NON-ISOGENOUS SUPERELLIPTIC JACOBIANS II

YURI G. ZARHIN

To the memory of Kolya Vavilov

ABSTRACT. Let ℓ be an odd prime and K a field of characteristic different from ℓ. Let $\bar{K}$ be an algebraic closure of K. Assume that K contains a primitive ℓth root of unity. Let $n \neq \ell$ be another odd prime. Let $f(x)$ and $h(x)$ be degree n polynomials with coefficients in K and without repeated roots.

Let us consider superelliptic curves $C_{f,\ell} : y^\ell = f(x)$ and $C_{h,\ell} : y^\ell = h(x)$ of genus $(n-1)(\ell-1)/2$, and their jacobians $J^{(f,\ell)}$ and $J^{(h,\ell)}$, which are $(n-1)(\ell-1)/2$-dimensional abelian varieties over $\bar{K}$.

Suppose that one of the polynomials is irreducible and the other reducible over K. We prove that if $J^{(f,\ell)}$ and $J^{(h,\ell)}$ are isogenous over $\bar{K}$ then both endomorphism algebras $\mathrm{End}^0(J^{(f,\ell)})$ and $\mathrm{End}^0(J^{(h,\ell)})$ contain an invertible element of multiplicative order n.

1. DEFINITIONS, NOTATIONS, STATEMENTS

This paper is a follow up of [20, 23] and we use their (more or less standard) notation. (See also [18, 22, 23].) In particular, ℓ is an odd prime, $\mathbb{F}_\ell$ the corresponding (finite) prime field of characteristic ℓ. We write $\mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$ for the ring of ℓ-adic integers and the field $\mathbb{Q}_\ell$ of ℓ-adic numbers respectively. Let us fix a primitive ℓth root of unity

$$\zeta_\ell \in \mathbb{C}$$

in the field $\mathbb{C}$ of complex numbers. We write $\mathbb{Q}(\zeta_\ell)$ for the ℓth cyclotomic field and

$$\mathbb{Z}[\zeta_\ell] = \sum_{i=0}^{\phi(q)-1} \mathbb{Z} \cdot \zeta_\ell^i$$

for its ring of integers. We write $\mathcal{P}_\ell(t)$ for the ℓth cyclotomic polynomial

$$\mathcal{P}_\ell(t) = \sum_{j=0}^{\ell-1} t^j \in \mathbb{Z}[t].$$

Let K be a field with $\mathrm{char}(K) \neq \ell$. Let us fix an algebraic closure $\bar{K}$ of K and write $\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K)$ for the group of its K-linear automorpisms. In what follows we always assume that K contains a primitive ℓth root of unity, say, ζ. Let $K_s \subset \bar{K}$ be the separable algebraic closure of K. The subfield K_s of $\bar{K}$ is the natural group homomorphism (restriction map)

$$\mathrm{Gal}(K) = \mathrm{Aut}(\bar{K}/K) \to \mathrm{Aut}(K_s/K) = \mathrm{Gal}(K_s/K)$$

is a group isomorphism.

Let X and Y be abelian varieties over K. By a theorem of Chow [2, Th. 3.19]), all $\bar{K}$-endomorphisms between X and Y are defined over K_s. In particular, all endomorphisms of X are defined over K_s. A more precise information about the field of definition of all endomorphisms of X is given by a theorem of A. Silverberg [16] (see Remark 2.1 below).

Let $n \geq 3$ be an odd integer. Throughout the paper, we assume that ℓ does *not* divide n.

Let $f(x) \in K[x]$ be a polynomial with coefficients in K, of degree n and without repeated roots. We write $\mathfrak{R}_f \subset \bar{K}$ for the n-element set of roots of $f(x)$, $K(\mathfrak{R}_f)$ for the splitting field of $f(x)$ and $\mathrm{Gal}(f/K)$ for the Galois group

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

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

We write $C_{f,\ell}$ for the smooth projective model of the plane affine curve $y^\ell = f(x)$. It is well known [12, 13] that the genus $g(C_{f,\ell})$ of $C_{f,\ell}$ is $(\ell-1)(n-1)/2$. The map

$$(x, y) \mapsto (x, \zeta y)$$

gives rise to a non-trivial biregular automorphism

$$\delta_\ell : C_{f,\ell} \to C_{f,\ell}$$

of period ℓ that is defined over K.

Let $J^{(f,\ell)}$ be the jacobian of $C_{f,\ell}$; it is a $(\ell-1)(n-1)/2$-dimensional abelian variety that is defined over K. We write $\mathrm{End}(J^{(f,\ell)})$ for the ring of $\bar{K}$-endomorphisms of $J^{(f,\ell)}$ and $\mathrm{End}^0((J^{(f,\ell)}) = \mathrm{End}(J^{(f,\ell)}) \otimes \mathbb{Q}$ for the corresponding endomorphism algebra of $J^{(f,\ell)}$. By functoriality,

δ_ℓ induces a K-automorphism of $J^{(f,\ell)}$, which we still denote by δ_ℓ. It is known ([12, p. 149], [13, p. 448]; see also [21]) that

$$\mathcal{P}_\ell(\delta_\ell) = \sum_{j=0}^{\ell-1} \delta_\ell^j = 0 \tag{1}$$

in $\mathrm{End}(J^{(f,\ell)})$. Then (1) gives rise to the ring homomorphism,

$$\mathbf{i}_{\ell,f} : \mathbb{Z}[\zeta_\ell] \hookrightarrow \mathbb{Z}[\delta_\ell] \subset \mathrm{End}(J^{(f,\ell)}), \ \zeta_\ell \mapsto \delta_\ell, \tag{2}$$

which is a *ring embedding* ([12, p. 149], [13, p. 448]; see also [21]). (Here $1 \in \mathbb{Z}[\zeta_\ell]$ goes to the *identity automorphism* $1_{J^{(f,\ell)}}$ of $J^{(f,\ell)}$.) This implies that the subring $\mathbb{Z}[\delta_\ell]$ of $\mathrm{End}(J^{(f,\ell)})$ generated by δ_ℓ is isomorphic to $\mathbb{Z}[\zeta_\ell]$. It follows that the $\mathbb{Q}$-subalgebra

$$\mathbb{Q}[\delta_\ell] \subset \mathrm{End}^0(J^{(f,\ell)}) \tag{3}$$

generated by δ_ℓ is canonically isomorphic to the ℓth cyclotomic field $\mathbb{Q}(\zeta_\ell)$ and therefore

$$\dim_{\mathbb{Q}}(\mathbb{Q}[\delta_\ell]) = \ell - 1.$$

Let $f(x)$ and $h(x)$ be degree n polynomials with coefficients in K and without repeated roots. Let

$$C_{f,\ell} : y^\ell = f(x), \ C_{h,\ell} : y^\ell = h(x)$$

be the corresponding genus $(n-1)(\ell-1)/2$ superelliptic curves over K, whose jacobians we denote by $J^{(f,\ell)}$ and $J^{(h,\ell)}$, respectively. These jacobians are $(n-1)(\ell-1)/2$-dimensional abelian varieties defined over K. Assuming that the Galois properties of roots of $f(x)$ and $h(x)$ are *distinct* (see below), we will prove that if the abelian varieties $J^{(f,\ell)}$ and $J^{(h,\ell)}$ are isogenous over $\bar{K}$ then they admit an "additional symmetry", i.e., the inclusion (3) is *not* an equality.

The main result of this paper is the following assertion.

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

If the corresponding superelliptic jacobians $J^{(f,\ell)}$ and $J^{(h,\ell)}$ are isogenous over $\bar{K}$ then both endomorphism algebras $\mathrm{End}^0(J^{(f,\ell)})$ and $\mathrm{End}^0(J^{(h,\ell)})$ contain an invertible element of multiplicative order n. In addition,

$$\dim_{\mathbb{Q}} \left(\mathrm{End}^0(J^{(f,\ell)}) \right) = \dim_{\mathbb{Q}} \left(\mathrm{End}^0(J^{(h,\ell)}) \right) \geq$$
$$(\ell-1)(n-1) = 2 \dim(J^{(f,\ell)}) = 2 \dim(J^{(h,\ell)}).$$

The next assertion may be viewed as a partial generalization of Theorem 1.1 to the case of an arbitrary odd $n \geq 3$.

Theorem 1.2. *Suppose that $n \geq 3$ is an odd integer and ℓ is an odd prime not dividing n. Let K be a field of characteristic different from ℓ. Let $f(x), h(x) \in K[x]$ be degree n polynomials without repeated roots. Suppose that $f(x)$ is irreducible over K.*

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

If the corresponding superelliptic jacobians $J^{(f,\ell)}$ and $J^{(h,\ell)}$ are isogenous over $\bar{K}$ then there is a prime divisor r of n such that both endomorphism algebras $\mathrm{End}^0(J^{(f,\ell)})$ and $\mathrm{End}^0(J^{(h,\ell)})$ contain an invertible element of multiplicative order r. In addition,

$$\dim_{\mathbb{Q}}\left(\mathrm{End}^0(J^{(f,\ell)})\right) = \dim_{\mathbb{Q}}\left(\mathrm{End}^0(J^{(h,\ell)})\right) \geq (\ell - 1)(r - 1).$$

Remark 1.3. If the conditions of Theorem 1.2 hold then $h(x)$ is reducible over K, see [23, Remark 1.4].

Corollary 1.4. *Suppose that n and ℓ are distinct odd primes. Let $f(x), h(x) \in K[x]$ be degree n polynomials without repeated roots. Suppose that $f(x)$ is irreducible over K and $\mathrm{Gal}(\mathfrak{R}_f)$ is a doubly reansitive permutation group of $\mathfrak{R}_f$. Assume also that $\mathrm{Gal}(h/K)$ is a cyclic group of order n. If the corresponding superelliptic jacobians $J^{(f,\ell)}$ and $J^{(h,\ell)}$ are isogenous over $\bar{K}$ then both endomorphism algebras $\mathrm{End}^0(J^{(f,\ell)})$ and $\mathrm{End}^0(J^{(h,\ell)})$ contain an invertible element of multiplicative order n. In addition,*

$$\dim_{\mathbb{Q}}\left(\mathrm{End}^0(J^{(f,\ell)})\right) = \dim_{\mathbb{Q}}\left(\mathrm{End}^0(J^{(h,\ell)})\right) \geq$$

$$(\ell - 1)(n - 1) = 2 \dim(J^{(f,\ell)}) = 2 \dim(J^{(h,\ell)}).$$

Example 1.5. Let ℓ be an odd prime and $n \geq 3$ an odd integer that is *not* divisible by ℓ. Let us take as K the ℓth cyclotomic field $\mathbb{Q}(\zeta_\ell)$. Let us put

$$f(x) = x^n - 2, \; h(x) = x^n - 1 \in K[x].$$

By the 2-dic Eisenstein criterion, $f(x)$ is irreducible over K (recall that prime 2 is unramified in $\mathbb{Q}(\zeta_\ell) = K$, because ℓ is odd) while $h(x)$ is obviously reducible over K. Let ℓ be an odd prime that does *not* divide n. The curves $C_{f,\ell}$ and $C_{h,\ell}$ are obviously isomorphic over $\bar{K}$. They both admit periodic $\bar{K}$-automorphisms $\tilde{\delta}_n$ of order n defined by the (same) formula

$$(x, y) \mapsto (\zeta_n x, y)$$

where

$$\zeta_n \in \bar{K} = \bar{\mathbb{Q}} \subset \mathbb{C}$$

is a primitive nth root of unity. This implies that their jacobians $J^{(f,\ell)}$ and $J^{(h,\ell)}$ are abelian varieties over $\bar{K}$ that are isomorphic over $\bar{K}$ and admit periodic automorphisms of order n that we continue to denote by $\tilde{\delta}_n$. It follows that if r is any prime divisor of n then both $J^{(f,\ell)}$ and $J^{(h,\ell)}$ admit automorphisms $\left(\tilde{\delta}_n\right)^{n/r}$ of multiplicative order r that may be viewed as invertible elements of multiplicative order r in $\mathrm{End}^0(J^{(f,\ell)})$ and $\mathrm{End}^0(J^{(h,\ell)})$.

Example 1.6. Let $n \geq 5$ be an odd integer and ℓ an odd prime not dividing n. Let us put $K = \mathbb{Q}(\zeta_\ell)$.

Let $f(x) \in K[x]$ be a degree n irreducible polynomial over K, whose Galois group $\mathrm{Gal}(f/K)$ is either the full symmetric group S_n or the alternating group A_n. It is known [17, 19, 24] that the endomorphism algebra $\mathrm{End}^0(J^{(f,\ell)})$ is isomorphic to the field $\mathbb{Q}(\zeta_\ell)$; in particular, $J^{(f,\ell)}$ is *absolutely simple*. The (cyclic) multiplicative group of all roots of unity in $\mathbb{Q}(\zeta_\ell)$ has order 2ℓ, which is prime to (odd) n. Hence, $\mathrm{End}^0(J^{(f,\ell)}) \cong \mathbb{Q}(\zeta_\ell)$ does not contain elements of multiplicative order r for any prime divisor r of n.

Let $h(x) \in K[x]$ be a degree n polynomial that splits over K into a product of linear factors.

Then it follows from Theorem 1.2 that $J^{(f,\ell)}$ and $J^{(h,\ell)}$ are *not* isogenous over $\bar{K} = \bar{\mathbb{Q}}$ (and therefore even over $\bar{\mathbb{C}}$, in light of a theorem of Chow [2, Th. 3.19]). Since $J^{(f,\ell)}$ is absolutely simple and has the same dimension as $J^{(h,\ell)}$, it follows that every $\mathbb{C}$-homomorphism between $J^{(f,\ell)}$ and $J^{(h,\ell)}$ is zero.

Example 1.7. Let $n \geq 5$ be an odd integer and ℓ an odd prime not dividing n. Let us consider the degree n polynomials

$$f_1(x) = x^n - x - 1, \quad f_2(x) = \sum_{j=0}^{n} \frac{x^j}{j!}$$

with rational coefficients. It is known (Selmer, Osada [10]) that $f_1(x)$ is irreducible over $\mathbb{Q}$ and $\mathrm{Gal}(f_1/\mathbb{Q}) = \mathrm{S}_n$. By a theorem of Schur [1], $f_2(x)$ is irreducible over $\mathbb{Q}$ and $\mathrm{Gal}(f_2/\mathbb{Q}) = \mathrm{S}_n$ or A_n.

Recall that $n \geq 5$ and therefore A_n is a simple non-abelian group that coincides with the commutator subgroup of S_n; in addition, A_n is a maximal subgroup of S_n. Since $K := \mathbb{Q}(\zeta_\ell)$ is an abelian extension of $\mathbb{Q}$, the Galois group $\mathrm{Gal}(f_k/K)$ is either S_n or A_n (for $k = 1, 2$). In particular, both f_1 and f_2 remain irreducible over K.

It follows from Example 1.6 that if $h(x) \in K[x]$ is a degree n polynomial that splits over K into a product of linear factors then every $\mathbb{C}$-homomorphism between $J^{(f_k,\ell)}$ and $J^{(h,\ell)}$ is zero (for both $k = 1, 2$).

Remark 1.8. Examples 1.6 and 1.7 illustrate the title of this paper, whose aim is to provide a criterion for certain superelliptic jacobians *not* to be isogenous.

Remark 1.9. In light of Theorem of Chow cited above, the assertions of Theorem 1.1, 1.2 (and of Theorem 2.2 below), and Corollary 1.4 remain true if one replaces $\bar{K}$ by K_s.

The paper is organized as follows. In Section 2 we recall basic facts about Galois properties of points of order ℓ on superelliptic jacobians. We also state Theorem 2.2 that is a slightly stronger version of Theorem 1.2. Section 3 contains the proof of Theorem 2.2. We prove Theorem 1.1 in Section 4. Corollary 1.4 is proven in Section 5.

Acknowledgments. I am deeply grateful to the referee for helpful comments.

2. Points of order ℓ on superelliptic jacobians

Recall that $K_s \subset \bar{K}$ is the separable algebraic closure of K. Let X be a positive-dimensional abelian variety over K. We write $\mathrm{End}(X)$ for the ring of all $\bar{K}$-endomorphisms of X and $\mathrm{End}^0(X) := \mathrm{End}(X) \otimes \mathbb{Q}$ for the corresponding *endomorphism algebra* of X, which is a semisimple *finite-dimensional* $\mathbb{Q}$-algebra. We write 1_X for the identity automorphism of X that is may be viewed as the *identity element* of the $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$.

If d is a positive integer then we write $X[d]$ for the kernel of multiplication by d in $X(\bar{K})$. Recall ([9, Sect. 6], [7, Sect. 8, Remark 8.4]) that if d is *not* divisible by $\mathrm{char}(K)$ then $X[d]$ is a $\mathrm{Gal}(K)$-submodule of $X(K_s)$; in addition, $X[d]$ is isomorphic as a commutative group to $(\mathbb{Z}/d\mathbb{Z})^{2\dim(X)}$.

Let $K(X[d])$ be the *field of definition* of all torsion points of order dividing d on X. It is well known [7, Remark 8.4] that $K(X[d])$ lies in K_s and is a finite Galois extension of K. Let us put

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

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

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

For example, if d is a prime $\ell \neq \mathrm{char}(K)$ then $X[\ell]$ is a $2\dim(X)$-dimensional vector space over the field $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$, and the inclusion

$\tilde{G}_{\ell,X,K} \subset \operatorname{Aut}_{\mathbb{F}_\ell}(X[\ell])$ defines a *faithful* linear representation of the group $\tilde{G}_{\ell,X,K}$ in the vector space $X[\ell]$ over $\mathbb{F}_\ell$.

Remark 2.1. If $d \geq 3$ is an integer *not* divisible by $\operatorname{char}(K)$ then all the endomorphisms of X are defined over $K(X[d])$, by a theorem of A. Silverberg [16, Th. 2.4]. (See also [4, 14, 3].)

The following assertion may be viewed as a variant of Theorem 1.2 (when $Y = J^{(h,\ell)}$).

Theorem 2.2. *Let ℓ be an odd prime and K a field of characteristic $\neq \ell$. Let $n \geq 3$ be an odd positive integer that is not divisible by ℓ, and $f(x) \in K[x]$ a degree n irreducible polynomial without repeated roots. Let us put $X = J^{(f,\ell)}$, which is a $(n-1)(\ell-1)/2$-dimensional abelian variety over K.*

Let Y be an abelian variety over K such that the order of $\tilde{G}_{\ell,Y,K}$ is prime to n. (E.g., $K(Y[\ell]) = K$ or this order is a power of ℓ.)

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

Then there is an odd prime r dividing n such that both endomorphism algebras $\operatorname{End}^0(X)$ and $\operatorname{End}^0(Y)$ contain an invertible element of multiplicative order r. In addition,

$$\dim_{\mathbb{Q}}\left(\operatorname{End}^0(J^{(f,\ell)})\right) = \dim_{\mathbb{Q}}\left(\operatorname{End}^0(Y)\right) \geq (\ell-1)(r-1).$$

Remark 2.3. Recall that the order of $\tilde{G}_{\ell,Y,K}$ coincides with the degree $[K(Y[\ell]) : K]$ of the Galois extension $K(Y[\ell])/K$.

We will prove Theorem 2.2 in Section 3. Our proof is based on the Galois properties of certain points of order ℓ on superelliptic jacobians $J^{(f,\ell)}$ that will be discussed in the next subsection.

2.1. **Galois properties.** In this subsection we recall an explicit description of a certain important Galois submodule of $J^{(f,\ell)}[\ell]$ [12, 13] for arbitrary separable $f(x)$, assuming as usual that ℓ does *not* divide n.

Let us start with the n-dimensional $\mathbb{F}_\ell$-vector space

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

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

$$\mathbb{F}_\ell^{\mathfrak{R}_f} = \mathbb{F}_\ell \cdot \mathbf{1}_{\mathfrak{R}_f} \oplus Q_{\mathfrak{R}_f} \tag{4}$$

of the one-dimensional subspace $\mathbb{F}_\ell \cdot \mathbf{1}_{\mathfrak{R}_f}$ of constant functions and the $(n-1)$-dimensional *heart* [5, 8]

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

(here we use that n is not divisible by ℓ). Clearly, the $\mathrm{Perm}(\mathfrak{R}_f)$-module $Q_{\mathfrak{R}_f}$ is faithful. It remains faithful if we view it as a $\mathrm{Gal}(f/K)$-module.

Remark 2.4. There is a nondegenerate $\mathrm{Perm}(\mathfrak{R}_f)$-invariant $\mathbb{F}_\ell$-bilinear pairing

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

and the splitting (4) is an orthogonal direct sum. Clearly, the restriction of Ψ to $\mathbb{F}_2 \cdot \mathbf{1}_{\mathfrak{R}_f}$ is nondegenerate and therefore the restriction of Ψ to $Q_{\mathfrak{R}_f}$ is nondegenerate as well. This implies that the $\mathrm{Gal}(f/K)$-module $Q_{\mathfrak{R}_f}$ and its *dual* $\mathrm{Hom}_{\mathbb{F}_\ell}(Q_{\mathfrak{R}_f}, \mathbb{F}_\ell)$ are *isomorphic*.

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

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

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

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

In order to explain why the structure of the Galois module $Q_{\mathfrak{R}_f}$ is important, let us consider the subgroup (actually, the Galois submodule)

$$J^{(f,\ell)}[1 - \delta_\ell] = \{z \in J^{(f,\ell)}(\bar{K}) \mid \delta_l(z) = z\}$$

of $J^{(f,\ell)}(\bar{K})$. B. Poonen and E. Schaefer [12, 13] observed that the Galois module $J^{(f,\ell)}[1 - \delta_\ell]$ is a Galois submodule of $J^{(f,\ell)}[\ell]$ and is isomorphic to $Q_{\mathfrak{R}_f}$. In particular, $K(\mathfrak{R}_f)$ coincides with the *field of definition* of all points of $J^{(f,\ell)}[1 - \delta_\ell]$.

We will need the following elementary assertion about homomorphisms of Galois modules related to $Q_{\mathfrak{R}_f}$.

Lemma 2.5. *Suppose that $f(x)$ is irreducible over K and a prime ℓ does not divide n. Then:*

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

$$Q_{\mathfrak{R}_f} \to W$$

is zero.

(iv) *Let V be a finite-dimensional $\mathbb{F}_\ell$-vector space provided with a linear action of $\mathrm{Gal}(K)$ in such a way that every simple (Jordan-Hölder) subquotient of V is a trivial Galois module. Then every homomorphism of the Galois modules $Q_{\mathfrak{R}_f} \to V$ is zero.*

(v) *Let V be a finite-dimensional $\mathbb{F}_\ell$-vector space provided with a linear action of $\mathrm{Gal}(K)$ in such a way that every simple (Jordan-Hölder) subquotient of V is a trivial Galois module. Let M be a finite-dimensional $\mathbb{F}_\ell$-vector space provided with a linear action of $\mathrm{Gal}(K)$ in such a way that there is a filtration*

$$M_0 = \{0\} \subset M_1 \subset \cdots \subset M_d = M$$

of M by Galois submodules M_i such that every quotient M_{i+1}/M_i is isomorphic to $Q_{\mathfrak{R}_f}$. Then every homomorphism of the Galois modules $M \to V$ is zero.

Proof. Recall that the irreducibility means that the Galois group acts transitively on $\mathfrak{R}_f$. Let $\phi \in Q_{\mathfrak{R}_f}$ be a Galois-invariant function on $\mathfrak{R}_f$. The transitivity implies that ϕ is constant. This means that there is $c \in \mathbb{F}_\ell$ such that $\phi(\alpha) = c$ for all $\alpha \in \mathfrak{R}_f$ and therefore (since $\phi \in Q_{\mathfrak{R}_f}$)

$$0 = \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = n \cdot c,$$

i.e., $c = 0$. This means that $\phi \equiv 0$, which proves (i). In order to prove the second assertion of Lemma, recall (Remark 2.4) that the Galois modules $Q_{\mathfrak{R}_f}$ and $\mathrm{Hom}_{\mathbb{F}_\ell}(Q_{\mathfrak{R}_f}, \mathbb{F}_\ell)$ are isomorphic. Now the second assertion of our Lemma follows from the already proven first one. On the other hand, the third assertion is an immmediate corollary of the second one: one has only to choose a basis of W. In order to prove (iv), we will use induction by $\dim(V)$. We may assume that the subspace $V \neq \{0\}$. It follows from our assumptions on the Galois module V that the subspace $V_0 = V^{\mathrm{Gal}(K)}$ of Galois invariants is not $\{0\}$ as well. If $u : Q_{\mathfrak{R}_f} \to V$ is a homomorphism of Galois modules then the induction assumption applied to the quotient V/V_0 implies that the induced homomorphism of Galois modules

$$Q_{\mathfrak{R}_f} \to V/V_0, \ \phi \mapsto u(\phi) + V_0$$

is zero. This means that $u(Q_{\mathfrak{R}_f}) \subset V$. Now the desired result follows from (iii) applied to

$$Q_{\mathfrak{R}_f} \to V_0, \ \phi \mapsto u(\phi) \in V_0,$$

because $\mathrm{Gal}(K)$ acts trivially on V_0.

In order to prove (v), let us use induction by d. Let $u : M \to V$ be a homomorphism of Galois modules. Since M_1 is isomorphic to $Q_{\mathfrak{R}_f}$, it follows from (iv) that $u(M_1) = \{0\}$, i.e., there is a homomorphism of Galois modules $u_1 : M/M_1 \to V$ such that u is the composition of

$$M \to M/M_1, \ m \mapsto m + M_1$$

and u_1. If $d = 1$ then we are done. If $d > 1$ then the desired result follows from the induction assumption applied to the filtered Galois module

$$M/M_1 = (M/M_1)_{d-1} \supset \cdots \supset M_1/M_1 = \{0\} = (M/M_0)_0.$$

$\square$

Towse

3. Isogenous superelliptic jacobians

We will deduce Theorem 2.2 from the following auxiliary statements.

Lemma 3.1 (See Lemma 3.1 of [23]). *Let G be a transitive permutation group of a finite nonempty set $\mathfrak{R}$, and H a normal subgroup of G. Then the number of H-orbits in $\mathfrak{R}$ divides both $\#(\mathfrak{R})$ and the index $(G : H)$. In particular, if $\#(\mathfrak{R})$ and $(G : H)$ are relatively prime then H acts transitively on $\mathfrak{R}$.*

Lemma 3.2 (See Lemma 3.2 of [23]). *Let $f(x)$ be a degree n irreducible polynomial over a field K and without repeated roots. Let K_1/K be a finite Galois field extension, whose degree is prime to n. Then $f(x)$ remains irreducible over K_1. In particular, the order of Galois group $\mathrm{Gal}(f/K_1)$ is divisible by n.*

Lemma 3.3. *Let ℓ be a prime, F a field of characteristic ℓ, and V a finite-dimensional vector space over F. Let $\mathcal{N} \subset \mathrm{End}_F(V)$ be a linear nilpotent Lie subalgebra of $\mathrm{End}_F(V)$, and*

$$V^{\mathcal{N}} := \{v \in V \mid x(v) = 0 \ \forall x \in \mathcal{N}\}.$$

Let σ be a linear automorphism of finite order in V that commutes with all linear operators from $\mathcal{N}$ and such that the subspace V^σ of all σ-invariants in V contains $V^{\mathcal{N}}$. Then the order of σ is either 1 or a power of ℓ.

Remark 3.4. We will apply the easy "commutative" case of Lemma 3.3 to $F = \mathbb{F}_\ell$, $V = X[\ell]$, and

$$\sigma \in \mathrm{Gal}(K(X[\ell])/K(X[1 - \delta_\ell])) \subset \mathrm{Aut}_{\mathbb{F}_\ell}(X[\ell])$$

where $X = J^{(f,\ell)}$.

Proof of Lemma 3.3. Replacing σ by its suitable power, we may assume that σ is a periodic automorphism, whose order is prime to ℓ. We need to prove that σ is the identity map.

Since σ is obviously a semisimple linear operator, V splits into a direct sum of σ-invariant subspaces

$$V = V^\sigma \oplus W \quad \text{where } W = (1 - \sigma)V.$$

In particular,

$$V^\sigma \cap W = \{0\}.$$

Assume that $W \neq \{0\}$. We need to arrive to a contradiction. Since $\mathcal{N}$ commutes with σ, the subspace $W = (1 - \sigma)V$ is $\mathcal{N}$-invariant. By Engel's theorem, there is a *nonzero* vector $w \in W$ that is killed all linear operators from $\mathcal{N}$, i.e., $w \in V^\mathcal{N}$. This implies that $w \in W \in V^\sigma$. Hence,

$$w \in V^\sigma \cap W = \{0\}.$$

This implies that $w = 0$, which gives us a desired contradiction.

$\square$

Corollary 3.5. *Let $X = J^{(f,\ell)}$. Then:*
  (i) *$K(X[\ell])/K(\mathfrak{R}_f)$ is a finite Galois ℓ-extension, i.e., either $K(X[\ell]) = K(\mathfrak{R}_f)$ or the Galois group $\mathrm{Gal}(K(X[\ell])/K(\mathfrak{R}_f))$ is a finite ℓ-group. In particular, if the order of $\mathrm{Gal}(f/K)$ is prime to n then the order of $\tilde{G}_{\ell,X,K}$ is also prime to n.*
  (ii) *The Galois module $X[\ell]$ admits a filtration*

$$M_0 = \{0\} \subset M_1 \subset \cdots \subset M_{\ell-1} = X[\ell],$$

  such that each consecutive quotient M_{i+1}/M_i is isomorphic to the Galois module $Q_{\mathfrak{R}_f}$.

Proof. Let us put

$$X[1 - \delta_\ell] := J^{(f,\ell)}[1 - \delta_\ell] \subset J^{(f,\ell)}[\ell] = X[\ell].$$

The ring $\mathbb{Z}[\delta_\ell] \otimes \mathbb{Z}_\ell =: \mathbb{Z}_\ell[\delta_\ell]$ acts naturally on the ℓ-adic Tate module $\mathrm{T}_\ell(X)$ of X. It is known [15] that $\mathrm{T}_\ell(X)$ is a free $\mathbb{Z}_\ell[\zeta_\ell]$-module of rank

$$\frac{2\dim(J^{(f,\ell)})}{[\mathbb{Q}(\zeta_\ell) : \mathbb{Q}]} = \frac{(n-1)(\ell-1)}{(\ell-1)} = n - 1.$$

In particular, the natural ring homomorphism

$$\Psi_\ell : \mathbb{Z}[\delta_\ell]/\ell = \mathbb{Z}_\ell[\delta_\ell]/\ell \to \mathrm{End}_{\mathbb{F}_\ell}(X[\ell])$$

is a ring *embedding* that makes $X[\ell]$ a free $\mathbb{Z}[\delta_\ell]/\ell$-module of rank $n-1$. This implies that

$$X[1 - \delta_\ell] = (1 - \delta_\ell)^{\ell-2} X[\ell],$$

because in the cyclotimic ring $\mathbb{Z}[\zeta_\ell]$ we have the equalities of ideals

$$\ell\mathbb{Z}[\zeta_\ell] = (1-\zeta_\ell)^{\ell-1}\mathbb{Z}[\zeta_\ell], \quad (1-\zeta_\ell)^{\ell-2}\mathbb{Z}[\zeta_\ell] = \{z \in \mathbb{Z}[\zeta_\ell] \mid (1-\zeta_\ell)z \in \ell\mathbb{Z}[\zeta_\ell]\}.$$

Now first assertion of (i) follows from Lemma 3.3 applied to

$$F = \mathbb{F}_\ell, \ V = X[\ell], \ \mathcal{N} = \Psi_\ell((1-\delta_\ell)\mathbb{Z}[\delta_\ell]/\ell),$$

and

$$\sigma \in \mathrm{Gal}(K(X[\ell]/K(X[1-\delta_\ell])) \subset \mathrm{Aut}_{\mathbb{F}_\ell}(X[\ell]).$$

The second one follows readily from the equality

$$[K(Y[\ell]) : K] = [K(Y[\ell]) : K(\mathfrak{R}_h)] \cdot [K(\mathfrak{R}_h) : K] \ )$$

(recall that the prime ℓ does *not* divide n).

In order to prove (ii), let us put

$$M_i := (1 - \delta_\ell)^{\ell-1-i}X[\ell] \subset X[\ell].$$

The freeness of the $\mathbb{Z}[\delta_\ell]/\ell$-module $X[\ell]$ implies that M_i coincides with the kernel of

$$(1 - \delta_\ell)^i : X[\ell] \to X[\ell].$$

In particular,

$$M_0 = \{0\}, \ M_1 = X[1 - \delta_\ell] \cong Q_{\mathfrak{R}_f}, \ M_{\ell-1} = X[\ell].$$

It is also clear that $(1 - \delta_\ell)^i$ induces an isomorphism of Galois modules M_{i+1}/M_i and $M_1/M_0 \cong Q_{\mathfrak{R}_f}$. This ends the proof of (ii).

$\square$

Lemma 3.6. *We keep the notation and assumptions of Theorem 2.2.*
Suppose that $K = K(Y[\ell])$. Then there is a nontrivial group homomorphism

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

whose image

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

is a finite group that enjoys the following property.

The integers n and $\#(\Gamma)$ are not relatively prime. In other words, there is a prime $r \neq \ell$ that divides both n and $\#(\Gamma)$. In particular, both endomorphism algebras $\mathrm{End}^0(J^{(f,\ell)})$ and $\mathrm{End}^0(Y)$ contain an invertible element of multiplicative order r.

Lemma 3.7. *Let ℓ and r be two distinct odd primes. Let $\mathcal{V}$ be a nonzero finite-dimensional vector space over $\mathbb{Q}$. Let A and B be two commuting automorphisms of $\mathcal{V}$ that enjoy the following properties.*

(i) *$A^\ell = B^r = 1_\mathcal{V}$ where $1_\mathcal{V}$ is the identity automorphism of $\mathcal{V}$.*
(ii) *$A - 1_\mathcal{V}$ is an automorphism of $\mathcal{V}$.*
(iii) *$B \neq 1_\mathcal{V}$.*

Then $\dim_{\mathbb{Q}}(\mathcal{V}) \geq (\ell - 1)(r - 1).$

Proof of Theorem 2.2 (modulo Lemmas 3.6 and 3.7). Recall that $X = J^{(f,\ell)}$.

It follows from Lemma 3.2 that $f(x)$ remains irreducible over $K(Y[\ell])$. So, replacing K by $K(Y[\ell])$, we may and will assume that $K(Y[\ell]) = K$. Now it follows from Lemma 3.6) that there is a prime $r \neq \ell$ that divides n and enjoys the following property.

Both endomorphism algebras $\mathrm{End}^0(X) = \mathrm{End}^0(J^{(f,\ell)})$ and $\mathrm{End}^0(Y)$ contain an invertible element of multiplicative order r. In order to finish the proof of our Theorem, we need to prove the inequality

$$\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) \geq (\ell - 1)(r - 1).$$

Let us use Lemma 3.7 applied to $\mathcal{V} = \mathrm{End}^0(X)$. We define the automorphisms $A, \ B : \mathcal{V} \to \mathcal{V}$ of the $\mathbb{Q}$-vector space $\mathcal{V} = \mathrm{End}^0(X)$ as

$$v \mapsto \delta_\ell v \ \text{ and } v \mapsto vu \quad \forall v \in \mathcal{V} = \mathrm{End}^0(X)$$

respectively. Clearly, A and B are commuting automorphisms of $\mathcal{V}$ such that both A^ℓ and B^r coincide with the *identity automorphism* $1_{\mathcal{V}}$ of $\mathcal{V}$. Since u has multiplicative order $r > 1$, $B \neq 1_{\mathcal{V}}$. On the other hand, we know that the $\mathbb{Q}$-subalgebra $\mathbb{Q}[\delta_\ell]$ of $\mathrm{End}^0(J^{(f,\ell)}) = \mathrm{End}^0(X)$ is a subfield with the same identity element as $\mathrm{End}^0(X)$. This implies that the nonzero $\delta_\ell - 1_X$ is an *invertible* element of the $\mathbb{Q}$-algebra $\mathrm{End}^0(X)$. It follows that $A - 1_{\mathcal{V}}$ is an invertible automorphism of the $\mathbb{Q}$-vector space $\mathcal{V}$. So, A and B satisfy all the conditions of Lemma 3.7. Applying Lemma 3.7, we conclude that $\dim_{\mathbb{Q}}(\mathrm{End}^0(X)) \geq (\ell - 1)(r - 1)$, which ends the proof of Theorem 2.2.

$\square$

Proof of Lemma 3.6. In light of the theorem of Silverberg (Remark 2.1(ii)), all endomorphisms of Y are defined over K. Applying this theorem (see Remark 2.1(ii) above) to $X \times Y$, we conclude that all the homomorphisms from X to Y are defined over $K(X[\ell])$.

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

$$\mu(X[\ell]) \neq \{0\}. \tag{5}$$

Let us put

$$G_\ell := \tilde{G}_{\ell,X,K} = \mathrm{Gal}(K(X[\ell])/K), \ G = \mathrm{Gal}(K(X[1-\delta_\ell])/K) = \mathrm{Gal}(f/K).$$

We know that μ is defined over $K(X[\ell])$. This allows us to define for each $\sigma \in G_\ell$ the isogeny $\sigma(\mu) : X \to Y$, which is the Galois-conjugate of μ (recall that both X and Y are defined over K). Then the same

construction as in [22, Sect. 4, proof of Prop. 2.4] allows us to define a map

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

where $c(\sigma)$ is determined by

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

We have for each $\sigma, \tau \in G_\ell$

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

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

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

This means that the map

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

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

Let H_ℓ be the kernel of χ, i.e.,

$$H_\ell = \{\sigma \in G_\ell \mid \sigma(\mu) = \mu\}. \tag{6}$$

By definition, H_ℓ is a normal subgroup of G_ℓ. Let H be the image of H_ℓ in G under the natural *surjective* group homomorphism

$$G_\ell = \mathrm{Gal}(K(X[\ell])/K) \twoheadrightarrow \mathrm{Gal}(K(X[1 - \delta_\ell])/K) =$$

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

induced by the inclusion

$$K(\mathfrak{R}_f) = K(X[1 - \delta_\ell]) \subset K(X[\ell])$$

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

$$(G_\ell : H_\ell) = \#(\Gamma).$$

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

Proposition 3.8. *The subgroup H of G is not transitive on $\mathfrak{R}_f$.*

End of Proof of Lemma 3.6 (modulo Proposition 3.8) Combining Proposition 3.8 with Lemma 3.1, we conclude that $(G : H)$ is *not* prime to n. Hence, there is a prime r that divides both $(G : H)$ and n. Since n is prime to ℓ and $(G : H)$ divides $(G_\ell : H_\ell)$, we conclude that $r \neq \ell$ and r divides $(G_\ell : H_\ell) = \#(\Gamma)$. This ends the proof.

$\square$

Proof of Proposition 3.8. Suppose that H is transitive. Then $f(x)$ remains *irreducible* over the subfield $E := K(\mathfrak{R}_f)^H$ of all H-invariants in $K(\mathfrak{R}_f) := F$. Clearly, E/K is a Galois extension and

$$K \subset E \subset F = K(\mathfrak{R}_f) = E(\mathfrak{R}_f).$$

Let us consider the subfield $L := K(X[\ell])^{H_\ell}$ of all H_ℓ-invariants in $K(X[\ell])$, which is also a Galois extension of K. We have

$$K(X[\ell]) = L(X[\ell]), \quad H_\ell = \mathrm{Gal}(K(X[\ell])/L) = \mathrm{Gal}(L(X[\ell])/L).$$

In addition,

$$K \subset L = K(X[\ell])^{H_\ell} \supset K(\mathfrak{R}_f)^H = F^H = E \supset K$$

and

$$E = F^H = F \cap K(X[\ell])^{H_\ell} = F \cap L,$$

becase H is the image of $H_\ell \subset \mathrm{Gal}(K(X[\ell])/K)$ in $\mathrm{Gal}(K(\mathfrak{R}_f)/K) = \mathrm{Gal}(F/K)$.

We want to prove that $f(x)$ remains *irreducible* over L. In order to do it, notice that H_ℓ acts transitively on $\mathfrak{R}_f$. Indeed, let α, β be elements of $\mathfrak{R}_f$. By our assumption, there is $\sigma \in H \in \mathrm{Gal}(K(\mathfrak{R}_f)/K)$ such that $\sigma(\alpha) = \beta$. Pick a field automorphism

$$\sigma_\ell \in H_\ell \subset \mathrm{Gal}(K(X[\ell])/L) \subset \mathrm{Gal}(K(X[\ell])/K)$$

such that the restriction of σ_ℓ to $K(\mathfrak{R}_f)$ coincides with σ. Since

$$\alpha \in \mathfrak{R}_f \subset K(\mathfrak{R}_f),$$

we get

$$\sigma_\ell(\alpha) = \sigma(\alpha) = \beta.$$

This proves the transitivity of of the action of H_ℓ on the set $\mathfrak{R}_f$ of roots of $f(x)$. It follows that $f(x)$ is *irreducible* over the field $K(X[\ell])^{H_\ell} = L$.

Replacing K by its overfield $L = K(X[\ell])^{H_\ell}$, we may and will assume that

$$H_\ell = \mathrm{Gal}(K(X[\ell])/K).$$

In particular,

$$\sigma(\mu) = \mu \ \forall \sigma \in H_\ell = \mathrm{Gal}(K(X[\ell])/K). \tag{7}$$

Recall that

$$\sigma(\mu)(\sigma(x)) = \sigma(\mu(x)) \ \forall \sigma \in \mathrm{Gal}(K(X[\ell])/K), \ x \in X(K[\ell]). \tag{8}$$

Since $X[\ell] \subset X(K[\ell])$ and *nonzero* $\mu(X[\ell])$ obviously lies in $Y[\ell]$, we conclude that the map

$$X[\ell] \to Y[\ell], \ x \mapsto \mu(x) \tag{9}$$

is a *nonzero* homomorphism of $\mathrm{Gal}(K)$-modules. Recall that we assume that the Galois action on $Y[\ell]$ is *trivial*. On the other hand, in light of Corollary 3.5, the Galois module $X[\ell]$ admits a filtration, all whose consecutuve quotients are isomorphic to $Q_{\mathfrak{R}_f}$. Since $f(x)$ is irreducible over K, it follows from Lemma 2.5 that the homomorphism (9) is *zero*, which is not the case. The obtained contradiction proves that H is not transitive. $\square$

Proof of Lemma 3.7. Clearly, B is a semisimple (i.e., diagonalizable over $\bar{\mathbb{Q}}$) linear operator in $\mathcal{V}$. The same is obviously true for the linear operator $B - 1_\mathcal{V} : \mathcal{V} \to \mathcal{V}$. The semisimplicity of $B - 1_\mathcal{V}$ implies that $\mathcal{V}$ splits into a direct sum

$$\mathcal{V} = (B - 1_\mathcal{V})(\mathcal{V}) \oplus \ker(B - 1_\mathcal{V})$$

of the image $(B - 1_\mathcal{V})(\mathcal{V})$ and the kernel $\ker(B - 1_\mathcal{V})$ of $B - 1_\mathcal{V}$; clearly, these two subspaces are B-invariant. In addition, the restriction of $B - 1_\mathcal{V}$ to the subspace

$$\mathcal{V}_0 := (B - 1_\mathcal{V})(\mathcal{V})$$

is an automorphism of $\mathcal{V}_0$. Recall that our conditions on B imply that

$$\mathcal{V}_0 \neq \{0\}.$$

Since A and B commute, both subspaces $(B - 1_\mathcal{V})(\mathcal{V}) = \mathcal{V}_0$ and $\ker(B - 1_\mathcal{V})$. are also A-invariant. Let

$$A_0, \; B_0 : \mathcal{V}_0 \to \mathcal{V}_0$$

be the restrictions to $\mathcal{V}_0$ of A and B respectively. Clearly, A_0 and B_0 commute, and both A_0^ℓ and B_0^r coincide with the *identity automorphism* $1_{\mathcal{V}_0}$ of $\mathcal{V}_0$. In addition, both $A_0 - 1_{\mathcal{V}_0}$ and $B - 1_{\mathcal{V}_0}$ are automorphisms of $\mathcal{V}_0$.

Let

$$\mathcal{P}_{A_0}(t), \; \mathcal{P}_{B_0}(t) \in \mathbb{Q}[t]$$

be the *minimal polynomials* of $A_0 : \mathcal{V}_0 \to \mathcal{V}_0$ and $B_0 : \mathcal{V}_0 \to \mathcal{V}_0$ respectively. Both minimal polynomials are monic of positive degree, and all their coefficients are rational numbers. Clearly, $\mathcal{P}_{A_0}(t)$ divides $t^\ell - 1$ and $\mathcal{P}_{B_0}(t)$ divides $t^r - 1$; in addition, $t - 1$ divides neither $\mathcal{P}_{A_0}(t)$ nor $\mathcal{P}_{B_0}(t)$. Recall that

$$t^\ell - 1 = (t - 1)\Phi_\ell(t), \quad t^r - 1 = (t - 1)\Phi_\ell(t)$$

where $\Phi_\ell(t)$ and $\Phi_r(t)$ are ℓth and rth cyclotomic polynomials respectively; they both are irreducible over $\mathbb{Q}$. It follows that

$$\mathcal{P}_{A_0}(t) = \Phi_\ell(t), \quad \mathcal{P}_{B_0}(t) = \Phi_r(t).$$

This implies that the $\mathbb{Q}$-subalgebra $\mathbb{Q}[A_0]$ of $\mathrm{End}_{\mathbb{Q}}(\mathcal{V}_0)$ generated by A_0 is isomorphic to the ℓth cyclotomic field

$$\mathbb{Q}[t]/\Phi_\ell(t)\mathbb{Q}[t] \cong \mathbb{Q}(\zeta_\ell).$$

Similarly, the $\mathbb{Q}$-subalgebra $\mathbb{Q}[B_0]$ of $\mathrm{End}_{\mathbb{Q}}(\mathcal{V}_0)$ generated by B_0 is isomorphic to the rth cyclotomic field

$$\mathbb{Q}[t]/\Phi_r(t)\mathbb{Q}[t] \cong \mathbb{Q}(\zeta_r).$$

Since A_0 and B_0 commute, the (commutative) $\mathbb{Q}$-subalgebras $\mathbb{Q}[A_0]$ and $\mathbb{Q}[B_0]$ also commute. This implies that the *nonzero* $\mathbb{Q}$-vector space $\mathcal{V}_0$ carries the natural structure of a module over the $\mathbb{Q}$-algebra

$$\mathbb{Q}[A_0] \otimes_{\mathbb{Q}} \mathbb{Q}[B_0] \cong \mathbb{Q}(\zeta_\ell) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_r).$$

Since r and ℓ are distinct odd primes, the cyclotomic fields $\mathbb{Q}(\zeta_\ell)$ and $\mathbb{Q}\mathbb{Q}(\zeta_r)$ are linearly disjoint over $\mathbb{Q}$; actually, this tensor product is canonically isomorphic to ℓrth cyclotomic field $\mathbb{Q}(\zeta_{\ell r})$ of degree $(\ell - 1)(r - 1)$. It follows that $\mathcal{V}_0$ carries the natural structure of a $\mathbb{Q}(\zeta_{\ell r})$-vector space. Hence, $\dim_{\mathbb{Q}}(\mathcal{V}_0)$ is divisible by the degree

$$[\mathbb{Q}(\zeta_{\ell r}) : \mathbb{Q}] = (\ell - 1)(r - 1).$$

Since $\mathcal{V}_0 \ne \{0\}$, we conclude that $\dim_{\mathbb{Q}}(\mathcal{V}_0) \ge (\ell - 1)(r - 1)$. Taking into account that $\mathcal{V}_0$ is a subspace of $\mathcal{V}$, we conclude that

$$\dim_{\mathbb{Q}}(\mathcal{V}) \ge \dim_{\mathbb{Q}}(\mathcal{V}_0) \ge (\ell - 1)(r - 1).$$

This ends the proof of our Lemma. $\qquad\qquad\qquad\qquad\qquad\square$

4. Proof of Theorem 1.1

So, n is an odd *prime*, both $f(x)$ and $h(x) \in K[x]$ are degree n polynomials without repeated roots, $f(x)$ is irreducible and $h(x)$ is reducible. Since n is a prime, the reducibility of $h(x)$ implies that the order of $\mathrm{Gal}(h/K)$ is prime to n (see [22, Lemma 2.6]). Let us put $Y = J^{(h,\ell)}$. We are given that the degree $[K(\mathfrak{R}_h) : K]$ of the field extension $K(\mathfrak{R}_h)/K$ is *not* divisible by n. Applying Corollary 3.5 to Y and $h(x)$ (instead of $X = J^{(f,\ell)}$ and $f(x)$), we conclude that the order of the group $\tilde{G}_{\ell,Y,K}$ is prime to n. Now the desired result follows readily from Theorem 2.2, because if r is a prime divisor of n then $r = n$.

5. Doubly transitive and cyclic Galois groups

Proof of Corollary 1.4. By definition of the field

$$K_h := K(\mathfrak{R}_h),$$

the polynomial $h(x)$ splits into a product of linear factors over K_h. Recall that $\mathrm{Gal}(K_h/K) = \mathrm{Gal}(h/K)$ is a *cyclic* group of prime order

n and $\mathrm{Gal}(f/K) = \mathrm{Gal}(K(\mathfrak{R}_f)/K)$ is *doubly transitive*. In light of Proposition 1.8 of [22], the field extensions $K(\mathfrak{R}_f)/K$ and K_h/K are *linearly disjoint*. This implies that $f(x)$ remains irreducible over K_h. Now the desired result follows readily from Theorem 1.1 applied to $f(x)$ and $h(x)$ over K_h (instead of K). $\qquad\square$

References

[1] R. Coleman, *On the Galois groups of the exponential Taylor polynomials.* Enseign. Math. (2) **33** (1987), no. 3–4, 183–189.

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

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

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

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

[6] S. Lang, Algebra, third edition. Springer Verlag, New York, 2002.

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

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

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

[10] H. Osada, *The Galois goups of the polynomials $X^n + aX^l + b$.* J. Number Theory **25:2** (1987), 230–238.

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

[12] B. Poonen, E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line.* J. reine angew. Math. **488** (1997), 141–188.

[13] E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve.* Math. Ann. **310** (1998), 447–471.

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

[15] K.A. Ribet, *Galois Action on Division Points of Abelian Varieties with Real Multiplications.* Amer. J. Math. **98:3** (1976), 751–804.

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

[17] Yu. G. Zarhin, *Cyclic covers of the projective line, their jacobians and endomorphisms.* J. reine angew. Math. **544** (2002), 91–110.

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

[19] Yu. G. Zarhin, *The endomorphism rings of Jacobians of cyclic covers of the projective line.* Math. Proc. Cambridge Philos. Soc. **136:2** (2004), 257–267.

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

[21] Yu. G. Zarhin, *Endomorphism algebras of abelian varieties with special reference to superelliptic jacobians.* In: Geometry, Algebra, Number Theory, and their information technology applications, p. 477–528 (A. Akbary, S. Gun, eds). Springer Nature Switzerland AG, 2018.

[22] Yu. G. Zarhin, *Non-isogenous elliptic curves and hyperelliptic jacobians.* Math. Research Letters **30** (2023), 267–294.

[23] Yu. G. Zarhin, *Non-isogenous elliptic curves and hyperelliptic jacobians* II. Algebraic Geometry and Physics **1:2**, to appear; arXiv:2204.10567 [math.NT].

[24] Yu. G. Zarhin, *Superelliptic jacobians and central simple representations.* arXiv:2305.12022 [math.NT].

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

Email address: zarhin@math.psu.edu