := 2^{2d+1}, n = q^2 + 1$ and $\mathrm{Gal}(f)$ contains a subgroup isomorphic to the Suzuki group $\mathrm{Sz}(q)$ and $\mathrm{Sz}(q)$ acts doubly transitively on $\mathfrak{R}_f$.

A polynomial f is called *nice* if either it is very nice or one of the following conditions holds:

(a3) $n = 3$ and $\mathrm{Gal}(f) = \mathbf{A}_3$.

(a4) $n = 4$ and $\mathrm{Gal}(f) = \mathbf{A}_4$.

(p3) There exist an odd prime p and its positive integral power q such that $n = q + 1$, and one may identify $\mathfrak{R}_f$ with the projective line $\mathbf{P}^1(\mathbf{F}_q)$ in such a way that $\mathrm{Gal}(f)$ becomes a doubly transitive subgroup of $\mathbf{P\Gamma L}(2, q)$. In addition, q must be congruent either to 3 or to 5 modulo 8.

Remark 2.2. The doubly transitive action of the Suzuki groups $\mathrm{Sz}(q)$ (the case (sz)) is described explicitly on pp. 184–187 of [5]; see [21] concerning the relations to hyperelliptic jacobians. Concerning the doubly transitive action of U_3 on the Hermitian curve (the case (u3)) see [4, Kap. II, Satz 4.12], [3, pp. 248–250]; the relations with hyperelliptic jacobians are discussed in [24].

In order to explain what nice polynomials are good for, let us recall the definition of the *heart* of the permutational action of $\mathrm{Gal}(f)$ on $\mathfrak{R}_f$ ([12], [21]).

Let $\mathfrak{R} = \mathfrak{R}_f = \{a_1, \ldots, a_n\} \subset K_a$ be the set of all roots of f. We may view $\mathbf{S}_n$ as the group of all permutations of $\mathfrak{R}$. The Galois group $G = \mathrm{Gal}(f)$ of f permutes the roots and therefore becomes a subgroup of $\mathbf{S}_n$. The action of G on $\mathfrak{R}$ defines the standard *permutational* representation in the n-dimensional $\mathbf{F}_2$-vector space $\mathbf{F}_2^{\mathfrak{R}}$ of all functions $\psi : R \to \mathbf{F}_2$. This representation is not irreducible. Indeed, the "line" of constant functions $\mathbf{F}_2 \cdot 1$ and the hyperplane $(\mathbf{F}_2^{\mathfrak{R}})^0 := \{\psi \mid \sum_{i=1}^n \psi(a_i) = 0\}$ are G-invariant subspaces in $\mathbf{F}_2^{\mathfrak{R}}$. If n is odd then one calls $(\mathbf{F}_2^{\mathfrak{R}})^0$ the *heart* of the permutational action of $G = \mathrm{Gal}(f)$ on $\mathfrak{R} = \mathfrak{R}_f$ over $\mathbf{F}_2$ and denotes it by $Q_{\mathfrak{R}} = Q_{\mathfrak{R}_f}$. If n is even then $(\mathbf{F}_2^{\mathfrak{R}})^0$ contains $\mathbf{F}_2 \cdot 1$ and we obtain the natural representation of $G = \mathrm{Gal}(f)$ in the $(n-2)$-dimensional $\mathbf{F}_2$-vector quotient-space

$$(\mathbf{F}_2^B)^{00} := (\mathbf{F}_2^{\mathfrak{R}})^0/(\mathbf{F}_2 \cdot 1).$$

In this case $(\mathbf{F}_2^B)^{00}$ is also called the *heart* of the permutational action of $G = \mathrm{Gal}(f)$ on $\mathfrak{R} = \mathfrak{R}_f$ over $\mathbf{F}_2$ and denoted by $Q_{\mathfrak{R}} = Q_{\mathfrak{R}_f}$.

It is known [7] that if n is odd and the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}_f}$ is absolutely simple then $\mathrm{Gal}(f)$ acts on $\mathfrak{R}_f$ doubly transitively.

Remark 2.3. If a polynomial $f(x)$ is nice then:
  (i) Either $(n, \mathrm{Gal}(f)) = (3, \mathbf{A}_3)$ or $\mathrm{Gal}(f)$ acts doubly transitively on $\mathfrak{R}_f$;
  (ii) The $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}_f}$ is simple. In addition, $Q_{\mathfrak{R}_f}$ is absolutely simple if and only if $f(x)$ is *very* nice. In the case of doubly transitive $\mathrm{Gal}(f)$ this assertion follows immediately from results of [12, 9]. The remaining case $n = 3, \mathrm{Gal}(f) = \mathbf{A}_3$ is easy. (See also [21, 24].)

Remark 2.4. Let us assume that a permutation group $\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$ is isomorphic to one of the *known doubly transitive* permutation groups [3, §7.7]. Then $f(x)$ is nice if and only if the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}_f}$ is simple. This assertion follows easily from results of [12, 9].

Now we are ready to state the promised generalization of Main Theorem.

Theorem 2.5. *Let K be a field of characteristic different from 2 and K_a its algebraic closure. Let $f(x), h(x) \in K[x]$ be irreducible polynomials without multiple roots of degree $n \geq 3$ and $m \geq 3$ respectively. Suppose that the splitting fields of f and h are linearly disjoint over K. Suppose that $f(x)$ is very nice and $h(x)$ is nice.*

Then either

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

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

Proof of Theorem 2.5. The canonical surjection $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(f)$ defines on the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}_f}$ the natural structure of $\mathrm{Gal}(K)$-module. It is well-known that the $\mathrm{Gal}(K)$-modules $Q_{\mathfrak{R}_f}$ and $J(C_f)_2$ are canonically isomorphic (see, for instance, [13], [11] or [21]). This implies, in particular, in light of Remark 2.3, that the $\tilde{G}_{2,J(C_f)}$-module is absolutely simple. Similarly, the canonical surjection $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(h)$ provides the $\mathrm{Gal}(h)$-module $Q_{\mathfrak{R}_h}$ with natural structure of the $\mathrm{Gal}(K)$-module and the $\mathrm{Gal}(K)$-modules $Q_{\mathfrak{R}_h}$ and $J(C_h)_2$ are canonically isomorphic. Now it follows from Remark 2.3 that the $\tilde{G}_{2,J(C_h)}$-module is simple. We have

$$K(J(C_f)_2) \subset K(\mathfrak{R}_f), \quad K(J(C_h)_2) \subset K(\mathfrak{R}_h).$$

Since the field extensions $K(\mathfrak{R}_f)/K$ and $K(\mathfrak{R}_h)/K$ are linearly disjoint, their subextensions $K(J(C_f)_2)/K$ and $K(J(C_h)_2)/K$ are also linearly disjoint. One has only to apply Theorem 2.1 to $\ell = 2, X = J(C_f), Y = J(C_h)$. $\square$

Remark 2.6. In fact, if $n \neq 4$ (respectfully $m \neq 4$) then the $\mathrm{Gal}(f)$-module $Q_{\mathfrak{R}_f}$ is faithful and $K(J(C_f)_2) = K(\mathfrak{R}_f)$ (respectfully the $\mathrm{Gal}(h)$-module $Q_{\mathfrak{R}_h}$ is faithful and $K(J(C_h)_2) = K(\mathfrak{R}_h)$).

Proof of Theorem 1.2. It follows from Theorem 2.5 that if there exists a non-zero homomorphism between $J(C_f)$ and $J(C_h)$ then $\mathrm{char}(K) > 0$ and both jacobians are supersingular. However if $\mathrm{char}(K) > 0$ then $n \geq 9$ and, thanks to Theorem 1.1, $\mathrm{End}(J(C_f)) = \mathbf{Z}$ and therefore $J(C_f)$ is *not* supersingular. $\square$

3. Homomorphisms of abelian varieties

In order to prove Theorem 2.1, we need the following elementary statement that is well known when the ground field is algebraically closed and has characteristic zero ([18, §3.2]; see also theorem 10.38 of [2]).

Lemma 3.1. *Let F be a field. Let H_1 and H_2 be groups. Let $\tau_1 : H_1 \to \mathrm{Aut}_F(W_1)$ be an irreducible finite-dimensional representation of H_1 over F and $\tau_2 : H_2 \to \mathrm{Aut}_F(W_2)$ be an absolutely irreducible finite-dimensional representation of H_2 over F. Then the natural linear representation*

$$\tau_1^* \otimes \tau_2 : H_1 \times H_2 \to \mathrm{Aut}_F(\mathrm{Hom}_F(W_1, W_2))$$

of the group $H_1 \times H_2$ in the F-vector space $\mathrm{Hom}_F(W_1, W_2)$ is irreducible.

Remark 3.2. Clearly, the representations of $H_1 \times H_2$ in $\mathrm{Hom}_F(W_1, W_2)$ and $\mathrm{Hom}_F(W_2, W_1)$ are mutually dual. Therefore the irreducibility of $\mathrm{Hom}_F(W_1, W_2)$ implies the irreducibility of $\mathrm{Hom}_F(W_2, W_1)$.

We will prove Lemma 3.1 at the end of this Section.

Proof of Theorem 2.1. First, notice that the natural representation

$$\mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbf{F}_\ell}(\mathrm{Hom}_{\mathbf{F}_\ell}(Y_\ell, X_\ell))$$

is irreducible. Indeed, let us denote this representation by τ and let us put

$$F = \mathbf{F}_\ell, H_1 = \tilde{G}_{\ell,Y}, W_1 = Y_\ell, H_2 = \tilde{G}_{\ell,X}, W_2 = X_\ell.$$

Denote by

$$\tau_1 : H_1 = \tilde{G}_{\ell,Y} \subset \mathrm{Aut}_{\mathbf{F}_\ell}(Y_\ell) = \mathrm{Aut}_{\mathbf{F}_\ell}(W_1)$$

and

$$\tau_2 : H_2 = \tilde{G}_{\ell,X} \subset \mathrm{Aut}_{\mathbf{F}_\ell}(X_\ell) = \mathrm{Aut}_{\mathbf{F}_\ell}(W_2)$$

the corresponding inclusion maps.

It follows from Lemma 3.1 that the linear representation

$$\tau_1^* \otimes \tau_2 : \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K) \to \mathrm{Aut}_{\mathbf{F}_\ell}(\mathrm{Hom}_{\mathbf{F}_\ell}(Y_\ell, X_\ell))$$

is irreducible.

One may easily check that the homomorphism τ, which defines the structure of $\mathrm{Gal}(K)$-module on $\mathrm{Hom}_{\mathbf{F}_\ell}(Y_\ell, X_\ell)$, coincides with the composition of the natural surjection $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K(X_\ell, Y_\ell)/K)$, the natural embedding

$$\mathrm{Gal}(K(X_\ell, Y_\ell)/K) \hookrightarrow \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K)$$

and

$$\tau_1^* \otimes \tau_2 : \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K) \to \mathrm{Aut}_{\mathbf{F}_\ell}(\mathrm{Hom}_{\mathbf{F}_\ell}(Y_\ell, X_\ell)).$$

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

$$\mathrm{Gal}(K(X_\ell, Y_\ell)/K) = \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K).$$

This implies that τ is the composition of *surjective* $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K)$ and $\tau_1^* \otimes \tau_2$. Since the representation

$$\tau_1^* \otimes \tau_2 : \mathrm{Gal}(K(Y_\ell)/K) \times \mathrm{Gal}(K(X_\ell)/K) \to \mathrm{Aut}_{\mathbf{F}_\ell}(\mathrm{Hom}_{\mathbf{F}_\ell}(Y_\ell, X_\ell))$$

is irreducible, the representation

$$\tau : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbf{F}_\ell}(\mathrm{Hom}_{\mathbf{F}_\ell}(Y_\ell, X_\ell))$$

is also irreducible.

Second, let $T_\ell(X)$ and $T_\ell(Y)$ be the Tate $\mathbf{Z}_\ell$-modules of abelian varieties X and Y respectively [14]. Recall that $T_\ell(X)$ and $T_\ell(Y)$ are free $\mathbf{Z}_\ell$-modules of rank $2\dim(X)$ and $2\dim(Y)$ respectively. There are also natural continuous homomorphisms

$$\rho_{\ell,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X)), \quad \rho_{\ell,Y} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(Y)).$$

There are also natural homomorphisms

$$X_\ell = T_\ell(X)/\ell T_\ell(X), Y_\ell = T_\ell(Y)/\ell T_\ell(Y),$$

which are isomorphisms of Galois modules. So one may view $\tilde{\rho}_{\ell,X}$ as the reduction of $\rho_{\ell,X}$ modulo ℓ and $\tilde{\rho}_{\ell,Y}$ as the reduction of $\rho_{\ell,Y}$ modulo ℓ. It is also convenient to consider the Tate $\mathbf{Q}_\ell$-modules $V_\ell(X) = T_\ell(X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ and $V_\ell(Y) = T_\ell(Y) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$, which are $\mathbf{Q}_\ell$-vector spaces of dimension $2\dim(X)$ and $2\dim(Y)$ respectively. The groups $T_\ell(X)$ and $T_\ell(Y)$ are naturally identified with the $\mathbf{Z}_\ell$-lattices in $V_\ell(X)$ and $V_\ell(Y)$ respectively and the inclusions

$$\mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X)) \subset \mathrm{Aut}_{\mathbf{Q}_\ell}(V_\ell(X)), \quad \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(Y)) \subset \mathrm{Aut}_{\mathbf{Q}_\ell}(V_\ell(Y))$$

allow us to consider $V_\ell(X)$ and $V_\ell(Y)$ as representations of $\mathrm{Gal}(K)$ over $\mathbf{Q}_\ell$.

Third, I claim that the natural representation of $\mathrm{Gal}(K)$ in $\mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell(X), V_\ell(Y))$ over $\mathbf{Q}_\ell$ is irreducible. Indeed, the $\mathbf{Z}_\ell$-module $\mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell(X), T_\ell(Y))$ is a $\mathrm{Gal}(K)$-invariant $\mathbf{Z}_\ell$-lattice in $\mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell(Y), V_\ell(X))$. On the other hand, the reduction of this lattice modulo ℓ coincides with

$$\mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell(Y), T_\ell(X)) \otimes \mathbf{Z}/\ell\mathbf{Z} = \mathrm{Hom}_{\mathbf{F}_\ell}(T_\ell(Y)/\ell T_\ell(Y), T_\ell(X)/\ell T_\ell(X)) = \mathrm{Hom}_{\mathbf{F}_\ell}(Y_\ell, X_\ell).$$

But we just established the simplicity of the $\mathrm{Gal}(K)$-module $\mathrm{Hom}_{\mathbf{F}_\ell}(Y_\ell, X_\ell)$. It follows easily that the $\mathrm{Gal}(K)$-module $\mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell(X), V_\ell(Y))$ is simple (see, for instance, exercise 2 in §15.2 of Serre's book [18]).

Fourth, notice that there is a natural embedding ([14], §19)

$$\mathrm{Hom}(Y, X) \otimes \mathbf{Q}_\ell \subset \mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell(X), V_\ell(Y)),$$

whose image is a $\mathrm{Gal}(K)$-invariant subspace. The irreducibility of $\mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell(X), V_\ell(Y))$ implies that either

$$\mathrm{Hom}(Y, X) \otimes \mathbf{Q}_\ell = \mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell(X), V_\ell(Y))$$

or $\mathrm{Hom}(Y, X) \otimes \mathbf{Q}_\ell = 0$. Since $\mathrm{Hom}(Y, X)$ is a free commutative group of finite rank, either $\mathrm{Hom}(Y, X) = 0$ or the rank of $\mathrm{Hom}(Y, X)$ equals $4 \cdot \dim(X) \cdot \dim(Y)$. In order to finish the proof, we need the following proposition.

Proposition 3.3. *Let A and B are abelian varieties of positive dimension over an algebraically closed field $\mathcal{K}$. Suppose that the rank of the group $\mathrm{Hom}(A, B)$ equals $4 \cdot \dim(A) \cdot \dim(B)$. Then $\mathrm{char}(\mathcal{K}) > 0$ and both A and B are supersingular.*

Proof of Proposition 3.3. The case $A = B$ was treated in lemma 3.1 of [20].

Replacing A and B by isogenous abelian varieties, we may assume that they split into products

$$A = \prod_i A_i, \quad B = \prod_j B_j$$

of simple abelian varieties A_i and B_j respectively. Since

$$\dim(A) = \sum_i \dim(A_i), \dim(B) = \sum_j \dim(B_j), \mathrm{Hom}(A, B) = \prod_{i,j} \mathrm{Hom}(A_i, B_j),$$

and the rank of the free commutative group $\mathrm{Hom}(A_i, B_j)$ does not exceed $4 \cdot \dim(A_i) \cdot \dim(B_j)$ ([14], §19, corollary 1 to theorem 3), the rank of $\mathrm{Hom}(A_i, B_j)$ equals $4 \cdot \dim(A_i) \cdot \dim(B_j)$ for all i and j. Since A_i and B_j are simple, they are isogenous. This implies that $\dim(A_i) = \dim(B_j)$ and the rank of each of the free commutative group (with respect to addition) $\mathrm{End}(A_i)$ and $\mathrm{End}(B_j)$ equals

$$4 \cdot \dim(A_i) \cdot \dim(B_j) = 4 \cdot \dim(A_i)^2 = 4 \cdot \dim(B_j)^2.$$

Applying lemma 3.1 of [20] to each A_i and B_j, we conclude that $\mathrm{char}(\mathcal{K}) > 0$ and all A_i and B_j are supersingular. It follows easily that A and B are also supersingular. $\square$

End of Proof of Theorem 2.1. Applying Proposition 3.3 to $A = Y$ and $B = X$, we conclude that $\mathrm{char}(K) > 0$ and X and Y are supersingular. $\square$

Proof of Lemma 3.1. Throughout the proof all the tensor products are taken over F. First, replacing the H_1-module W_1 by its dual $W_1^* = \mathrm{Hom}_F(W_1, F)$, we reduce the problem to the assertion about the irreducibility of the tensor product

$$\tau_1 \otimes \tau_2 : H_1 \times H_2 \to \mathrm{Aut}_F(W_1 \otimes W_2).$$

Since the H_2-module W_2 is absolutely simple, the corresponding F-algebra homomorphism

$$F[H_2] \to \mathrm{End}_F(W_2)$$

(induced by τ_2) is surjective. Here $F[H_2]$ is the group algebra of H_2.

Let us denote by D the endomorphism ring of the $F[H_1]$-module W_1. Since W_1 is simple, D is a division algebra, whose center contains F. Clearly, the F-dimension of D is finite and W_2 is a free D-module of finite rank. It follows from Jacobson's density theorem that the image of the (induced by τ_2) F-algebra homomorphism

$$F[H_1] \to \mathrm{End}_F(W_1)$$

coincide with $\mathrm{End}_D(W_1)$. Here $F[H_1]$ is the group algebra of H_1. There is the natural structure of the free $D \otimes F = D$-module of finite rank on $W_1 \otimes W_2$. Clearly, the $\mathrm{End}_D(W_1 \otimes W_2)$-module $W_1 \otimes W_2$ is simple.

It follows that the image of the (induced by $\tau_1 \otimes \tau_2$) F-algebra homomorphism

$$F[H_1 \times H_2] = F[H_1] \otimes F[H_2] \to \mathrm{End}_F(W_1 \otimes W_2)$$

coincides with $\mathrm{End}_D(W_1) \otimes \mathrm{End}_F(W_2)$. Applying lemma 10.37 on p. 252 of [2], we conclude that

$$\mathrm{End}_D(W_1) \otimes \mathrm{End}_F(W_2) = \mathrm{End}_{D \otimes F}(W_1 \otimes W_2).$$

Therefore the image of the group algebra $F[H_1 \times H_2]$ in $\mathrm{End}_F(W_1 \otimes W_2)$ coincides with

$$\mathrm{End}_{D \otimes F}(W_1 \otimes W_2) = \mathrm{End}_D(W_1 \otimes W_2).$$

Now the simplicity of the $\mathrm{End}_D(W_1 \otimes W_2)$-module $W_1 \otimes W_2$ implies the simplicity of the $F[H_1 \times H_2]$-module $W_1 \otimes W_2$. $\square$

4. Proof of Corollaries 1.4 and 1.5

We start with the following useful definition.

Definition 4.1. Finite groups G_1 and G_2 are called *disjoint* if they do not have isomorphic quotients except the trivial one-element group.

Examples 4.2. Clearly, the following pairs provide examples of disjoint groups.

  (i) SS_3 and $\mathbf{A}_3$;
 (ii) SS_n and $\mathbf{A}_m$ $(m \geq 5)$;
(iii) $\mathbf{A}_n$ and $\mathbf{A}_m$ $(n \neq m$ and $m \geq 5)$;
 (iv) $G_1 := \mathrm{PSL}(d,q) \subset G_2 := \mathrm{PGL}(d,q)$, where
      (a) $d > 1, (d,q) \neq (2,2), (d,q) \neq (2,3)$;
      (b) integers d and $q-1$ have a common divisor > 1.
      The condition (a) means that G_1 is a finite simple non-abelian group [19, Ch. 1, §9]. The condition (b) means that $G_1 \neq G_2$. Clearly, G_1 is a normal subgroup of G_2 and the quotient G_2/G_1 is a cyclic group of order r where r is the largest common divisor of d and $q-1$. In

order to prove that G_1 and G_2 are disjoint, it suffices to check that there does not exist a surjective homomorphism $\phi : G_2 \twoheadrightarrow G_1$. Let us assume that such a surjection does exist. Then its kernel $\ker(\phi)$ is a proper normal subgroup of $G_2 = \mathrm{PGL}(d, q)$ and its preimage G' in $\mathrm{GL}(d, q)$ is a proper normal subgroup of $\mathrm{GL}(d, q)$ containing all the scalars and also an element that is not a scalar. Since every normal subgroup of $\mathrm{GL}(d, q)$ either contains $\mathrm{SL}(d, q)$ or consists of scalars [19, Ch. 1, §9, Th. 9.9], we conclude that G' contains $\mathrm{SL}(d, q)$ and therefore $\ker(\phi)$ contains $\mathrm{PSL}(d, q) = G_1$. This implies that the image G_1 of the surjection ϕ is isomorphic to a quotient of the cyclic group G_2/G_1 and therefore is also cyclic. Since $G_1 := \mathrm{PSL}(d, q)$ is non-abelian, we obtain the desired contradiction, which proves the disjointness of G_1 and G_2.

Let us recall the statement of well-known Goursat's lemma (see for instance [10, p. 75])

Lemma 4.3. *Let G_1 and G_2 be finite groups. Let H be a subgroup of the product $G_1 \times G_2$ such that the corresponding projection maps $\mathrm{pr}_1 : H \to G_1$ and $\mathrm{pr}_2 : H \to G_2$ are surjective. Denote by H_1 (respectfully by H_2) the normal subgroup of G_1 (respectfully of G_2), such that the kernel of pr_2 (respectfully of pr_1) coincides with $H_1 \times \{1\}$ (respectfully with $\{1\} \times H_2$). Then there exists an isomorphism $\gamma : G_1/H_1 \cong G_2/H_2$ such that H coincides with the preimage in $G_1 \times G_2$ of the graph of γ in $G_1/H_1 \times G_2/H_2$.*

Remark 4.4.   (i) If $H_1 = G_1, H_2 = G_2$ then $H = G_1 \times G_2$. If $H_1 = \{1\}, H_2 = \{1\}$ then $G_1 \cong G_2 \cong G$.
  (ii) If G_1 and G_2 are disjoint finite groups then one may easily check that every subgroup of $G_1 \times G_2$ that maps surjectively on each of the factors coincides with $G_1 \times G_2$.
 (iii) If $G_1 = G_2 = G$ is a finite simple group then one may easily check that either $H_1 = G_1, H_2 = G_2, H = G_1 \times G_2$ or $H_1 = \{1\}, H_2 = \{1\}$ and $G_1 \cong G_2 \cong G$.

Proposition 4.5. *Let K be a field of characteristic different from 2 and K_a its algebraic closure. Let $f(x), h(x) \in K[x]$ -are irreducible polynomials without multiple roots of degree $n \geq 3$ and $m \geq 3$ respectively. Suppose that the Galois groups $\mathrm{Gal}(f)$ of f and $\mathrm{Gal}(h)$ of h are disjoint. Suppose that $f(x)$ is very nice and $h(x)$ is nice.*
    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 jacobians $J(C_f)$ and $J(C_h)$ are supersingular abelian varieties.

Proof of Proposition 4.5. Let $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ be the splitting fields of f and h respectively and let L be the compositum of $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$. Then the Galois group $\mathrm{Gal}(L/K)$ of L/K may be viewed as a certain subgroup

of $\mathrm{Gal}(f) \times \mathrm{Gal}(h)$ that maps surjectively (under the projection maps) on each of the factors $\mathrm{Gal}(f)$ and $\mathrm{Gal}(h)$. It follows from Remark 4.4(ii) and disjointness of $\mathrm{Gal}(f)$ and $\mathrm{Gal}(h)$ that $\mathrm{Gal}(L/K)$ coincides with the product $\mathrm{Gal}(f) \times \mathrm{Gal}(h)$. This means that the extensions $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ are linearly disjoint over K and Proposition 4.5 follows readily from Theorem 1.2.   □

Proof of Corollary 1.4. It follows from Theorem 1.1 that $\mathrm{End}(J(C_f)) = \mathbf{Z}$. Therefore if $\mathrm{Hom}(J(C_f), J(C_h)) \neq 0$, then $\dim(J(C_h)) \geq \dim(J(C_f))$. It follows that $\deg(h) \geq 5$ but if $\mathrm{char}(K) > 0$ then $m = \deg(h) \geq 9$. Applying again Theorem 1.1, we observe that $\mathrm{End}(J(C_h)) = \mathbf{Z}$. It follows that if $\mathrm{Hom}(J(C_f), J(C_h)) \neq 0$ then $\dim(J(C_h)) = \dim(J(C_f))$. The last equality means that either $n = m$ or n is even and $m = n - 1$ or m is even and $n = m - 1$.

Further, replacing in the case $n \neq m, \mathrm{Gal}(f) = \mathbf{S}_n$ the field K by the corresponding quadratic or biquadratic extension, we may assume that either

$$ n \neq m, \quad \mathrm{Gal}(f) = \mathbf{A}_n, \quad \mathrm{Gal}(h) = \mathbf{A}_m $$

or

$$ n = m, \quad \mathrm{Gal}(f) = \mathbf{S}_n, \quad \mathrm{Gal}(h) = \mathbf{A}_m = \mathbf{A}_n. $$

Notice that in both cases the groups $G_1 := \mathrm{Gal}(f)$ and $G_2 := \mathrm{Gal}(h)$ are disjoint. One has only to apply Proposition 4.5.   □

In order to prove Corollary 1.5 we need a certain elementary assertion from Galois theory. But first let us introduce the following notations. Let L/K be the splitting field of a separable polynomial $f(x) \in K[x]$ of degree n. Then the set of roots $\mathfrak{R}_f$ of f lies in L and generates it over K. This gives rise to the natural embedding $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_f)$, which we denote by r_f. On the other hand, every ordering $\{\alpha_1, \cdots \alpha_n\}$ of elements of $\mathfrak{R}_f$ (i.e., of roots of f) allows us to identify $\mathrm{Perm}(\mathfrak{R}_f)$ and $\mathbf{S}_n$ and we may view r_f as homomorphism

$$ r_f : \mathrm{Gal}(L/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_f) = \mathbf{S}_n. $$

Notice that for each positive integer $j \leq n$ the stabilizer $\mathrm{Gal}(L/K)_{\alpha_j}$ of α_j in $\mathrm{Gal}(L/K)$ coincides with the preimage $r_f^{-1}(\mathbf{S}_n^{\{j\}})$ of the subgroup $\mathbf{S}_n^{\{j\}}$ of all permutations that send j into itself.

Lemma 4.6. *Let us assume that a finite Galois extension L/K, a positive integer n and a transitive permutation group$\Gamma \subset \mathbf{S}_n$ enjoy the following properties:*

  (i) *If $\mathrm{Gal}(L/K)$ is the Galois group of L/K then there exists an embedding $\mathrm{Gal}(L/K) \hookrightarrow \mathbf{S}_n$, whose image coincides with Γ;*
  (i) *For each automorphism $u : \Gamma \to \Gamma$ of Γ there is a permutation $s \in \mathbf{S}_n$ such that $u(z) = szs^{-1} \ \forall z \in \Gamma$.*

Suppose that $f(x), h(x) \in K[x]$ are two separable (i.e., without multiple roots) irreducible polynomials of degree n such that L is a splitting field of each of them. Let as assume additionally that there exist orderings $\{\alpha_1, \cdots \alpha_n\}$ of roots of f and $\{\beta_1, \cdots \beta_n\}$ of roots of h such that the image of both natural homomorphisms

$$r_f : \mathrm{Gal}(L/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_f) = \mathbf{S}_n, \quad r_h : \mathrm{Gal}(L/K) \hookrightarrow \mathrm{Perm}(\mathfrak{R}_h) = \mathbf{S}_n$$

coincides with Γ.

Then if α is a root of f, then there exists a root $\beta \in L$ of h such that $K(\alpha) = K(\beta)$.

Proof of Lemma 4.6. Clearly, $\mathrm{Gal}(L/K) \cong \Gamma$ and there is a permutation $s \in \mathbf{S}_n$ such that

$$r_h(\sigma) = s r_f(\sigma) s^{-1} \quad \forall \sigma \in \mathrm{Gal}(L/K).$$

If $j = s(i)$ then one may easily check that

$$r_h^{-1}(\mathbf{S}_n^{\{j\}}) = r_f^{-1}(\mathbf{S}_n^{\{i\}}),$$

and therefore in $\mathrm{Gal}(L/K)$ the stabilizer $\mathrm{Gal}(L/K)_{\beta_j}$ of β_j coincides with the stabilizer $\mathrm{Gal}(L/K)_{\alpha_j}$ of α_j. This means that $K(\alpha_i) = K(\beta_j)$.   □

Proof of . In light of Corollary 1.4, we may assume that either

$$\mathrm{Gal}(f) = \mathbf{S}_n, \quad \mathrm{Gal}(h) = \mathbf{S}_n$$

or

$$\mathrm{Gal}(f) = \mathbf{A}_n, \quad \mathrm{Gal}(h) = \mathbf{A}_n.$$

Let us assume that the normal field extensions $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ do *not* coincide (are not isomorphic). Then their compositum L coincides neither with $K(\mathfrak{R}_f)$ nor with $K(\mathfrak{R}_h)$ and therefore $\mathrm{Gal}(L/K)$ is isomorphic neither to $\mathrm{Gal}(f)$ nor to $\mathrm{Gal}(h)$. Applying Remark 4.4(iii) to $H = \mathrm{Gal}(L/K), G_1 = \mathrm{Gal}(f)$ and $G_2 = \mathrm{Gal}(h)$, we conclude that if $\mathrm{Gal}(f) = \mathbf{A}_n, \mathrm{Gal}(h) = \mathbf{A}_n$ then $\mathrm{Gal}(L/K) = \mathrm{Gal}(f) \times \mathrm{Gal}(h)$, since $H = \mathrm{Gal}(L/K)$ is not isomorphic to $G_1 = \mathrm{Gal}(f)$. Therefore $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ are linearly disjoint over K and Corollary 1.5 follows readily from Theorem 1.2. If $\mathrm{Gal}(f) = \mathbf{S}_n, \mathrm{Gal}(h) = \mathbf{S}_n$ then an easy check up of the short list of quotients of $\mathbf{S}_n$ allows us, applying Lemma 4.3 to $H = \mathrm{Gal}(L/K), G_1 = \mathrm{Gal}(f)$ and $G_2 = \mathrm{Gal}(h)$, to conclude that either $\mathrm{Gal}(L/K) = \mathrm{Gal}(f) \times \mathrm{Gal}(h)$ and Corollary 1.5 follows readily from Theorem 1.2 or $\mathrm{Gal}(L/K)$ contains $\mathbf{A}_n \times \mathbf{A}_n$ and coincides with the following subgroup of index 2 in $\mathrm{Gal}(f) \times \mathrm{Gal}(h) = \mathbf{S}_n \times \mathbf{S}_n$:

$$\{(\sigma, \tau) \in \mathbf{S}_n \times \mathbf{S}_n \mid \mathrm{sign}(\sigma) = \mathrm{sign}(\tau)\}.$$

(Here $\mathrm{sign}(\sigma)$ is the sign of σ.) Replacing (in the latter case) K by the corresponding quadratic extension, we may assume that

$$\mathrm{Gal}(L/K) = \mathbf{A}_n \times \mathbf{A}_n, \mathrm{Gal}(f) = \mathbf{A}_n, \mathrm{Gal}(h) = \mathbf{A}_n,$$

and the same arguments as in in the previous case prove Corollary 1.5. Therefore in order to prove Corollary 1.5, it suffices to check that the extensions $K(\mathfrak{R}_f)$ and $K(\mathfrak{R}_h)$ do not coincide. That is what we are going to do right now.

Let us assume that $K(\mathfrak{R}_f) = K(\mathfrak{R}_h)$. Replacing K by corresponding quadratic or biquadratic extension, we may assume that

$$\mathrm{Gal}(f) = \mathbf{A}_n, \quad \mathrm{Gal}(h) = \mathbf{A}_n.$$

Let us put $L = K(\mathfrak{R}_f) = K(\mathfrak{R}_h)$. Clearly, $\mathrm{Gal}(L/K) \cong \mathbf{A}_n$. Recall that if $n \geq 5$ and $n \neq 6$ then $\mathrm{Aut}(\mathbf{A}_n) = \mathbf{S}_n$ [19, §2.17, pp. 299-300]. Applying Lemma 4.6, we conclude that $K(\alpha) = K(\beta)$ for some roots α of f and β of h. However, $K(\alpha) \cong K[x]/fK[x] = K_f$ and $K(\beta) \cong K[x]/hK[x] = K_h$. Therefore the field extensions K_f/K and K_h/K are isomorphic. Contradiction. $\qquad\square$

5. Examples

We write $\bar{\mathbf{Q}}$ for the (algebraically closed) field of all algebraic numbers in $\mathbf{C}$.

Let us put $f_n(x) = x^n - x - 1 \in \mathbf{Q}[x]$ and consider the number field $E_n = \mathbf{Q}[x]/f_n\mathbf{Q}[x]$. According to Serre [17, remark 2 on p. 45], for each positive integer n the Galois group of $f_n(x)$ over $\mathbf{Q}$ coincides with $\mathbf{S}_n$. It is also known (ibid) that for each prime p the polynomial $\tilde{f}_n(x) := x^n - x - 1 \in \mathbf{F}_p[x]$ either has no multiple roots or p does not divide $n(n-1)$ and

$$\tilde{f}_n(x) = (x - \frac{n}{1-n})^2 \tilde{w}(x)$$

where $w(x) \in \mathbf{F}_p[x]$ is a polynomial without multiple roots and $0 \neq \tilde{w}(\frac{n}{1-n}) \in \mathbf{F}_p$. Clearly, if $\tilde{f}_n$ has no multiple roots then, by Hensel's lemma, $f_n(x)$ splits into a product of linear factors over an unramified extension of $\mathbf{Q}_p$ and therefore the field extension $E_n/\mathbf{Q}$ is unramified over p. But if $\tilde{f}_n$ has a multiple root then the polynomials $\tilde{w}(x)$ and $(x - \frac{n}{1-n})^2$ are relatively prime in $\mathbf{F}_p(x)$ and, thanks to well-known generalization of Hensel's lemma [6, §3.5, p.105], $f_n(x)$ splits over $\mathbf{Q}_p$ into a product of a quadratic polynomial (that is a lifting of $(x - \frac{n}{1-n})^2$) and a certain polynomial $w(x)$(that is a lifting of $\tilde{w}(x)$). In addition, $w(x)$ splits into a product of linear factors over an unramified extension of $\mathbf{Q}_p$. It follows that if $E_n/\mathbf{Q}$ is ramified over p then it does occur exactly at one prime ideal of the ring of integers of E_n and the ramification index is 2.

Let us consider the hyperelliptic curve $A_n : y^2 = f_n(x)$ defined over $\mathbf{Q}$ and its jacobian $J(A_n)$. If $n \leq 4$ then $J(A_n)$ is an elliptic curve. If $n \geq 5$ then $\mathrm{End}(J(A_n)) = \mathbf{Z}$ [20]. Therefore the abelian variety $J(A_n)$ is always absolutely simple. It follows from Corollary 1.4 that if $n \geq 5, m \geq 3$ and $n \neq m$ then every homomorphism between the jacobians $J(A_n)$ and $J(A_m)$ defined over $\bar{\mathbf{Q}}$ is zero. It follows readily that every homomorphism between $J(A_n)$ and $J(A_m)$ defined over the field of complex numbers $\mathbf{C}$ is zero. (Of

course, here the only interesting case is when $n = 2g+1$ is odd and $m = 2g+2$ is even and absolutely simple abelian varieties $J(A_{2g+1})$ and $J(A_{2g+2})$ have the same dimension g).

According to Schur [15], the Galois group $\mathrm{Gal}(\exp_n)$ of the polynomial

$$\exp_n(x) := 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots + \frac{x^n}{n!}$$

over $\mathbf{Q}$ is $\mathbf{S}_n$ if n is not divisible by 4; if $4 \mid n$ then $\mathrm{Gal}(\exp_n) = \mathbf{A}_n$. Let us consider the hyperelliptic curve $B_n : y^2 = f_n(x)$ defined over $\mathbf{Q}$ and its jacobian $J(B_n)$. If $n \leq 4$ then $J(B_n)$ is an elliptic curve; if $n \geq 5$ then $\mathrm{End}(J(B_n)) = \mathbf{Z}$ [20]. Therefore the abelian variety $J(B_n)$ is always absolutely simple. It follows from Corollary 1.4 that if $n \geq 5, m \geq 3$ and $n \neq m$ then every homomorphism between $J(B_n)$ and $J(B_m)$ and also between $J(B_n)$ and $J(A_m)$ defined over $\bar{\mathbf{Q}}$ or (which is the same) over $\mathbf{C}$ is zero. It also follows from Corollary 1.4 that if $n > 5$ and $4 \mid n$ then every homomorphism between $J(B_n)$ and $J(A_n)$ is zero.

Let us prove, using Corollary 1.5, that for all $n > 6$ every homomorphism between $J(B_n)$ and $J(A_n)$ is zero. In order to do that, let us consider the number field $H_n = \mathbf{Q}[x]/\exp_n \mathbf{Q}[x]$. Our goal will be reached if we prove that the fields E_n are H_n non-isomorphic. To that end, using Chebyshev's theorem (Bertrand's postulate), pick a prime p with

$$g + 1 \leq p \leq 2g + 1$$

where either $n = 2g + 1$ is odd or $n = 2g + 2$ is even. In particular,

$$p \geq g + 1 \geq \frac{n}{2} > 3.$$

We write

$$\mathrm{ord}_p : \mathbf{Q}^* \to \mathbf{Z}$$

for the discrete valuation of $\mathbf{Q}$ attached to p and normalized by the condition $\mathrm{ord}_p(p) = 1$ [8]. One may easily check that for all positive integers $i < p$

$$\mathrm{ord}_p\left(\frac{1}{i!}\right) = 0,$$

and for all integers i with $p \leq i \leq n$

$$\mathrm{ord}_p\left(\frac{1}{i!}\right) = -1,$$

except the case

$$n = 2g + 2 = i, p = g + 1, \mathrm{ord}_p\left(\frac{1}{i!}\right) = \mathrm{ord}_{g+1}\left(\frac{1}{(2g+2)!}\right) = -2.$$

It follows that the rational number $\frac{-1}{p}$ is a *slope* of the p-adic Newton polygon of $\exp_n(x)$. The well-known connection between (reciprocal) roots of a polynomial and slopes of its Newton polygon conclude [8] allows us to conclude that there is a prime ideal in the ring of integers of H_n that divides p and whose ramification index in $H_n/\mathbf{Q}$ is divisible by $p > 3$. Since all

the ramification indices in $E_n/\mathbf{Q}$ do not exceed 2 (see the beginning of this Section), the fields E_n and H_n are non-isomorphic. Applying Corollary 1.5 to $f = f_n, h = \exp_n$, we conclude that for all $n > 6$ every homomorphism between $J(B_n)$ and $J(A_n)$ defined over $\bar{\mathbf{Q}}$ or (which is the same) over $\mathbf{C}$ is zero.

Let us turn now to a completely different class of examples. Let p be an odd prime, k_p an algebraically closed field of characteristic p, K=K(t) the field of rational functions in independent variable t with coefficients in k_p and K_a an algebraic closure of K. Let an integer $q > 1$ be an integral power of p. Let $d > 1$ be a positive integer. Let us put

$$n = \frac{q^d - 1}{q - 1} = \#(\mathbf{P}^{d-1}(\mathbf{F}_q))$$

and consider the polynomials

$$f(x) = x^n + tx + 1 \in K[x], \quad h(x) = x^n + x + t \in K[x].$$

According to Abhyankar [1], there are bijections

$$\mathfrak{R}_f \cong \mathbf{P}^{d-1}(\mathbf{F}_q), \quad \mathfrak{R}_f \cong \mathbf{P}^{d-1}(\mathbf{F}_q),$$

such that $\mathrm{Gal}(f)$ becomes $\mathrm{PSL}(d,q)$ and $\mathrm{Gal}(h)$ becomes $\mathrm{PGL}(d,q)$. Let us assume, in addition, that $m > 2$. Then both $f(x)$ and $h(x)$ are very nice. Suppose also that d and $q - 1$ are *not* relatively prime. Then $\mathrm{Gal}(f) = \mathrm{PSL}(d,q)$ and $\mathrm{Gal}(f) = \mathrm{PGL}(d,q)$ are disjoint (see 4.2(iv)). According to Proposition 4.5, if $J(C_f)$ and $J(C_h)$ are the jacobians of the hyperelliptic curves

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

then either both jacobians are supersingular or every homomorphism between $J(C_f)$ and $J(C_h)$ defined over K_a is zero. However, by theorem 2.4(iv) of [23], if $(q,d) \neq (3,4)$ then

$$\mathrm{End}(J(C_f)) = \mathbf{Z}, \quad \mathrm{End}(J(C_h)) = \mathbf{Z},$$

and therefore both jacobians are not supersingular. Therefore if $(q,d) \neq (3,4)$ then every homomorphism between $J(C_f)$ and $J(C_h)$ defined over K_a is zero.

References

[1] S. S. Abhyankar, *Projective polynomials*. Proc. Amer. Math. Soc. **125** (1997), 1643–1650.

[2] Ch. W. Curtis, I. Reiner, Methods of Representation Theory, Vol. I, John Wiley & Sons, New York Chichester Brisbane Toronto, 1981.

[3] J. D. Dixon, B. Mortimer, Permutation Groups. Springer-Verlag, New York Berlin Heidelberg, 1996.

[4] B. Huppert, Endliche Gruppen I. Springer-Verlag, Berlin Heidelberg New York, 1967.

[5] B. Huppert, N. Blackburn, Finite groups III. Springer-Verlag, Berlin Heidelberg New York, 1982.

[6] G. J. Janusz, Algebraic Number Fields, Second Edition, American Mathematical Society, Providence, RI, 1996.

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

[8] N. Koblitz, *p*-adic numbers, *p*-adic analysis and zeta-functions. Springer-Verlag, Berlin Heidelberg New York, 1977.

[9] A. A. Ivanov, Ch. E. Praeger, *On finite affine 2-Arc transitive graphs.* Europ. J. Combinatorics **14** (1993), 421–444.

[10] S. Lang, Algebra, Third Edition, Addison-Wesley, Reading, MA, 1993.

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

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

[13] D. Mumford, *Theta characteristics of an algebraic curve.* Ann. scient. Éc. Norm. Sup. (4) **4** (1971), 181–192.

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

[15] I. Schur, *Gleichungen ohne Affect.* Sitz. Preuss. Akad. Wiss. 1930, Physik-Math. Klasse 443–449 (= Ges. Abh. III, 191–197).

[16] J.-P. Serre, Lectures on the Mordell-Weil Theorem, 2nd edition, Friedr. Vieweg & Sons, Braunschweig/Wiesbaden, 1990.

[17] J.-P. Serre, Topics in Galois Theory, Jones and Bartlett Publishers, Boston-London, 1992.

[18] J.-P. Serre. *Représentations linéares des groupes finis*, Troisiéme édition. Hermann, Paris, 1978.

[19] M. Suzuki, Group theory I, Springer Verlag, Berlin Heidelberg New York, 1982.

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

[21] 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.

[22] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication in positive characteristic.* Math. Res. Letters **8** (2001), 429–435.

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

[24] Yu. G. Zarhin, *Hyperelliptic jacobians and simple groups* $U_3(2^m)$. Proc. Amer. Math. Soc. **131** (2003), no. 1, 95–102.

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

Institute of Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, Russia

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