

A Torelli theorem for curves over finite fields

Fedor Bogomolov, Mikhail Korotiaev and Yuri Tschinkel
Courant Institute of Mathematical Sciences, N.Y.U.
251 Mercer str., New York, NY 10012, U.S.A.

To John Tate, with admiration

Abstract. We study hyperbolic curves and their Jacobians over finite fields in the context of anabelian geometry.

1. Introduction

This paper is inspired by the foundational results and ideas of John Tate in the theory of abelian varieties over finite fields. To this day, the depth of this theory has not been fully explored. Here we apply Tate's theorems to anabelian geometry of curves over finite fields.

Let C be an irreducible smooth projective curve of genus $g = g(C) \geq 2$ defined over a field k and let $C(k)$ be its set of k -rational points. When k is the field of complex numbers, the complex torus

$$H^0(C(\mathbb{C}), \Omega_C^1)^\vee / H_1(C(\mathbb{C}), \mathbb{Z})$$

is the set of complex points of an algebraic variety, the Jacobian variety J of C . Choosing a point $c_0 \in C(\mathbb{C})$ we get a map

$$\begin{aligned} C(\mathbb{C}) &\rightarrow J(\mathbb{C}) \\ c &\mapsto (\omega \mapsto \int_\gamma \omega), \end{aligned}$$

where $\omega \in \Omega_C^1$ is a global section of the sheaf of holomorphic differentials on C and γ is any path from c_0 to c . In a more algebraic interpretation, the abelian group $J(\mathbb{C})$ is isomorphic to $\text{Pic}^0(C)$, the group of degree-zero divisors on C modulo principal divisors, and the map above is simply:

$$\begin{aligned} C(\mathbb{C}) &\rightarrow J(\mathbb{C}) \\ c &\mapsto c - c_0. \end{aligned}$$

This construction can be carried out over any field k , provided the basepoint c_0 is defined over k , by a fundamental result of Weil, the Jacobian J is defined over the field of definition of C , and the set-theoretic maps above arise from k -morphisms.

For each $n \in \mathbb{N}$, we get maps

$$C^n(k) \xrightarrow{\sigma_n} C^{(n)}(k) \xrightarrow{\varphi_n} J(k)$$

where C^n is the n -th power and $C^{(n)} = C^n/\mathfrak{S}_n$ is the n -th symmetric power of C , i.e., $C^{(n)}(k)$ is the set of effective degree- n zero-cycles on C which are defined over k . The map to the Jacobian assigns to a degree- n zero-cycle $c_1 + \dots + c_n \in C^{(n)}(k)$ the degree-0 zero-cycle $(c_1 + \dots + c_n) - nc_0$. The maps φ_n capture interesting geometric information. For example, φ_g is birational, which leads to an alternative definition of J as the unique abelian variety birational to $C^{(g)}$. The locus $\Theta := \varphi_{g-1}(C^{(g-1)}) \subset J$ is an ample divisor, the theta-divisor. The classical Torelli theorem says that the pair (J, Θ) , consisting of the Jacobian J of C and its polarization Θ , determines C up to isomorphism. This theorem holds over any field and is one of the main tools in geometric and arithmetic investigations of algebraic curves, relating these to much more symmetric objects - abelian varieties.

From now on, let k_0 be a finite field of characteristic p and $k = \bar{k}_0$ an algebraic closure of k_0 . Recall that $J(k)$ is a torsion abelian group, with ℓ -primary part

$$J\{\ell\} \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}, \quad \text{for } \ell \neq p.$$

The description of $J\{p\}$ is slightly more complicated: there exists a nonnegative integer $n \leq g$ such that $J\{p\} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^n$. Nevertheless, as an abstract abelian group, $J(k)$ depends “almost” only on the genus g of C . The procyclic Galois group of k/k_0 acts on $J(k)$ and one can consider the Galois representation on the Tate-module:

$$T_\ell(J) := \varprojlim J[\ell^n], \quad \ell \neq p,$$

where $J[\ell^n] \subset J(k)$ is the subgroup of ℓ^n -torsion points. Let F_J be the characteristic polynomial of the Frobenius endomorphism on

$$V_\ell(J) := T_\ell(J) \otimes \mathbb{Q}_\ell.$$

By a fundamental result of Tate, F_J determines the Jacobian as an algebraic variety, modulo isogenies:

Theorem 1.1 (Tate [Tat66]). *Let J, \tilde{J} be abelian varieties over k_0 and $F_J, F_{\tilde{J}} \in \mathbb{Z}[T]$ the characteristic polynomials of the k_0 -Frobenius endomorphism Fr acting on $V_\ell(J)$, resp. $V_\ell(\tilde{J})$. Then*

$$\text{Hom}(J, \tilde{J}) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \text{Hom}_{\mathbb{Z}_\ell[\text{Fr}]}(T_\ell(J), T_\ell(\tilde{J})).$$

The abelian varieties J and \tilde{J} are isogenous if and only if $F_J = F_{\tilde{J}}$.

In particular, while the Galois-module structure of $J(k)$ distinguishes J in a rather strong sense (but not up to isomorphism of abelian varieties, an example can be found in [Zar08], Section 12), the group structure of $J(k)$ does not.

In this paper, we investigate a certain “group-theoretic” analog of the Torelli theorem for curves over *finite* fields. This analog has a natural setting in the anabelian geometry of curves. Throughout, we work in characteristic ≥ 3 .

Let J^1 be the Jacobian of (degree-1 zero-cycles of) C and

$$\begin{array}{ccc} j_1 : C(k) & \hookrightarrow & J^1(k) \\ c & \mapsto & [c] \end{array} \quad (1)$$

the corresponding embedding. The Jacobian J of degree-0 zero-cycles on C acts on J^1 , translating by points $c \in C(k)$. Let \tilde{C} , resp. \tilde{J} , be another smooth projective curve, resp. its Jacobian. We will say that

$$\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$$

is an isomorphism of pairs if there exists a diagram

$$\begin{array}{ccccc} J(k) & & J^1(k) & \xleftarrow{j_1} & C(k) \\ \phi^0 \downarrow & & \phi^1 \downarrow & & \phi_s \downarrow \\ \tilde{J}(k) & & \tilde{J}^1(k) & \xleftarrow{\tilde{j}_1} & \tilde{C}(k) \end{array}$$

where

- ϕ^0 is an isomorphism of abstract abelian groups;
- ϕ^1 is an isomorphism of homogeneous spaces, compatible with ϕ^0 ;
- the restriction $\phi_s : C(k) \rightarrow \tilde{C}(k)$ of ϕ^1 is a bijection of sets.

Our main result is:

Theorem 1.2. *Let $k = \bar{\mathbb{F}}_p$, with $p \geq 3$, and let C, \tilde{C} be smooth projective curves over k of genus ≥ 2 , with Jacobians J , resp. \tilde{J} . Suppose that there exists an isomorphism of pairs*

$$\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J}).$$

Then J and \tilde{J} are isogenous.

Conjecture 1.3. *Under the assumptions of Theorem 1.2, C and \tilde{C} are isomorphic as algebraic varieties, modulo Frobenius twisting.*

There are examples of geometrically nonisomorphic curves over finite fields with isomorphic Jacobians, as (unpolarized) algebraic varieties over k_0 . Pairs of such curves are given by

$$y^2 = (x^3 + 1)(x^3 - 1) \quad \text{and} \quad y^2 = (x^3 - 1)(x^3 - 4)$$

over \mathbb{F}_{11} with Jacobian $E \times E$, for a supersingular elliptic curve E , or

$$y^2 = x^5 + x^3 + x^2 - x - 1 \quad \text{and} \quad y^2 = x^5 - x^3 + x^2 - x - 1$$

over \mathbb{F}_3 , with a geometrically simple Jacobian (see [IKO86], [How96] and the references therein).

Theorem 1.2 was motivated by Grothendieck's anabelian geometry. This is a program relating algebraic fundamental groups of hyperbolic varieties over arithmetic fields to the underlying algebraic structure. One of the recent theorems in this direction is due to A. Tamagawa: Let Π be a *nonabelian* profinite group. Then there are at most finitely many curves over $k = \overline{\mathbb{F}}_p$ with tame fundamental group isomorphic to Π [Tam04]. Tamagawa generalized previous results by Pop-Saidi [PS03] and Raynaud [Ray02], who proved similar statements under some technical restrictions on curves. The main new ingredient in Tamagawa's proof is a delicate geometric analysis of special loci in Jacobians.

In the second part of this paper, we apply Theorem 1.2 to a somewhat orthogonal problem. Namely, we focus on the prime to p part of the *abelianization* of the absolute Galois group of the function field of the curve, together with the set of valuation subgroups. Our main result (Theorem 8.4) is that for projective curves C over k , of genus $g(C) > 3$, the pair $(\mathcal{G}_K^a, \mathcal{I})$, consisting of the abelianization of the Galois group of $K = k(C)$ and the set $\mathcal{I} = \{I_\nu^a\}_\nu$ of inertia subgroups $I_\nu^a \subset \mathcal{G}_K^a$ corresponding to nontrivial valuations of K , determines the isogeny class of the Jacobian of C .

Here is a road-map of the paper. In Section 2, included as a motivation for Conjecture 1.3, we discuss certain subvarieties of moduli spaces of curves cut out by conditions on the order of zero-cycles of the form $c - c'$ on C in the group $J(k)$ (i.e., images of Hurwitz schemes and their intersections). Typically, very few such conditions suffice to determine C , up to a *finite* choice. In Section 3 we study the formal automorphism group G_C of the pair (C, J) and derive some of its basic properties. In Section 4 we collect several group-theoretic results about profinite groups which we apply in Section 5 to prove that any elements $\gamma, \tilde{\gamma} \in G_C$ have the property that some integral powers $\gamma^n, \tilde{\gamma}^{\tilde{n}}$ commute. We then prove that this holds for the Frobenius endomorphisms $\phi^0(\text{Fr})$ and $\tilde{\text{Fr}}$, as elements in $\text{Aut}(\tilde{J}(k))$, whenever we have an isomorphism of pairs $\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$. In Section 6 we apply the theory of integer-valued linear recurrences as in [CZ02] to obtain a sufficient condition for isogeny of abelian varieties. In Section 7 we construct towers of degree-2 field extensions

$$k_0 \subset \dots \subset k_n \subset \dots \subset k_\infty, \quad \text{resp.} \quad \tilde{k}_0 \subset \dots \subset \tilde{k}_n \subset \dots \subset \tilde{k}_\infty,$$

provide set-theoretic intrinsic definitions of $J(k_n)$, resp. $\tilde{J}(\tilde{k}_n)$, and establish that

$$\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n), \quad \text{for all } n.$$

Combining Tate's theorem 1.1 with Theorem 6.3 we conclude that J and \tilde{J} are isogenous. In Section 8 we discuss extensions and applications of Theorem 1.2 to anabelian geometry.

Acknowledgments: We very much appreciate the extremely helpful reports by the referee. We are grateful to A. Venkatesh and U. Zannier for useful suggestions, and to B. Hassett, L. Kindler and Yu. Zarhin for their comments. The first author was partially supported by NSF grant DMS-0701578. The third author was partially supported by NSF grant DMS-0602333.

2. Curves and their moduli

Let k_0 be a finite field of characteristic p and let k be an algebraic closure of k_0 . Let C be an irreducible smooth projective curve of genus $\mathbf{g} = \mathbf{g}(C) > 1$ over k_0 with $C(k_0) \neq \emptyset$, and let $J = J_C$ be its Jacobian. The Jacobian of degree-1 zero-cycles J^1 is a principal homogeneous space for J . For ℓ a prime number let

$$J\{\ell\} := \cup_{n \in \mathbb{N}} J[\ell^n] \subset J(k), \quad \text{resp.} \quad T_\ell(J) = \varprojlim J[\ell^n]$$

be the ℓ -primary part of $J(k)$, resp. the Tate-module. For any set of primes S , put

$$J\{S\} := \bigoplus_{\ell \in S} J\{\ell\} \subset J(k).$$

The order of $x \in J(k)$ will be denoted by $\text{ord}(x)$.

Lemma 2.1. Let C be a curve of genus $\mathbf{g} > 1$. Let J be its Jacobian and $a \in J(k)$ be such that

$$a + C(k) \subset C(k) \subset J^1(k).$$

Then $a = 0$.

Proof. Let $\langle a \rangle$ be the cyclic subgroup generated by a and let n be its order. The translation by a gives an action of $\langle a \rangle$ on J^1 and a separable unramified covering $C \rightarrow C/\langle a \rangle$ of degree n . The quotient $\bar{J} := J/\langle a \rangle$ acts on the corresponding principal homogeneous space $\bar{J}^1 = J^1/\langle a \rangle$. The image \bar{C} of C under the projection $J^1 \rightarrow \bar{J}^1$ has genus $\bar{\mathbf{g}} = \mathbf{g}/n - 1/n + 1 < \mathbf{g}$, since $n \geq 2$ and $\mathbf{g}(C) \geq 2$. Hence the Jacobian of \bar{C} is a proper abelian subvariety of \bar{J} , of dimension at most $\bar{\mathbf{g}}$. It follows that the same holds for its preimage C , contradicting the fact that C generates J . \square

Definition 2.2. An ordered set $R_n = \{r_1, \dots, r_n\}$ of integers $r_j > 1$ will be called an n -string. Let J be an abelian variety over k and $X \subset J(k)$. An ordered subset $\{x_0, x_1, \dots, x_n\} \subset X$ will be called an R_n -configuration on X if $r_j = \text{ord}(x_j - x_0)$, for $1 \leq j \leq n$.

We will mostly consider the case when $X = C(k) \hookrightarrow J(k)$, where C is a curve of genus $g = g(C) \geq 1$. Note that an isomorphism of pairs $\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$ preserves all configurations, i.e., for all $n \in \mathbb{N}$, every R_n -configuration in $C(k) \subset J(k)$ is mapped to an R_n -configuration in $\tilde{C}(k) \subset \tilde{J}(k)$. In particular, ϕ maps equivalent effective divisors on C to equivalent divisors on \tilde{C} . Since the projective dimension of the space of global sections of a divisor D on a curve is defined as the maximal degree of an effective divisor D' such that $D - D'$ is still effective, the isomorphism ϕ respects these dimensions. Since the canonical class on a curve of genus ≥ 2 is the unique class of dimension $2g - 2$, the map ϕ maps a canonical divisor of C to a canonical divisor of \tilde{C} . However, *a priori*, the corresponding set-theoretic bijection

$$\mathbb{P}(\mathbf{H}^0(C, K_C))(k) \leftrightarrow \mathbb{P}(\mathbf{H}^0(\tilde{C}, K_{\tilde{C}}))(\tilde{k})$$

does not preserve the projective structure. If we had an isomorphism of projective structures, we would immediately obtain an isomorphism of curves, as algebraic varieties.

Theorem 2.3. *Let C be a curve over $k = \bar{\mathbb{F}}_p$ of genus $g > 1$. Then there exists an n -string R_n , with $n < 3g - 2$ such that*

- $C(k) \subset J(k)$ contains an R_n -configuration,
- there exist at most finitely many nonisomorphic curves of genus g containing an R_n -configuration.

Proof. We write $\mathcal{M}_{g,n}$ for the moduli space (stack) of genus g curves with n -marked points. The subvariety of \mathcal{M}_g parametrizing curves with an R_n -configuration is contained in the intersection of varieties corresponding to configurations of order 1 built from appropriate subsets of R_n .

Every 1-string $R_1 = \{r_1\}$ defines an algebraic subvariety $\mathcal{D}_{R_1,g} \subset \mathcal{M}_{g,1}$. By [Hru96] and [PR04], the number of points of finite order on a nonisotrivial curve embedded into an abelian variety, over a function field of positive dimension, is bounded. Applying this theorem to the Jacobian fibration of the universal curve over the function field of \mathcal{M}_g , we conclude that the subvariety $\mathcal{D}_{R_1,g}$ projects with finite fibers onto a *proper* subvariety of \mathcal{M}_g for all $r_1 \gg 0$. Now we can proceed by induction. Assume that C contains an R_n -configuration $\{c_0, \dots, c_n\} \subset C(k)$ and let $\mathcal{D}_{R_n} \subset \mathcal{M}_{g,1}$ be a union of irreducible subvarieties of dimension $\leq 3g - n$, corresponding to curves with such a configuration, each having a finite map onto a subvariety of \mathcal{M}_g . Using [Hru96] and [PR04] for each irreducible component \mathcal{D} of \mathcal{D}_{R_n} we conclude that there exists an N_{r+1} such that:

1. there is a point $c_{r+1} \in C(k)$ with $c_{r+1} - c_0$ of order N_{r+1} ,
2. in each irreducible component of \mathcal{D}_{R_r} the subvariety parametrizing curves with a torsion point of order N_{r+1} is proper.

Iterating this, in at most $3g - 2$ steps we obtain a string R and a zero-dimensional variety \mathcal{D} such that $C(k)$ contains an R -configuration which distinguishes C from all but finitely many other genus g curves over k . \square

Remark 2.4. Over \mathbb{C} , the Hurwitz scheme parametrizing genus g curves admitting a degree- m map onto \mathbb{P}^1 , with ramification of degree m at two distinct points, is irreducible and has dimension $2g-1$. The generic point of this scheme corresponds to a cover with simple additional ramification points whose images are all distinct. Indeed, a cycle c_1-c_0 of order m defines a function f on C with divisor $m(c_1-c_0)$, and thus a cover $C \rightarrow \mathbb{P}^1$ of degree m , which is totally ramified over two points: $0, \infty$. The genus computation gives an upper bound of $2g$ for the number of additional ramification points. Since there are only finitely many covers of fixed degree with fixed branch points in \mathbb{P}^1 , the dimension of the corresponding Hurwitz scheme is bounded by $2g-1$.

We have $\dim \mathcal{M}_{g,1} = 3g-2$ and $\text{codim } \mathcal{D}_{r_1,g} = g-1$. Accordingly, a general 3-configuration should give a subvariety of dimension 1 in $\mathcal{M}_{g,1}$ and a 4-configuration - a zero-dimensional subvariety in $\mathcal{M}_{g,1}$.

Conjecture 2.5. *For any curve C of genus $g(C) \geq 2$ there exist a string R_4 and an R_4 -configuration on C such that there are only finitely many curves \tilde{C} with an R_4 -configuration on \tilde{C} realizing the R_4 -string. Moreover, all such curves and such R_4 -configurations are Galois conjugated.*

Clearly, this would imply a strong version of Conjecture 1.3.

Remark 2.6. Consider $R_3 = \{2, 3\}$. Transversality would give $3g-2-(2g-2) = g$ in this case. However, the corresponding intersection is trivial.

Indeed, in general the set of solutions $nc_0 = nc$ is trivial for odd $n \leq g-1$, and a point c_0 invariant under a hyperelliptic involution. For $n \leq g-1$ and n even the point c is always invariant under a hyperelliptic involution.

In fact, we have a “supertransversality” for these Hurwitz schemes.

Proposition 2.7. *Let r_1, r'_1 be coprime integers. Let $R_1 = \{r_1\}$ and $R'_1 = \{r'_1\}$ be the corresponding 1-strings and $\mathcal{Z} := \mathcal{D}_{R_1,g} \cap \mathcal{D}_{R'_1,g} \subset \mathcal{M}_{g,1}$ the intersection of the associated Hurwitz schemes. Then $\mathcal{Z} = \emptyset$, provided $g \geq (r_1-1)(r'_1-1)/2$.*

Proof. The coprimality condition implies that the pair of functions $(f_{r_1}, f_{r'_1})$, with divisors $r_1(c_1-c_0)$, resp. $r'_1(c'_1-c_0)$, realizing the configuration, gives a map $C \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$, birational onto its image. The family of such curves in $\mathbb{P}^1 \times \mathbb{P}^1$ is algebraic. Hence $g(C) \leq (r_1-1)(r'_1-1)/2$. Indeed, a smooth curve in the family has genus $g = (C(C+K)/2) + 1$ (where $K = K_{\mathbb{P}^1 \times \mathbb{P}^1}$ is the canonical class) which gives

$$(r_1H+r'_1H')((r'_1-2)H+(r_1-2)H')/2+1 = (2r_1r'_1-2r_1-2r'_1)/2+1 = (r_1-1)(r'_1-1).$$

The image of C in $\mathbb{P}^1 \times \mathbb{P}^1$ has a singularity in the image of c_0 , the same singularity as the rational curve $(t^{r_1}, t^{r'_1})$. This rational curve has the same homology class as C and has exactly two equivalent singularities, at $(0,0)$ and at (∞, ∞) . Thus if $(r_1-1)(r'_1-1) - 2\delta(r_1, r'_1) = 0$ then the defect of the singularity is $\delta(r_1, r'_1) = (r_1-1)(r'_1-1)/2$, which gives a lower bound for the defect for C . Hence $g(C) \leq (r_1-1)(r'_1-1)/2$. \square

Conjecture 2.8. Let $r_1, r'_1, r''_1 \in \mathbb{N}$ be pairwise coprime, let $f_{r_1}, f_{r'_1}, f_{r''_1} \in k(C)$ be functions as above and $\lambda \in k^* \setminus \{1\}$. Assume that there are four points $c_0, c_1, c_2, c_3 \in C(k)$ such that

$$\begin{aligned}\operatorname{div}(f_{r_1}) &= r_1(c_0 - c_1) \\ \operatorname{div}(f_{r'_1}) &= r'_1(c_0 - c_2) \\ \operatorname{div}(f_{r''_1}) &= r''_1(c_0 - c_3)\end{aligned}$$

and such that

$$f_{r_1}(c_2) = 1 \text{ and } f_{r_1}(c_3) = \lambda.$$

Then there are only finitely many curves \tilde{C} with the same property.

This would imply that the 3-point scheme intersection

$$\mathcal{D}_{R_1, \mathfrak{g}} \cap \mathcal{D}_{R'_1, \mathfrak{g}} \cap \mathcal{D}_{R''_1, \mathfrak{g}} \subset \mathcal{M}_{\mathfrak{g}, 1}$$

has dimension at most 1, and, using the argument in the proof of Theorem 2.3, the claim in Conjecture 2.5 concerning the finiteness of the set of curves with prescribed 4-strings. We don't know whether or not this intersection is irreducible. We would expect it at least for sufficiently large coprime r_1, r'_1, r''_1 .

3. Formal automorphisms

Let A be an abelian variety defined over an algebraic closure k of a finite field, A^1 a principal homogeneous space for A and $X \subset A^1$ a closed subvariety not preserved by the action of an abelian subvariety of A of positive dimension.

Lemma 3.1. The subgroup

$$\operatorname{Stab}_X := \{a \in A(k) \mid a + X(k) \subset X(k)\}$$

is finite.

Proof. See, e.g., [Abr94]. □

Let $\operatorname{Aut}(A)$ be the group of automorphisms of the torsion abelian group $A(k)$ and let $\operatorname{Aut}(A)^{\text{aff}}$ be the group of affine automorphisms of the principal homogeneous space $A^1(k)$. We have

$$\operatorname{Aut}(A) = \operatorname{Aut}(A)_p \times \prod_{\ell \neq p} \operatorname{GL}_{2d}(\mathbb{Z}_\ell),$$

with $d = \dim A$ and $\operatorname{Aut}(A)_p = \operatorname{GL}_t(\mathbb{Z}_p)$, where t is the rank of the étale p -subgroup of $A(k)$. There is a split affine extension

$$1 \rightarrow A(k) \rightarrow \operatorname{Aut}(A)^{\text{aff}} \xrightarrow{\theta} \operatorname{Aut}(A) \rightarrow 1, \quad (2)$$

where the projection ϱ corresponds to the action on zero-cycles. Let

$$G_X := \{\gamma \in \text{Aut}(A)^{\text{aff}} \mid \gamma(X(k)) \subseteq X(k) \subset A^1(k)\}$$

be the subgroup preserving $X(k)$. We call G_X the group of automorphisms of the pair (X, A) .

Lemma 3.2. The projection of G_X to $\text{Aut}(A)$ has finite kernel.

Proof. Follows from Lemma 3.1. \square

Lemma 3.3. For every $a \in A^1(k)$ the intersection $G_a \cap G_X$ has finite index in G_X .

Proof. Consider

$$G_X \subset \text{Aut}(A)^{\text{aff}} \xrightarrow{\varrho} \text{Aut}(A)$$

and let ϱ_X be the restriction of ϱ to G_X . For each $\alpha \in A(k)$ let $G_{\alpha, X} \subset G_X$ be the preimage of the intersection of $\varrho(G_X)$ with the stabilizer of α in $\text{Aut}(A)$. The group $G_{\alpha, X}$ has finite index in G_X since the order of α is unchanged under an automorphism of X . Hence, if $G_a \cap G_X$ has finite index in G_X for at least one point $a \in A^1(k)$, we have the same property for all points.

We now assume that $a \in X(k)$. Put

$$X_a := \bigcap_{x \in X(k)} (X(k) + (a - x)).$$

Then X_a is the set of k -points of an algebraic subvariety of X , containing a . Since the intersection runs over k -points of an algebraic variety, we can find finitely many x_1, \dots, x_r such that

$$X_a = \bigcap_{j=1}^r (X(k) + \alpha_j) \quad \text{with } \alpha_j := a - x_j.$$

We have, for all j ,

$$(G_{X_a} \cap G_X) \supseteq \bigcap_j G_{\alpha_j, X},$$

as a subgroup of finite index. If X_a is finite then $G_a \cap G_X$ has finite index in G_X , as claimed. Otherwise, note that for all $a' \in X(k)$, $X_{a'}$ is a translate of X_a by $a' - a$. In particular, if $a' \in X_a$ then

$$a' = x' + (a - x),$$

for some $x' \in X(k)$. Thus, for any $x \in X(k)$ the translate $x + (a' - a) \in X(k)$ so that $X(k) = X(k) + (a - a')$. Conversely, X_a is also invariant under translations by $a - a'$, provided $a, a' \in X_a$, i.e., X_a is a principal homogeneous space for (k -points of) a positive-dimensional subvariety of A , which preserves X . This contradicts our assumptions on X . \square

Remark 3.4. The group G_X always contains the procyclic subgroup $\hat{\mathbb{Z}}$ generated by a Frobenius automorphism, and its extension by a finite group of algebraic automorphisms of the pair (X, A) .

Proposition 3.5. *Let A be an abelian variety of dimension d . Let $X \subset A^1$ be a subvariety which is not preserved under translations by a positive-dimensional abelian subvariety of A . Assume that all components of X have dimension ≥ 1 . Let G_X be the group of automorphisms of the pair (X, A) . Let*

$$\psi = \prod_{\ell} \psi_{\ell} : G_X \rightarrow \mathrm{GL}_t(\mathbb{Z}_p) \times \prod_{\ell \neq p} \mathrm{GL}_{2d}(\mathbb{Z}_{\ell}), \quad t \in [0, d],$$

be the corresponding homomorphism. Then, for all $\gamma \in G_X \setminus \mathrm{Ker}(\psi)$, there are infinitely many ℓ such that $\psi_{\ell}(\gamma) \neq 1$.

Proof.

Step 1. Fix $\gamma \in G_X$ and $x_0 \in X(k)$ and write $\gamma(x) - x_0 = \beta_{\gamma}(x - x_0) + a_{\gamma} \in A(k)$, where $\beta_{\gamma} = \varrho(\gamma)$ (see Equation (2)) and $a_{\gamma} \in A(k)$ is an affine translation. In particular, if β_{γ} acts trivially on $A\{\ell\}$ and a_{γ} projects to $0 \in A\{\ell\}$, for $\ell \notin S$, then the action of γ is trivial on the fibers of the projection $A^1(k) \rightarrow A^1(k)/\oplus_{\ell \notin S} A\{\ell\}$.

Step 2. Assume that $\beta_{\gamma} \neq 1$. Then for any $x \in A^1(k)/\oplus_{\ell \notin S} A\{\ell\}$, with $\gamma(x) \neq x$ define $X_{\gamma(x)} := X \cap (X + (\gamma(x) - x))$. By assumption on γ and the projection, $X_{\gamma(x)}$ contains all points of X over x .

Step 3. Let us show that X is invariant under translations by $\gamma(x) - x$. Assume on the contrary that $X_{\gamma(x)}$ is a proper subvariety of X . Thus for some component $X_i \subset X$, with $\dim(X_i) > 0$, the intersection $X_{\gamma(x)} \cap X_i \subsetneq X_i$. Then there is a curve $C \in X_i$ which has finite intersection with $X_{i, \gamma(x)}$. However, the intersection of C with the preimage of $\gamma(x)$ is infinite (see Theorem 5.5 and [BT05]), contradiction.

Step 4. Hence, for any $x \in A^1(k)$, the element $\gamma(x) - x$ belongs to the subgroup of those translations which keep X invariant. By our assumptions on X , this subgroup is finite.

Step 5. The group generated by $\gamma(x) - x, x \in A\{S\}$ is finite only if the $\beta_{\gamma} = 1$. Assume the contrary. Consider the action of γ on $A\{\ell\}$, for $\ell \in S$. The group generated by $\beta_{\gamma}(x) - x$ in $A\{\ell\}$ is infinite unless $\beta_{\gamma} = 1$. Indeed, if $\beta_{\gamma}(x) - x = y$ then $n(\beta_{\gamma}(x/n) - x/n) = y$ and hence the image of $(\beta_{\gamma} - 1)$ is a divisible subgroup of $A\{\ell\}$ and hence infinite for the linearized action of $\beta_{\gamma} \neq 1$. On the other hand, the group R generated by projections of $\gamma(x) - x$ to $A\{\ell\}, x \in A^1(k)$ contains the group R_{ℓ} generated by $\beta_{\gamma}(z) - z, z \in A\{\ell\}$ as a subgroup of finite index. Indeed, if we write $z = x - y, x, y \in R$ then $\beta_{\gamma}(z) - z = \gamma(x) - x - (\gamma(y) - y)$. Thus R_{ℓ} has to be trivial for R to be finite which implies that $\beta_{\gamma}(z) - z = 0$ for any $z \in A\{\ell\}, \ell \in S$. \square

Definition 3.6. *A homomorphism of abelian groups $\phi^0 : A(k) \rightarrow A(k)$ is called a formal endomorphism if it arises from a sequence $\{\phi_i^0\}$ of algebraic endomor-*

phisms $\phi_i^0 : A \rightarrow A$, with the property that for all finite subgroups $G \subset A(k)$, there exists an $n(G) \in \mathbb{N}$ such that $\phi_i^0|_G = \phi^0|_G$, for all $i \geq n(G)$.

An example is a $\hat{\mathbb{Z}}^*$ -power of the Frobenius endomorphism $\text{Fr} \in \text{End}_{k_0}(A)$.

Proposition 3.7. *Let (X, A) be a pair as in Proposition 3.5 and let $\gamma \in G_X$ be an element which commutes with the Frobenius action. Then $\varrho(\gamma)$ is a formal endomorphism.*

Proof. Recall that the endomorphism ring $\text{End}(A)$ is finitely-generated over \mathbb{Z} and that $\text{End}(A)_{\mathbb{Q}}$ is a sum of simple algebras over \mathbb{Q} corresponding to simple components of the isogeny type of A . Any element in $\text{End}(A)$ with non-trivial projection into the factors defines an endomorphism of A . Note that $\prod_{\ell \neq p} \text{End}(T_{\ell}) \times \text{End}(T_p^{et})$ contains a subalgebra E_F of elements commuting with the action of Frobenius on $T_{\ell}, \ell \neq p$ and T_p^{et} .

The statement of the lemma is equivalent to the existence, for any $h \in E_F$ and any finite subgroup $S \subset A(k)$, of an $h' \in \text{End}(A)$ such that $h' = h$ on S . If S is an ℓ -group then the result follows from Tate's theorem, which identifies $\text{End}(A) \otimes \mathbb{Z}_{\ell}$ with the centralizer of the ℓ -component of E_F . Similar result for any S of order coprime to p follows from the density of $\text{End}(A)$ under projection to any finite product of $\text{End}(T_{\ell})$. Tate's theorem implies the same result for the full p -divisible subgroup A_p of A . Note that A_p splits functorially into a product of the étale A_p^{et} and the local A_p^0 parts. In order to prove the lemma it suffices to extend an endomorphism of A_p^{et} , which commutes with the Frobenius endomorphism, to an endomorphism of A_p . The action of Frobenius respects the splitting above. Thus we can always extend an automorphism of A_p^{et} by identity on A_p^0 . If the endomorphism of A_p^{et} commutes with Frobenius the same holds for the extension. This implies the lemma. \square

4. Group-theoretic background

In this section we collect some group-theoretic facts which will be needed in the proof of Theorem 5.11 - assuring that the Frobenius endomorphisms in $\text{Aut}(J(k)) = \text{Aut}(\tilde{J}(k))$ commute.

Lemma 4.1. Let $\ell > n + 1$ be a prime and $G \subset \text{GL}_n(\mathbb{Z}_{\ell})$ a closed subgroup with an abelian ℓ -Sylow subgroup. Assume further that G is generated by its ℓ -Sylow subgroups. Then G is abelian.

Proof. Since $\ell > n + 1$, the group G does not contain elements of finite ℓ -order. Indeed, assume that $\gamma \in \text{GL}_n(\mathbb{Z}_{\ell})$ has order ℓ . Then it generates a subalgebra of the matrix algebra which contains a subfield $\mathbb{Q}_{\ell}(\sqrt[\ell]{1})$, which has dimension $\ell - 1$ over \mathbb{Q}_{ℓ} , and has to embed into the natural representation space \mathbb{Q}_{ℓ}^n . This implies that $\ell \leq n + 1$.

Consider the reduction homomorphism

$$\bar{\psi}_{\ell} : G \rightarrow \text{GL}_n(\mathbb{Z}/\ell).$$

The preimage $G^0 = \bar{\psi}_\ell^{-1}(1)$ of the identity in $\mathrm{GL}_n(\mathbb{Z}/\ell)$ is a normal pro- ℓ subgroup. In particular, G_0 is contained in every ℓ -Sylow subgroup of G . Hence G_0 is abelian and torsion-free, i.e., $G_0 \simeq \mathbb{Z}_\ell^r$, for some $r \in \mathbb{N}$.

Step 1. Since G is generated by its ℓ -Sylow subgroups, which are abelian, and G_0 is contained in all these subgroups, G_0 commutes with all elements of G . Let G'_0 be the ℓ -component of the center of G . It is a torsion-free group isomorphic to \mathbb{Z}_ℓ^r and containing G_0 as a subgroup of finite index.

Thus G is a central extension

$$1 \rightarrow G'_0 \rightarrow G \rightarrow G' \rightarrow 1 \quad (3)$$

where G' is a finite group.

Step 2. By Schur's theorem, since G is a group whose center has finite index, the derived group $[G, G]$ is finite, and G is a split extension of $[G, G]$, a finite group of ℓ -prime order, by a Sylow pro- ℓ subgroup, which is isomorphic to \mathbb{Z}_ℓ^r .

Step 3. Since G has no ℓ -torsion, \tilde{G} has order coprime to ℓ . It follows that \tilde{G} admits a section $\sigma : \mathbb{Z}_\ell^r \rightarrow \tilde{G}$.

Step 4. We claim that \mathbb{Z}_ℓ^r acts trivially on \tilde{G} and that the extension

$$1 \rightarrow \tilde{G} \rightarrow G \xrightarrow{f} \mathbb{Z}_\ell^r \rightarrow 1$$

splits.

Let $g \in \mathrm{GL}_n(\mathbb{Z}_\ell)$ be an element of infinite ℓ -order (i.e., all but finitely many reductions $\bar{\psi}_{\ell^m}(g) \in \mathrm{GL}_n(\mathbb{Z}/\ell^m)$ are of nontrivial ℓ -power order). Consider an element $h \in G \subset \mathrm{GL}_n(\mathbb{Z}_\ell)$ of finite order. Assume that g^ℓ commutes with h . Then g commutes with h . Indeed, in that case, both g and hgh^{-1} are in the same triangular subgroup U as $g^\ell = (hgh^{-1})^\ell$, and in this subgroup U the extraction of ℓ -th roots is unique (log is bijective from U to its Lie algebra).

We have $g = g_s g_u$ where g_s is semi-simple, g_u is unipotent, and g_s, g_u commute. If an element $h \in \mathrm{GL}_n(\mathbb{Z}_\ell)$ has finite order and commutes with g then it commutes with g_s and g_u . Note that $(g^\ell)_u = (g_u)^\ell$ and that they have the same commutators. Thus we can assume $g = g_s$. In this case the algebra $\mathbb{Q}_\ell[g] \subset \mathrm{Mat}_{n \times n}(\mathbb{Q}_\ell)$ is a direct sum of fields $K_i^{(g)}$ (finite extensions of \mathbb{Q}_ℓ).

The subalgebra in $\mathrm{Mat}_{n \times n}(\mathbb{Q}_\ell)$ of elements commuting with h is a direct sum of matrix algebras over division algebras with centers $K_i^{(g)}$. We have a natural embedding of algebras $\mathbb{Q}_\ell[g^\ell] \subseteq \mathbb{Q}_\ell[g]$. If this embedding is an isomorphism then h commutes with g . Otherwise, there is a proper subfield $K_i^{(g^\ell)} \subset K_i^{(g)}$, which does not contain the projection of g to this component of the matrix algebra. The Galois group $\mathrm{Gal}(K_i^{(g)}/K_i^{(g^\ell)})$ is a subgroup of the affine extension of \mathbb{Z}/ℓ by $\mathbb{Z}/(\ell-1) \simeq \mathrm{Gal}(\mathbb{Q}_\ell(\zeta_\ell)/\mathbb{Q}_\ell)$. If $K_i^{(g)}/K_i^{(g^\ell)}$ is not Galois then $[K_i^{(g)} : K_i^{(g^\ell)}] = \ell$, contradicting the assumption $\ell > n+1$. Otherwise, both $K_i^{(g)}, K_i^{(g^\ell)}$ are subfields of $\mathbb{Q}_\ell(\zeta_\ell)$. Note that the ℓ -subgroup of invertible elements in the multiplicative

group of any subfield of $\mathbb{Q}_\ell(\zeta_\ell)$ is a direct summand of the ℓ -group of this field, hence primitive. Since g^ℓ is a primitive element in $K_i^{(g^\ell)}$ it will remain primitive in $\mathbb{Q}_\ell(\zeta_\ell)$, contradicting the assumption that g^ℓ is an ℓ -power of an element in $\mathbb{Q}_\ell(\zeta_\ell)$.

Step 5. Since G is generated by its ℓ -Sylow subgroups and all elements of \tilde{G} commute with \mathbb{Z}_ℓ^r , it follows that $\tilde{G} = 1$ and $G = \mathbb{Z}_\ell^r$. \square

Lemma 4.2. Let $H' \rightarrow H$ be a surjective homomorphism of finite groups. Assume that we have an exact sequence

$$1 \rightarrow S_\ell \rightarrow H \rightarrow C \rightarrow 1$$

where S_ℓ is a nontrivial normal ℓ -subgroup of H , C is a cyclic group whose order is a power of a prime number $\neq \ell$.

Then there is an ℓ -Sylow subgroup $S'_\ell \subset H'$ such that

- S'_ℓ surjects onto S_ℓ ,
- the normalizer N' of S'_ℓ in H' surjects onto H .

In particular, there exists an element $h' \in N'$ of order coprime to ℓ which surjects onto a generator of C .

Proof. All ℓ -Sylow subgroups of H' surject onto S_ℓ . Hence they generate a proper normal subgroup $S' \subset H'$ which surjects onto S_ℓ . Any $h' \in H'$ acts (by conjugation) on the set $\mathcal{S}(H')$ of ℓ -Sylow subgroups of H' .

Since S' acts transitively on $\mathcal{S}(H')$ there exists an element $s' \in S'$ such that $h's'$ acts with a fixed point on $\mathcal{S}(H')$. Let \tilde{S}' be an ℓ -Sylow subgroup preserved by $h's'$. The normalizer N' of \tilde{S}' surjects onto H . In particular, we can find an element \tilde{h}' contained in this normalizer, of order coprime to ℓ , which is mapped to a generator of C . \square

Let H be a finite group and ℓ, p two distinct primes. We say that H contains an (ℓ, p^m) -extension $\{s \in S_\ell, n \in N\}$ if the following holds:

- $S_\ell \subset H$ is an ℓ -Sylow subgroup,
- $N \subset H$ is a subgroup containing S_ℓ as a normal subgroup,
- the quotient $C := N/S_\ell$ is a cyclic group of order p^{m_1} with $m_1 > m$,
- $n \in N$ projects onto a generator of C ,
- $s \in S_\ell$ satisfies $[s, n^{p^m}] \neq 1$ in S_ℓ .

Corollary 4.3. Let $\pi : H' \rightarrow H$ be a surjective homomorphism of finite groups. Assume that H contains an (ℓ, p^m) -extension $\{s \in S_\ell, n \in N\}$. Then H' contains an $(\ell, p^{m'})$ -extension $\{s' \in S'_\ell, n' \in N'\}$. Moreover,

- $m' \geq m$,
- $\pi(S'_\ell) = S_\ell$,
- $\pi(s') = s$,
- $\pi(n') = n$.

Proof. We start with the exact sequence

$$1 \rightarrow S_\ell \rightarrow N \rightarrow C \rightarrow 1. \quad (4)$$

The full preimage of N in H' contains an ℓ -Sylow subgroup S'_ℓ of H' . By Lemma 4.2, the normalizer of S'_ℓ in H' contains an element n' of order coprime to ℓ such that $\pi(n') = n$, surjecting onto a generator of C . We may correct n' such that its order becomes a power of p . It is divisible by the order of C , i.e., it equals $p^{m'}$, with $m' \geq m$. Let $N' \subset H'$ be the subgroup generated by S'_ℓ and n' . Take s' to be any element in the preimage $\pi^{-1}(s)$. Then $\{s' \in S'_\ell, n' \in N'\}$ is the required $(\ell, p^{m'})$ -extension. \square

Let G be a smooth \mathbb{Z} -model of a reductive linear algebraic group defined over \mathbb{Q} . We will use the following generalization of a theorem of Jordan:

Theorem 4.4. *Let k_0 be a field with $q = p^r$ elements. There exists an $n = n(G) \in \mathbb{N}$ such that every subgroup $G \subset \mathbf{G}(k_0)$ with $p \nmid |G|$ contains an abelian normal subgroup $H \subset G$ with $|G/H| \leq n$.*

Further, there exists an $\ell_0 = \ell_0(G)$ such that for all primes ℓ' and all primes $\ell \geq \ell_0$ with $\ell \neq \ell'$, the ℓ -Sylow subgroups of $\mathbf{G}(\mathbb{Z}/\ell')$ and $\mathbf{G}(\mathbb{Z}/\ell)$ are abelian.

Proof. See [BF66], [Wei84]. \square

Proposition 4.5. *Let G be a profinite group. Let S be an infinite set of primes. Let*

$$\psi = \prod_{\ell \in S} \psi_\ell : G \rightarrow \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}_\ell)$$

be a continuous homomorphism. Assume that for all $\gamma \in G$, $\gamma \neq 1$ one has

$$\psi_\ell(\gamma) \neq 1 \in \mathbf{G}(\mathbb{Z}_\ell) \quad (5)$$

for infinitely many $\ell \in S$ (i.e., γ has infinite support). Then

1. *the induced reduction map*

$$\bar{\psi} := \prod_{\ell \in S} \bar{\psi}_\ell : G \rightarrow \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}/\ell)$$

is injective;

2. *there exists an $\ell_0 = \ell_0(G)$ such that for all primes $\ell > \ell_0$ the ℓ -Sylow subgroup of G is abelian;*
3. *there exist a normal closed abelian subgroup $H \subset G$ and an $n = n(G)$ such that G/H has exponent bounded by n , i.e., the order of every element in G/H is bounded by n .*

Proof. Put

$$K_\ell := \text{Ker}(\mathbf{G}(\mathbb{Z}_\ell) \rightarrow \mathbf{G}(\mathbb{Z}/\ell)).$$

We have an exact sequence

$$1 \rightarrow \prod_{\ell \in S} K_\ell \rightarrow \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}_\ell) \rightarrow \prod_{\ell \in S} \mathbf{G}(\mathbb{Z}/\ell) \rightarrow 1$$

Our assumption implies that ψ is injective, and we get an injection of the kernel of the reduction $\text{Ker}(\bar{\psi}) \hookrightarrow \prod_{\ell \in S} K_\ell$. If we had a nontrivial $\gamma \in \text{Ker}(\bar{\psi})$, its image $\psi(\gamma)$ would generate a nontrivial closed procyclic subgroup isomorphic to $\prod_{\ell' \in S'} \mathbb{Z}_{\ell'} \subset \prod_{\ell \in S} K_\ell$, for some infinite set $S' \subset S$. Thus, there would exist a nontrivial element $\gamma_{\ell'} \in \text{Ker}(\bar{\psi})$ such that $\psi_\ell(\gamma_{\ell'}) = 1$ for all $\ell \neq \ell'$, contradicting our assumption. This proves the first claim.

The second claim follows by combining the injectivity of

$$\prod_{\ell' \in S \setminus \ell} \psi_{\ell'} : G \rightarrow \prod_{\ell' \in S \setminus \ell} \mathbf{G}(\mathbb{Z}/\ell')$$

with Theorem 4.4.

From now on, we assume that $\ell > \ell_0$ so that the ℓ -Sylow subgroup of G is abelian.

Lemma 4.6. There exists a constant $\kappa = \kappa(\mathbf{G})$ such that for all $\ell > \ell_0$, there exists a normal abelian subgroup $Z_\ell \subset \bar{\psi}_\ell(G)$ of index

$$[\bar{\psi}_\ell(G) : Z_\ell] \leq \kappa.$$

Proof. If the image $\bar{\psi}_\ell(G) \subset \mathbf{G}(\mathbb{Z}/\ell)$ does not contain elements of order ℓ we can directly apply Theorem 4.4 to conclude that $\bar{\psi}_\ell(G)$ contains a normal abelian subgroup of index $\kappa(\mathbf{G}) = n(\mathbf{G})$.

We may now assume that the image does contain elements of order ℓ . We claim that there do not exist $\gamma, \gamma' \in G$ such that

- $\bar{\psi}_\ell(\gamma), \bar{\psi}_\ell(\gamma')$ have ℓ -power order and
- $\bar{\psi}_\ell(\gamma), \bar{\psi}_\ell(\gamma')$ do not commute in $\mathbf{G}(\mathbb{Z}/\ell)$.

Otherwise, both $\psi_\ell(\gamma)$ and $\psi_\ell(\gamma')$ are contained in some ℓ -Sylow subgroups of $\psi_\ell(G)$, which are both abelian, by the assumption $\ell > \ell_0$. By Lemma 4.1, the subgroup of $\mathbf{G}(\mathbb{Z}_\ell)$ generated by these ℓ -Sylow subgroups is abelian, contradicting the second assumption.

It follows that all elements of ℓ -power order in $\bar{\psi}_\ell(G)$ commute, so that the group \bar{S}_ℓ generated by them is in fact the ℓ -Sylow subgroup of $\bar{\psi}_\ell(G)$. It is abelian and normal. Consider the exact sequence

$$1 \rightarrow \bar{S}_\ell \rightarrow \bar{\psi}_\ell(G) \rightarrow \mathbf{U}_\ell \rightarrow 1 \tag{6}$$

where $\mathbf{U}_\ell := \bar{\psi}_\ell(G)/\bar{S}_\ell$. Since $\ell \nmid |\mathbf{U}_\ell|$ the sequence (6) admits a section and there is an embedding

$$\mathbf{U}_\ell \hookrightarrow \bar{\psi}_\ell(G) \subset \mathbf{G}(\mathbb{Z}/\ell).$$

We apply Theorem 4.4 to conclude that \mathbf{U}_ℓ has an abelian normal subgroup $\mathbf{A}_\ell \subset \mathbf{U}_\ell$ with $|\mathbf{U}_\ell/\mathbf{A}_\ell| \leq n(\mathbf{G})$. We have the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \bar{\mathbf{S}}_\ell & \longrightarrow & \bar{\psi}_\ell(G) & \longrightarrow & \mathbf{U}_\ell & \longrightarrow & 1 \\ & & \parallel & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \bar{\mathbf{S}}_\ell & \longrightarrow & \mathbf{H}_\ell & \longrightarrow & \mathbf{A}_\ell & \longrightarrow & 1 \end{array}$$

where \mathbf{H}_ℓ is the full preimage of \mathbf{A}_ℓ in $\bar{\psi}_\ell(G)$. It is a normal subgroup of $\bar{\psi}_\ell(G)$ with

$$|\bar{\psi}_\ell(G)/\mathbf{H}_\ell| = |\mathbf{U}_\ell/\mathbf{A}_\ell| \leq n(\mathbf{G}).$$

Let $\mathbf{Z}_\ell \subset \mathbf{H}_\ell$ be the centralizer of $\bar{\mathbf{S}}_\ell$, it is a normal abelian subgroup of \mathbf{H}_ℓ . Lemma 4.6 follows if we show that the index $[\mathbf{H}_\ell : \mathbf{Z}_\ell]$ is bounded independently of ℓ .

There is a section

$$\sigma : \mathbf{A}_\ell \rightarrow \bar{\psi}_\ell(G) \subset \mathbf{G}(\mathbb{Z}/\ell).$$

In particular, the finite abelian group \mathbf{A}_ℓ has at most $n := \text{rank}(\mathbf{G})$ generators. Consider the conjugation action of \mathbf{A}_ℓ on $\bar{\mathbf{S}}_\ell$. For $\mathbf{a} \in \mathbf{A}_\ell$ let $\mathbf{C}(\mathbf{a})$ be the cyclic subgroup generated by the image of \mathbf{a} in the group of outer automorphisms of $\bar{\mathbf{S}}_\ell$. It suffices to show that for each of the $\leq n$ generators of \mathbf{A}_ℓ the order $|\mathbf{C}(\mathbf{a})|$ is bounded independently of ℓ and \mathbf{a} .

Let $\mathbf{C}_p(\mathbf{a}) \subset \mathbf{C}(\mathbf{a})$ be the p -Sylow cyclic subgroup, with $p^{m+1} = |\mathbf{C}_p(\mathbf{a})|$. We have an extension of abelian groups

$$1 \rightarrow \bar{\mathbf{S}}_\ell \rightarrow \mathbf{N}_\ell \rightarrow \mathbf{C}_p(\mathbf{a}) \rightarrow 1. \quad (7)$$

We claim that the length of the orbits of $\mathbf{c} \in \mathbf{C}_p(\mathbf{a})$ on $\bar{\mathbf{S}}_\ell$ is universally bounded, provided that $q := p^m$ and ℓ are sufficiently large. More precisely, we have:

Lemma 4.7. There exists a constant $n' = n'(\mathbf{G})$ such that for all $\mathbf{a} \in \mathbf{A}_\ell$, all $\mathbf{s} \in \bar{\mathbf{S}}_\ell$ and all generators \mathbf{c} of $\mathbf{C}_p(\mathbf{a})$ the commutator

$$[\mathbf{s}, \mathbf{c}^q] = 1,$$

provided $\ell, q := p^m \geq n'$.

Proof. We will argue by contradiction. We have

$$G = \varprojlim_i G_i, \quad \text{where } G_i := \left(\prod_{j=1}^i \bar{\psi}_{\ell_j} \right) (G),$$

$\{\ell_1, \ell_2, \dots\}$ is the set of primes, with $\ell_1 = \ell$, and the maps $\pi_i : G_{i+1} \rightarrow G_i$ are the natural projections. Assume that

$$[\mathfrak{s}, \mathfrak{c}^q] = \mathfrak{s}' \neq 1 \text{ in } \bar{S}_\ell. \quad (8)$$

We apply Corollary 4.3 inductively to conclude that each of the groups G_i has an (ℓ, p^{m_i}) -extension

$$\{\mathfrak{s}_i \in S_{\ell,i}, \mathfrak{n}_i \in N_i\}.$$

More precisely, there is a sequence of groups $S_{\ell,i} \subset G_i$ and elements $\mathfrak{s}_i, \mathfrak{n}_i \in G_n$ with the following properties:

- $S_{\ell,i}$ is an ℓ -Sylow subgroup of G_i ,
- $\mathfrak{s}_i \in S_{\ell,i}$
- \mathfrak{n}_i is in the normalizer of $S_{\ell,i}$,
- \mathfrak{n}_i has order $p^{m_{i,1}}$ with $m_{i,1} > m_i \geq m$,
- $[\mathfrak{s}_i, \mathfrak{n}_i^{p^{m_i}}] \neq 1$,
- $\pi_i(S_{\ell,i+1}) = S_{\ell,i}$, $\pi_{i+1}(\mathfrak{s}_{i+1}) = \mathfrak{s}_i$, $\pi_i(\mathfrak{n}_{i+1}) = \mathfrak{n}_i$, for all i .

The corresponding limits

$$\gamma_{\mathfrak{s}} = \varprojlim \mathfrak{s}_i, \quad \gamma_{\mathfrak{c}} = \varprojlim \mathfrak{c}_i \in G$$

have infinite support and don't commute. Thus there exists a prime number $r > \ell, q$ (and $\ell_0(\mathbf{G})$) such that

$$[\bar{\psi}_r(\gamma_{\mathfrak{s}}), \bar{\psi}_r(\gamma_{\mathfrak{c}})] \neq 1.$$

Let i be sufficiently large so that the prime r is among the primes ℓ_1, \dots, ℓ_i . There is a natural projection

$$\bar{\psi}_r : G_i \rightarrow \bar{\psi}_r(G) \subset \mathbf{G}(\mathbb{Z}/r).$$

The ℓ -Sylow subgroup $S_{\ell,i}$ surjects onto the ℓ -Sylow subgroup of $\bar{\psi}_r(G)$, which is abelian by Theorem 4.4. Let

$$\bar{N}_r \subset \bar{\psi}_r(G) \subset \mathbf{G}(\mathbb{Z}/r)$$

be the *nonabelian* group generated by $\bar{\psi}_r(\gamma_{\mathfrak{s}})$ and $\bar{\psi}_r(\gamma_{\mathfrak{n}})$, i.e., by $\bar{\psi}_r(\mathfrak{s}_i)$ and $\bar{\psi}_r(\mathfrak{n}_i)$. It fits into an exact sequence

$$1 \rightarrow \bar{S}_{\ell,r} \rightarrow \bar{N}_r \rightarrow \bar{A}_r \rightarrow 1,$$

where $\bar{S}_{\ell,r}$ is an abelian group of ℓ -power order, \bar{A}_r a cyclic abelian group of order divisible by p^{m+1} , $p \neq \ell$.

Since $r \nmid |\bar{N}_r|$ we can apply Theorem 4.4: Any subgroup of $\mathbf{G}(\mathbb{Z}/r)$ of order coprime to r has a normal abelian subgroup of index bounded by some constant $n(\mathbf{G})$. However, any abelian normal subgroup of \bar{N}_r has index $\geq \min(\ell, q)$. We obtain a contradiction, when ℓ and q are $\geq n(\mathbf{G})$. \square

This finishes the proof of Lemma 4.6. \square

We complete the proof of Proposition 4.5. Indeed, put

$$\bar{H} := \prod_{\ell \in S} Z_\ell \subset \prod_{\ell \in S} G(\mathbb{Z}/\ell).$$

This is an closed abelian normal subgroup of $\psi(G) = \prod_{\ell \in S} \bar{\psi}_\ell(G)$. Since ψ is an injection, the preimage $H := \psi^{-1}(\bar{H})$ is a closed abelian normal subgroup of G . By Lemma 4.6, $[\bar{\psi}_\ell(G) : Z_\ell] \leq \kappa$, for all ℓ , the quotient G/H has exponent bounded by κ . \square

5. Curves and their Jacobians

Let C be a smooth projective curve of genus $g \geq 2$ over a field k and J^n the Jacobian of degree- n zero-cycles, or alternatively, degree- n line bundles on C , with the convention $J = J^0$. We have the diagram

$$\begin{array}{ccc} C^n & \xrightarrow{\sigma_n} & C^{(n)} \\ & & \downarrow \varphi_n \\ & & J^n. \end{array}$$

For any field k_0 we denote by $C^{(n)}(k_0)$ the set of k_0 -points of the variety $C^{(n)}$, i.e., the set of effective cycles $c_1 + \dots + c_n$ defined over k_0 . We write $C(k_0)^{(n)} \subset C^{(n)}(k_0)$ for the subset of cycles $c_1 + \dots + c_n$ where *each* c_i is defined over k_0 . Put

$$W_n^r(C) := \{[L] \in J^n \mid \dim H^0(C, L) \geq r + 1\}, \quad W_n(C) := W_n^0(C).$$

The map φ_n is surjective for $n \geq g$. For $n = g$ there is a divisor $D \subset J$ such that for all $x \in J(k) \setminus D(k)$, the fiber $\varphi_n^{-1}(x)$ consists of one point. For $n \geq 2g - 1$, the map φ_n is a \mathbb{P}^{n-g} -bundle.

We assume that $C(k_0) \neq \emptyset$, fix a point $c_0 \in C(k_0)$ and the embedding

$$\begin{array}{ccc} C & \hookrightarrow & J \\ c & \mapsto & [c - c_0]. \end{array}$$

This allows us to identify J^n and J .

The following lemma will be used in Section 7.

Lemma 5.1. Let k_0 be a finite field of characteristic p . Fix a prime number $\ell \neq p$ and assume that $J(k_0) \supset J[\ell]$. For $\ell = 2$ assume that $J(k_0) \supset J[4]$, respectively. Let k_1/k_0 be a degree- ℓ -extension. Then

- $\frac{1}{\ell}J(k_0) \subset J(k_1)$,
- $J\{\ell\} \cap J(k_1) = \frac{1}{\ell}J(k_0) \cap J\{\ell\}$.

Proof. Let Fr be the k_0 -Frobenius automorphism of $k = \bar{k}_0$, whose action on $J(k)$ coincides with that of the k_0 -Frobenius endomorphism $\text{Fr} \in \text{End}(J)$. By assumption, Fr acts trivially on $J[\ell^\delta]$, hence we have $\text{Fr} - 1 = \ell^\delta f$, for some $f \in \text{End}(J)$, where $\delta = 1$ (resp. 2) for $\ell \neq 2$ (resp. $\ell = 2$). Then, a direct computation (using the binomial expansion) shows that

$$\text{Fr}^\ell - 1 = \ell u(\text{Fr} - 1),$$

for some $u \in 1 + \ell \mathbb{Z}[f] \subset 1 + \ell \text{End}(J)$. Since u acts on $J\{\ell\}$ as an isomorphism, this implies the second assertion. The first assertion follows from the second. \square

Lemma 5.2. For $n \geq 2g - 1$, a finite field k_0 such that $\#k_0$ is sufficiently large, any finite extension k_1/k_0 and any point $x \in J(k_1)$ there exists a point $z \in \mathbb{P}^{n-g}(k_1) = \varphi_n^{-1}(x)$ such that the fiber $\sigma_n^{-1}(z)$ is completely reducible over k_1 .

Proof. Follows from the equidistribution theorem [Kat02], Theorem 9.4.4. \square

Corollary 5.3. *There exists a finite extension k'_0/k_0 such that $C(k_1)$ generates $J(k_1)$, for all finite extensions k_1/k'_0 .*

Proof. The claim follows from the existence of z in Lemma 5.2. \square

It will be useful to be able to bound indices of subgroups in $J(k_1)$ generated by fewer points from $C(k_1)$. Assume that k_1/k_0 is a finite extension with $\#k_1 = q$. Write

$$\#J(k_1) = q^g(1 + \Delta_q) \quad \text{and} \quad \#C(k_1) = q(1 + \delta_q)$$

We know that $\Delta_q, \delta_q = O(\frac{1}{\sqrt{q}})$, the implicit constant depending only on the genus $g(C)$. We may assume that q is such that

$$|\Delta_q|, |\delta_q| \leq 1/2. \tag{9}$$

Lemma 5.4. Let $D \subset C(k_1)$ be a subset of points such that

$$\#D/\#C(k_1) \leq \epsilon_q.$$

Let $H \subset J(k_1)$ be the subgroup generated by points in $C(k_1) \setminus D$. Then

$$I := |J(k_1)/H| \leq \frac{(2g-1)!g2^{2g-1}}{(1-\epsilon_q)^{2g-1}}.$$

Proof. We have

$$\#H = \frac{q^g(1 + \Delta_q)}{I}.$$

Observe that

$$\#(C(k_1) \setminus D)^{(2g-1)} \geq \frac{1}{(2g-1)!} q^{2g-1} (1 + \delta_q)^{2g-1} (1 - \epsilon_q)^{2g-1}.$$

On the other hand, $C^{(2g-1)} \rightarrow J^{2g-1}$ is a projective bundle of relative dimension $g-1$. This implies that

$$\frac{1}{(2g-1)!} q^{2g-1} (1 + \delta_q)^{2g-1} (1 - \epsilon_q)^{2g-1} \leq \frac{q^g (1 + \Delta_q)}{I} \cdot \frac{q^g - 1}{q - 1}.$$

Using the bound (9), we obtain

$$I < \frac{(2g-1)!g}{((1 + \delta_q)(1 - \epsilon_q))^{2g-1}}.$$

□

Recall that the Galois group $\Gamma := \text{Gal}(k/k_0)$ is isomorphic to $\hat{\mathbb{Z}} = \prod_{\ell} \mathbb{Z}_{\ell}$ and is topologically generated by the Frobenius automorphism Fr . For a finite set of primes S let $k_S \subset k$ be the fixed field of $\Gamma_S := \prod_{\ell \notin S} \mathbb{Z}_{\ell}$; the Galois group of the (infinite) extension k_S/k_0 is $\prod_{\ell \in S} \mathbb{Z}_{\ell}$. Note that $J\{S\} \subset J(k_S)$ and that $C(k_S) \subset J(k_S)$ is infinite. We have a natural projection map

$$\lambda_S : C(k) \rightarrow J(k) \rightarrow J\{S\},$$

(depending on the choice of c_0).

Theorem 5.5. *Let S be a finite set of primes. Then*

- *the set $C(k) \cap J\{S\}$ is finite;*
- *the map $\lambda_S : C(k_S) \rightarrow J\{S\}$ is surjective with infinite fibers.*

Proof. The first statement is due to Boxall [Box92]. The second was proved in [BT05]. □

Remark 5.6. Theorem 5.5 admits a generalization: Let $X \subset A$ be a proper subvariety of an abelian variety. If S is a finite set of primes and if the intersection $Y := X(k) \cap \prod_{\ell \in S} A\{\ell\}$ is infinite then

$$Y \subset (\cup_{i \in I} x_i + A_i(k)) \subset X(k) \subset A(k),$$

where I is a finite set, $A_i \subset A$ are abelian subvarieties and $x_i \in A(k)$ [Box92].

Note that for finite fields k_0 with $\#k_0$ sufficiently large, the image of $C(k_0)^{(g)}$ does not coincide with $J(k_0)$. Indeed, the number of \mathbb{F}_q -points in $C(\mathbb{F}_q)^{(g)}$ is approximately equal to

$$\frac{q^g}{g!} < q^g.$$

On the other hand, among infinite extensions of k'/k_0 we can easily find some with $C(k')^{(g)} = J(k')$.

Proposition 5.7. *Let k_0 be a finite field with algebraic closure k , S the set of primes $\leq \mathfrak{g}$ and $\Gamma_S = \prod_{\ell \notin S} \mathbb{Z}_\ell \subset \text{Gal}(k/k_0)$. Put $k' := k^{\Gamma_S}$. Then*

$$C(k')^{(\mathfrak{g})} = J(k').$$

Proof. There exists a subvariety $Y \subset J$ of codimension ≥ 2 such that for all $x \in J(k) \setminus Y(k)$ there is a unique representation $x = \sum_{i=1}^{\mathfrak{g}} c_i$, with $c_i \in C(k)$, modulo permutations.

Assume that $x \in J(k') \setminus Y(k')$ and that its representation as a cycle contains at least one $c_i \notin C(k')$. For any $\gamma \in \Gamma_S$ we have $x = \sum_1^{\mathfrak{g}} \gamma(c_i)$. If $\gamma \neq 1$, then the size of any nontrivial orbit of γ is strictly greater than \mathfrak{g} . Thus there is more than one representation of x as a sum of points in $C(k)$, modulo permutations within the cycle. Contradiction.

Assume that $x \in Y(k')$. Consider the fibration $C^{(\mathfrak{g})} \rightarrow J$. The fiber over x is the projective space \mathbb{P}^r , defined over k' , parametrizing all representations of x as a sum of degree- \mathfrak{g} zero-cycles. There exists $(c_1, \dots, c_{\mathfrak{g}}) \in C^{(\mathfrak{g})}(k')$ with $\sum_{i=1}^{\mathfrak{g}} c_i = x$. We are done if $c_i \in C(k')$, for all i . Otherwise, observing that Γ_S preserves this cycle, we can apply the argument above about the minimal length of Galois orbits in the complement $C(k) \setminus C(k')$. \square

Lemma 5.8. Let $J_\gamma(k) \subset J(k)$ be the subset of elements fixed by $\gamma \in G_C$. If C is not hyperelliptic then

$$j_\gamma : C(k) \setminus C_\gamma(k) \rightarrow J(k)/J_\gamma(k)$$

is an embedding of sets. If C is hyperelliptic let

$$C[4] := \{c \in C(k) \mid c \in J[4] \text{ and } \gamma(c) = -c\}.$$

Then

$$j_\gamma : C(k) \setminus (C_\gamma(k) \cup C[4]) \rightarrow J(k)/J_\gamma(k)$$

is an embedding of sets.

Proof. Assume there exist two points $c, c' \in C(k)$ with $\gamma(c) \neq c$ and $\gamma(c') \neq c'$ and such that $j_\gamma(c) = j_\gamma(c')$. Then $\gamma(c) - \gamma(c') = c - c'$ and hence $\gamma(c) + c' = c + \gamma(c')$. The cycles $\gamma(c) + c', c + \gamma(c')$ consist of different points since $c' \neq c, c' \neq \gamma(c')$, by assumption. Thus $\gamma(c) + c'$ defines a hyperelliptic pencil and we have proved the lemma for nonhyperelliptic curves.

In the hyperelliptic case assume that the pencil consists of elements $c, -c$ (since the pencil is clearly γ -invariant and belongs to J_γ). Thus $c' = -c$ and γ acts as -1 on c . Note that $j_\gamma(c) = -j_\gamma(c)$ implies that $j_\gamma(2c) = 0$ and $2c \in J_\gamma(k)$. Then $2c = -2c$ implies that $4c = 0$. Thus in this case a possible exceptional subset consists of points $c \neq c' = -c$ of order 4 such that $\gamma(c) = -c$. \square

Theorem 5.9. *The group of automorphisms G_C satisfies conditions of Proposition 4.5.*

Proof. Immediate from Proposition 3.5. \square

Corollary 5.10. *For all $\gamma, \tilde{\gamma} \in G_C$ there exists an $n \in \mathbb{N}$ such that γ^n and $\tilde{\gamma}^n$ commute.*

Proof. It suffices to combine Theorem 5.9 and Proposition 4.5. \square

Theorem 5.11. *Let $\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$ be an isomorphism of pairs. Then there exists an $n \in \mathbb{N}$ such that Fr_C^n and $\phi^{-1}(\text{Fr}_{\tilde{C}}^n)$ commute in $\text{Aut}(J(k))$.*

Proof. Immediate from Corollary 5.10. \square

Lemma 5.12. *Assume that Fr and $\tilde{\text{Fr}}$ generate the same ℓ -adic subgroup in $\text{GL}_n(\mathbb{Z}_\ell)$. Then there exist $n, \tilde{n} \in \mathbb{N}$ such that*

$$\text{Fr}^n = \tilde{\text{Fr}}^{\tilde{n}}.$$

Proof. The assumption implies that there exist an $\alpha \in \mathbb{Z}_\ell^*$ and an $\tilde{n} \in \mathbb{N}$ such that

$$\text{Fr}^\alpha = \tilde{\text{Fr}}^{\tilde{n}}.$$

The same equality holds for the determinants. However, the determinants are positive integer powers of p . \square

6. Detecting isogenies

In this section, we recall some facts from divisibility theory for linear recurrences, as developed in [CZ02], and apply these to derive a sufficient condition for isogeny of abelian varieties.

A function $F : \mathbb{N} \rightarrow \mathbb{C}$ is called a *linear recurrence* if there exist an $r \in \mathbb{N}$, and $a_i \in \mathbb{C}$, such that for all $n \in \mathbb{N}$ one has

$$F(n+r) = \sum_{i=0}^{r-1} a_i F(n+i).$$

There is a unique expression

$$F(n) = \sum_{i=1}^m f_i(n) \gamma_i^n,$$

where $f_i \in \mathbb{C}[x]$ are nonzero and $\gamma_i \in \mathbb{C}^*$. The complex numbers $\gamma_i \in \mathbb{C}^*$ are called the roots of the recurrence. Let Γ be a torsion-free finitely-generated subgroup of the multiplicative group \mathbb{C}^* . Then the ring of linear recurrences with roots in Γ is isomorphic to the unique factorization domain $\mathbb{C}[x, \Gamma]$ (see [CZ02, Lemma 2.1]); the element in $\mathbb{C}[x, \Gamma]$ corresponding to a linear recurrence F will be denoted by the same letter.

We say that $\{F(n)\}_{n \in \mathbb{N}}$ is a *simple* linear recurrence, if $\deg(f_i) = 0$, for all i , i.e., f_i are constants.

Proposition 6.1. *Let $\{F(n)\}_{n \in \mathbb{N}}$, $\{\tilde{F}(n)\}_{n \in \mathbb{N}}$ be simple linear recurrences such that $F(n), \tilde{F}(\tilde{n}) \neq 0$ for all $n, \tilde{n} \in \mathbb{N}$. Assume that*

1. *The set of roots of F and \tilde{F} generates a torsion-free subgroup of \mathbb{C}^* .*
2. *There is a finitely-generated subring $\mathfrak{R} \subset \mathbb{C}$ with $F(n)/\tilde{F}(n) \in \mathfrak{R}$, for infinitely many $n \in \mathbb{N}$.*

Then

$$G : \mathbb{N} \rightarrow \mathbb{C} \\ n \mapsto F(n)/\tilde{F}(n)$$

is a simple linear recurrence.

Proof. The fact that G is a linear recurrence is proved in [CZ02, p. 434]. Enlarging Γ , if necessary, we obtain an identity

$$G \cdot \tilde{F} = F,$$

in the ring $\mathbb{C}[x, \Gamma]$. Since F, \tilde{F} are simple, i.e., in $\mathbb{C}[\Gamma]$, G is also simple. \square

Lemma 6.2. Let Γ be a finitely-generated torsion-free abelian group of rank r with a fixed basis $\{\gamma_1, \dots, \gamma_r\}$. Let $\mathbb{C}[\Gamma]$ be the corresponding algebra of Laurent polynomials, i.e., finite linear combinations of monomials $x^\gamma = \prod_{j=1}^r x_j^{g_j}$, where $\gamma = \sum_{i=1}^r g_i \gamma_i \in \Gamma$. Let γ be a primitive element in Γ , i.e., $\gcd(g_1, \dots, g_r) = 1$. Then, for each $\lambda \in \mathbb{C}^*$, the polynomial $x^\gamma - \lambda$ is irreducible in $\mathbb{C}[\Gamma]$, i.e., defines an irreducible hypersurface in the torus $(\mathbb{C}^*)^r$.

Let $\gamma, \gamma' \in \Gamma$ be arbitrary elements. The polynomials $x^\gamma - 1$ and $x^{\gamma'} - 1$ are not coprime in $\mathbb{C}[\Gamma]$, i.e., the corresponding divisors in $(\mathbb{C}^*)^r$ have common irreducible components, if and only if γ, γ' generate a cyclic subgroup of Γ .

Proof. The map defined by the monomial $x^\gamma : (\mathbb{C}^*)^r \rightarrow \mathbb{C}^*$ has irreducible fibers, if and only if γ is primitive. For other γ , put $m := \gcd(g_1, \dots, g_r) > 1$ and $\gamma = m\tilde{\gamma}$. Then $x^\gamma - 1 = \prod_{s=1}^m (x^{\tilde{\gamma}} - \zeta_m^s)$, where ζ_m is a primitive m -th root of 1. By the first observation, the polynomials $x^{\tilde{\gamma}} - \zeta_m^s$ are irreducible. To prove the last statement, note that coprimality of $x^\gamma - 1$ and $x^{\gamma'} - 1$ is equivalent to coprimality of $x^{\tilde{\gamma}} - 1$ and $x^{\tilde{\gamma}'} - 1$, for the corresponding primitivizations $\tilde{\gamma}, \tilde{\gamma}'$ of γ, γ' . This coprimality is equivalent to $\tilde{\gamma} \neq \pm \tilde{\gamma}'$. \square

Let A be an abelian variety of dimension \mathfrak{g} defined over a finite field k_1 of characteristic p , and let $\{\alpha_j\}_{j=1, \dots, 2\mathfrak{g}}$ be the set of eigenvalues of the corresponding Frobenius endomorphism Fr on the ℓ -adic Tate module, for $\ell \neq p$. Let k_n/k_1 be the unique extension of degree n . The sequence

$$F(n) := \#A(k_n) = \prod_{j=1}^{2\mathfrak{g}} (\alpha_j^n - 1). \quad (10)$$

is a simple linear recurrence. Let Γ be the multiplicative subgroup of \mathbb{C}^* generated by $\{\alpha_j\}_{j=1, \dots, 2\mathfrak{g}}$. Choosing k_1 of sufficiently large and divisible degree over \mathbb{F}_p , we may assume that Γ is torsion-free. Choose a basis $\gamma_1, \dots, \gamma_r$ of Γ , and write

$$\alpha_j = \prod_{i=1}^r \gamma_i^{a_{ij}},$$

with $a_{ij} \in \mathbb{Z}$. Recall that all α_j are Weil numbers, i.e., all Galois-conjugates of α_j have absolute value \sqrt{q} , where $q = \#k_1$. It follows that, for $j \neq j'$, either $\alpha_j = \alpha_{j'}$ or $\alpha_j, \alpha_{j'}$ generate a subgroup of rank two in Γ (since Γ does not contain torsion elements). We get a subdivision of the sequence of eigenvalues

$$\{\alpha_j\}_{j=1, \dots, 2g} = \sqcup_{s=1}^t I_s, \quad t \leq 2g,$$

into subsets of equal elements. Put $d_s = \#I_s$ and let $\alpha_s \in I_s$.

Theorem 6.3. *Let A and \tilde{A} be abelian varieties of dimension g over finite fields k_1 , resp. \tilde{k}_1 . Let F , resp. \tilde{F} , be a simple linear recurrence as in equation (10). Assume that $\tilde{F}(n) \mid F(n)$ for infinitely many $n \in \mathbb{N}$. Then A and \tilde{A} are isogenous.*

Proof. Let $\Gamma \in \mathbb{C}^*$ be the (multiplicative) subgroup generated by $\{\alpha_j\} \cup \{\tilde{\alpha}_j\}$. Choosing k_1 , resp. \tilde{k}_1 , of sufficiently large and divisible degree over the corresponding prime fields, we may assume that Γ is torsion-free. Proposition 6.1 implies that F/\tilde{F} is a simple linear recurrence.

The Laurent polynomial corresponding to F , resp. \tilde{F} , has the form

$$\prod_{s=1}^t \left(\prod_{i=1}^r x_i^{a_{is}} - 1 \right)^{d_s}, \quad \text{resp.} \quad \prod_{\tilde{s}=1}^{\tilde{t}} \left(\prod_{i=1}^r x_i^{\tilde{a}_{i\tilde{s}}} - 1 \right)^{d_{\tilde{s}}}.$$

Observe that

$$\gcd\left(\prod_{i=1}^r x_i^{a_{is}} - 1, \prod_{i=1}^r x_i^{a_{is'}} - 1\right) \in \mathbb{C}^*,$$

for $s \neq s'$. The same holds for \tilde{F} . Using Lemma 6.2, we conclude that $t = \tilde{t}$, that we can order the indices so that $\#I_s = \#\tilde{I}_s$, and so that the multiplicative groups generated by $\alpha_s \in I_s$ and $\tilde{\alpha}_s \in \tilde{I}_s$ have rank 1, for each $s = 1, \dots, t$. Thus $\tilde{\alpha}_s = \alpha_s^u$, where $u \in \mathbb{Q}$ depends only on k_1 and \tilde{k}_1 . It follows that some integer powers of $\text{Fr}, \tilde{\text{Fr}}$ have the same sets of eigenvalues, with equal multiplicities. It suffices to apply Theorem 1.1 to conclude that A is isogenous to \tilde{A} . \square

7. Reconstruction

We return to the setup in Section 1: C, \tilde{C} are irreducible smooth projective curves over k of genus ≥ 2 , with Jacobians J , resp. \tilde{J} . We have a diagram

$$\begin{array}{ccccc} J(k) & & J^1(k) & \xleftarrow{j_1} & C(k) \\ \phi^0 \downarrow & & \phi^1 \downarrow & & \phi_s \downarrow \\ \tilde{J}(k) & & \tilde{J}^1(k) & \xleftarrow{\tilde{j}_1} & \tilde{C}(k) \end{array}$$

where

- ϕ^0 is an isomorphism of abstract abelian groups;
- ϕ^1 is an isomorphism of homogeneous spaces, compatible with ϕ^0 ;
- the restriction $\phi_s : C(k) \rightarrow \tilde{C}(k)$ of ϕ^1 is a bijection of sets.

It will be convenient to choose a point $c_0 \in C(k_0)$ and fix the embeddings

$$\begin{array}{ccc} C(k) & \rightarrow & J(k) & & \tilde{C}(k) & \rightarrow & \tilde{J}(k) \\ c & \mapsto & c - c_0 & & \tilde{c} & \mapsto & \tilde{c} - \phi_s(c_0). \end{array}$$

With this choice, the isomorphism of abelian groups ϕ induces a bijection on the sets $C(k)$ and $\tilde{C}(k)$. In this situation we will say that

$$\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$$

is an isomorphism of pairs.

Lemma 7.1. For any choice of $n_1, \dots, n_r \in \mathbb{N}$ and $c_1, \dots, c_r \in C(k)$ one has

$$\dim \mathbf{H}^0(C, \mathcal{O}(\sum_i n_i c_i)) = \dim \mathbf{H}^0(\tilde{C}, \mathcal{O}(\sum_i n_i \phi^0(c_i))).$$

Proof. The effectivity of a divisor on C is intrinsically determined by the group $J(k)$: the images of the maps $C^{(d)} \rightarrow J$, resp. $\tilde{C}^{(d)} \rightarrow \tilde{J}$, are the same (under ϕ^0). We can distinguish $D \in J(k)$ with $\dim \mathbf{H}^0(C, D) \geq 1$, and therefore all sets of linearly equivalent divisors. By induction, we can detect that $\dim \mathbf{H}^0(C, D) \geq n$, with $n > 1$: there are infinitely many points $c \in C(k) \subset J(k)$ such that $\dim \mathbf{H}^0(C, D - c) \geq n - 1$. \square

Corollary 7.2. *If C is hyperelliptic, trigonal or special (i.e., violate the Brill–Noether inequality) then so is \tilde{C} .*

Corollary 7.3. *Let $A \subset C^{(d)} \hookrightarrow J$, for $d < g$, be a proper abelian subvariety of maximal dimension. Then there is a proper abelian subvariety $\tilde{A} \subset \tilde{C}^{(d)} \hookrightarrow \tilde{J}$ such that ϕ^0 induces an isomorphism of abelian groups between $A(k)$ and $\tilde{A}(k)$.*

Proof. Any such abelian subvariety of maximal dimension is characterized by the property that it contains an arbitrarily large abelian subgroup of rank equal to twice its dimension. By [Box92], ϕ^0 induces an isomorphism on such subvarieties. \square

Lemma 7.4. Assume that $g(C) > 2$ and that C is bielliptic. Then \tilde{C} is also bielliptic and the map ϕ^0 commutes with every bielliptic involution on C and \tilde{C} , respectively.

Recall that a bielliptic structure is a map $j_E : C \rightarrow E$ of degree 2, where E is an elliptic curve. All bielliptic structures correspond to embedded elliptic curves $E \subset C^{(2)} \subset J$. Since we assume $g(C) > 2$, there is a finite number of such embeddings and they are preserved under ϕ^0 . Thus if C is bielliptic then so is \tilde{C} , and the groups generated by bielliptic reflections are isomorphic.

Corollary 7.5. *If C is the Klein curve then \tilde{C} is also a Klein curve.*

Proof. Indeed, this is a unique curve of genus 3 which has the action of $\mathrm{PGL}_2(\mathbb{F}_7)$. The action is generated by bielliptic involutions, hence \tilde{C} is isomorphic to C . \square

Remark 7.6. Note that the isomorphism ϕ^0 itself does not have to be algebraic, a profinite power of the Frobenius will have the same properties.

Assume that $\mathrm{char}(k_0) \neq 2$, and that $\#k_0$ is sufficiently large, i.e., for all finite extensions k_1/k_0 the points $C(k_1)$ generate $J(k_1)$, and same for \tilde{C} (see Corollary 5.3).

Lemma 7.7. Assume that C and \tilde{C} are not hyperelliptic. Fix finite fields k_0, \tilde{k}_0 such that $\#k_0, \#\tilde{k}_0$ are sufficiently large and $J(k_0) \subset \tilde{J}(\tilde{k}_0)$. Consider the tower of field extensions: $k_0 \subset k_1 \subset \dots$, where k_i/k_{i-1} is the unique extension of degree 2, and similarly for \tilde{k}_0 . Then, for all $n \in \mathbb{N}$,

$$\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n).$$

Proof. We have an intrinsic inductive characterization of $C(k_n)$ and $J(k_n)$, resp. $\tilde{C}(\tilde{k}_n)$ and $\tilde{J}(\tilde{k}_n)$. Namely, $c \in C(k_n)$, iff there exists a point $c' \in C(k)$ such that $c + c' \in J(k_{n-1})$. Indeed, if $c \in C(k_n) \setminus C(k_{n-1})$ then c' is the conjugate for the Galois automorphism σ of k_n/k_{n-1} . Conversely, if $c + c'$ is a pair as above and $\sigma(c) \neq c'$, then $\sigma(c + c') = c + c' \in J(k)$, which defines a non-trivial hyperelliptic pencil on C , contradicting our assumption. By Corollary 5.3, points $C(k_n)$ generate $J(k_n)$, as an abelian group. By induction, it follows that $\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n)$. \square

By Corollary 7.2, the hyperelliptic property of C implies the same for \tilde{C} . The hyperelliptic case requires a more delicate analysis of point configurations.

Let C be a hyperelliptic curve over a finite field \mathbb{F}_q . The Jacobian J^2 of zero cycles of degree 2 contains a unique effective zero-cycle $z_0 \in J^2(\mathbb{F}_q)$ corresponding to the hyperelliptic pencil on C . We use this cycle to identify $J^2(k) \simeq J(k) = J^0(k)$. Let k_0/\mathbb{F}_q be a finite extension, k_1/k_0 a quadratic extension and σ the nontrivial element of the Galois group $\mathrm{Gal}(k_1/k_0)$. Put

$$C(k_1)^- := \{c \in C(k_1) \mid \sigma(c) + c = z_0 \in J^2(k_0)\}.$$

Lemma 7.8. Let C be a hyperelliptic curve defined over \mathbb{F}_q . Then there exists an $N \in \mathbb{N}$ such that for all finite extensions k_0/\mathbb{F}_q with $q^N \mid \#k_0$, the zero-cycles of even degree with support in $C(k_1) \setminus C(k_1)^-$ generate $J(k_1) \simeq J^2(k_1)$.

Proof. Let $H \subset J(k_1)$ be the subgroup generated by zero-cycles of even degree with support in $C(k_1) \setminus C(k_1)^-$. Put $q := \#k_0$. Note that

$$|\#C(k_1)^- - (q + 1)| \leq 2g\sqrt{q}.$$

Indeed, let $\iota : C \rightarrow \mathbb{P}^1$ be the hyperelliptic projection. Then $\iota(C(k_1)^-) \subseteq \mathbb{P}^1(k_0)$, and the image corresponds to those points on $b \in \mathbb{P}^1(k_0)$ such that the degree-2

cycle $\iota^{-1}(b)$ does not split over k_0 . The claim follows from standard Weil estimates. Lemma 5.4 implies a universal (k_1 independent) bound for the index $I := [J(k_1) : H]$, e.g., $I < m$.

Now we apply the argument of Lemma 5.1. Let k_0 be such that $J(k_0)$ contains all $J(k)[\ell]$, for $\ell < m$ (resp. $J(k)[4]$, when $2 < m$). Then $H = J(k_1)$. Indeed, for $\ell \neq 2$ and $J(k)[\ell] \subset J(k_0)$ the order of $J(k_1)/J(k_0)$ is coprime to ℓ : if an automorphism of order 2 acts trivially on $J(k)[\ell]$ then it also acts trivially on all elements of ℓ -power order in $J(k_1)$. Next, note that the elements of the form $\frac{1}{2}x, x \in J(k_0)$ generate the 2-primary part of $J(k_1)$ but that $\sigma(\frac{1}{2}x) = x + z_0, z_0 \in \tilde{J}^2(k_0)$ and hence $\frac{1}{2}x$ is never in $J(k_1)^-$ (the subgroup generated by $C(k_1)^-$). This completes the argument for $\ell = 2$. \square

Lemma 7.9. Assume that C and \tilde{C} are hyperelliptic. There exist finite fields k_0, \tilde{k}_0 and towers of quadratic field extensions: $k_0 \subset k_1 \subset \dots$, resp. for \tilde{k}_0 , such that for all $n \in \mathbb{N}$

$$\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n).$$

Proof. By Lemma 7.8, the points in $C(k_i) \setminus C(k_i)^-$ generate $J(k_i)$. This subset of points is defined intrinsically in $C(k)$, provided $J(k_{i-1})$ is already known. By induction, as in the proof of Lemma 7.7, we obtain the required tower of degree-2 extensions, with an embedding

$$\phi^0 : J(k_i) \rightarrow \tilde{J}(\tilde{k}_i).$$

\square

Theorem 7.10. Let $\phi : (C, J) \rightarrow (\tilde{C}, \tilde{J})$ be an isomorphism of pairs. Then J and \tilde{J} are isogenous.

Proof. In both hyperelliptic and nonhyperelliptic case we have shown that, for sufficiently large finite ground fields k_0, \tilde{k}_0 , there exist towers $\{k_n\}_{n \in \mathbb{N}}$ and $\{\tilde{k}_n\}_{n \in \mathbb{N}}$ of degree-2 field extensions with the following property:

$$\phi^0(J(k_n)) \subset \tilde{J}(\tilde{k}_n)$$

(see Lemma 7.7 and Lemma 7.9). Now we apply Theorem 6.3 to the Frobenius automorphisms $\text{Fr}, \tilde{\text{Fr}}$. \square

8. Anabelian geometry

In this section we discuss an application of the above results to Grothendieck's Anabelian Program - the reconstruction of function fields from Galois groups.

Let C be an irreducible smooth projective curve over $k = \bar{\mathbb{F}}_p$ of genus $g \geq 2$, J its Jacobian and $K = k(C)$ its function field. Throughout, we assume that $p > 2$. Fix a separable closure \bar{K}/K and let $\mathcal{G} = \mathcal{G}_K = \text{Gal}(\bar{K}/K)$ be the absolute Galois

group. The main idea of anabelian geometry is that \mathcal{G} , or even one of its factors, determines C . Note that \mathcal{G} is the completion of a free group with an infinite number of generators [Har95], [Pop95]. In particular, for any two curves over k the corresponding groups are isomorphic as abstract topological groups. However, we will see that in some instances additional structures allow us to recover the curve from the Galois group.

Let

$$\mathcal{G}^a = \mathcal{G}/[\mathcal{G}, \mathcal{G}]$$

be the abelianization of \mathcal{G} . Let ℓ be a prime number, \mathcal{G}_ℓ the ℓ -completion of \mathcal{G} , and \mathcal{G}_ℓ^a the abelianization of \mathcal{G}_ℓ . Clearly, $\mathcal{G}^a = \prod_\ell \mathcal{G}_\ell^a$. A k -rational point $c \in C(k)$ determines a discrete rank-one valuation $\nu = \nu_c$ of the function field K . We write $\mathcal{I}_\nu \subset \mathcal{G}$ for the corresponding inertia subgroup and \mathcal{I}_ν^a , resp. $\mathcal{I}_{\nu, \ell}^a$, for its image in \mathcal{G}^a , resp. \mathcal{G}_ℓ^a . The group $\mathcal{I}_{\nu, \ell}^a$ is topologically cyclic for $\ell \neq p$. For $\ell \neq p$, let $\mathcal{G}_\ell^{ram} \subset \mathcal{G}_\ell^a$ be the subgroup generated by all $\mathcal{I}_{\nu, \ell}^a$. We have an exact sequence

$$1 \rightarrow \mathcal{G}_\ell^{ram} \rightarrow \mathcal{G}_\ell^a \rightarrow \mathcal{G}_\ell^{un} \rightarrow 1 \quad (11)$$

where the quotient group $\mathcal{G}_\ell^{un} = \hat{\pi}_{1, \ell}^a$ is the ℓ -part of the abelianized étale fundamental group.

Consider $\mathcal{G}_{(p)}^a := \prod_{\ell \neq p} \mathcal{G}_\ell^a$ and let $\mathcal{I}^a = \{\mathcal{I}_\nu^a\}$, resp. $\mathcal{I}_\ell^a = \{\mathcal{I}_{\nu, \ell}^a\}$, be the set of inertia subgroups $\mathcal{I}_\nu^a \subset \mathcal{G}_{(p)}^a$, resp. $\mathcal{I}_{\nu, \ell}^a \subset \mathcal{G}_\ell^a$, corresponding to points in $C(k)$.

Conjecture 8.1. *Let C be a curve of genus $g(C) > 2$ over $k = \bar{\mathbb{F}}_p$. The pair $(\mathcal{G}_{(p)}^a, \mathcal{I}^a)$ determines the function field $k(C)$, modulo isomorphisms.*

Remark 8.2. This fails when $g(C) = 1$. For any two elliptic curves over k the pairs $(\mathcal{G}_{(p)}^a, \mathcal{I}^a)$ are isomorphic. There are two types: supersingular curves with $J\{p\} = 0$ (which are all isogenous) and ordinary curves.

Remark 8.3. In principle, one could include the p -part of \mathcal{G}^a into the conjecture. However, the p -part is of a completely different nature. It corresponds to abelian towers of Artin-Schreier extensions; fixing the inertia subgroups yields much stronger information about $k(C)$.

We have the following partial result:

Theorem 8.4. *Let C, \tilde{C} be curves of genus ≥ 2 over $k = \bar{\mathbb{F}}_p$, with $p > 2$. Assume that there is an isomorphism of pairs*

$$(\mathcal{G}_{(p)}^a, \mathcal{I}^a) \xrightarrow{\sim} (\tilde{\mathcal{G}}_{(p)}^a, \tilde{\mathcal{I}}^a). \quad (12)$$

Assume in addition that either

- $J\{p\} = 0$ or
- $g(C) > 2$.

Then there is an isogeny $J \rightarrow \tilde{J}$.

We are grateful to the referee whose arguments helped to improve the lower bound for g from 4 to 2. The rest of this section is devoted to a proof of this theorem. We will reduce to a version of Theorem 1.2, following closely the description of Galois groups in [BT08], Section 11.

Proposition 8.5. *Let C and \tilde{C} be curves of genus ≥ 2 over $k = \bar{\mathbb{F}}_p$ and let ℓ be a prime $\neq p$. Assume that there exists an isomorphism of pairs:*

$$(\mathcal{G}_\ell^a, \mathcal{I}_\ell^a) \xrightarrow{\sim} (\tilde{\mathcal{G}}_\ell^a, \tilde{\mathcal{I}}_\ell^a),$$

i.e., an isomorphism of abelian groups inducing a bijection of sets. Then exists a diagram

$$\begin{array}{ccc} C(k) & \xrightarrow{\iota_\ell} & J\{\ell\} \\ \phi_s \downarrow & & \downarrow \phi^0 \\ \tilde{C}(k) & \xrightarrow{\tilde{\iota}_\ell} & \tilde{J}\{\ell\} \end{array}$$

where ι_ℓ and $\tilde{\iota}_\ell$ are the standard maps induced from embeddings of C and \tilde{C} into their Jacobians, and ϕ^0 is an isomorphism of abelian groups such that the induced map ϕ_s is a bijection of sets.

Proof. We start with a description of \mathcal{G}_ℓ^a , for $\ell \neq p$, following Sections 9 and 11 of [BT08] (the structure of \mathcal{G}_p^a is more refined). Dualizing the exact sequence

$$0 \rightarrow K^*/k^* \rightarrow \text{Div}(C) \rightarrow \text{Pic}(C) \rightarrow 0$$

we obtain the sequence

$$0 \rightarrow \Delta_\ell \rightarrow \mathcal{M}(C(k), \mathbb{Z}_\ell) \rightarrow \mathcal{G}_\ell^a \rightarrow \text{Ext}^1(J(k), \mathbb{Z}_\ell) \rightarrow 0, \quad (13)$$

with the identifications

- $\Delta_\ell := \text{Hom}(\text{Pic}(C), \mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell$ (since $J(k) = \text{Pic}^0(C)$ is torsion);
- $\mathcal{M}(C(k), \mathbb{Z}_\ell) := \text{Hom}(\text{Div}(C), \mathbb{Z}_\ell)$ is the \mathbb{Z}_ℓ -linear space of maps $C(k) \rightarrow \mathbb{Z}_\ell$ (regarding $\text{Div}(C)$ as the free abelian group generated by $c \in C(k)$);
- $\text{Ext}^1(J(k), \mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell^{2g}$.

The interpretation

$$\mathcal{G}_\ell^a = \text{Hom}(K^*/k^*, \mathbb{Z}_\ell), \quad (14)$$

arising from Kummer theory allows us to identify

$$\mathcal{G}_\ell^a \subset \mathcal{M}(C(k), \mathbb{Q}_\ell)/\text{constant maps} \quad (15)$$

as the subspace of maps $\mu : C(k) \rightarrow \mathbb{Q}_\ell$ (modulo constant maps) such that

$$[\mu, f] \in \mathbb{Z}_\ell \text{ for all } f \in K^*/k^*.$$

Here $[\cdot, \cdot]$ is the pairing:

$$\begin{aligned} \mathcal{M}(C(k), \mathbb{Q}_\ell) \times K^*/k^* &\rightarrow \mathbb{Q}_\ell \\ (\mu, f) &\mapsto [\mu, f] := \sum_c \mu(c) f_c, \end{aligned} \quad (16)$$

where $\text{div}(f) = \sum_c f_c c$. In this language, elements of inertia subgroups $\mathcal{I}_{\nu, \ell}^a \subset \mathcal{G}_\ell^a$ correspond to “delta”-maps (constant outside the point $c = c_\nu$).

Consider the following exact sequences

$$0 \rightarrow K^*/k^* \xrightarrow{\rho_C} \text{Div}^0(C) \xrightarrow{\varphi} J(k) \rightarrow 0, \quad (17)$$

$$0 \rightarrow K^*/k^* \otimes \mathbb{Z}_\ell \xrightarrow{\rho_{C, \ell}} \text{Div}^0(C) \otimes \mathbb{Z}_\ell \xrightarrow{\varphi_\ell} J\{\ell\} \rightarrow 0. \quad (18)$$

Put

$$\mathcal{T}_\ell(C) := \varprojlim \text{Tor}_1(\mathbb{Z}/\ell^n, J\{\ell\}).$$

We have $\mathcal{T}_\ell(C) \simeq \mathbb{Z}_\ell^{2\mathfrak{g}}$, where $\mathfrak{g} = \mathfrak{g}(C)$. Passing to ℓ -adic completions in (17) we obtain an exact sequence of torsion-free groups

$$0 \rightarrow \mathcal{T}_\ell(C) \rightarrow \hat{K}_\ell^* \xrightarrow{\hat{\rho}_C} \widehat{\text{Div}}^0(C)_\ell \rightarrow 0, \quad (19)$$

since $J(k)$ is a ℓ -divisible. We write $\widehat{\text{Div}}^0(C)_\ell$ for the ℓ -adic completion of $\text{Div}^0(C)$. Clearly, $\text{Div}^0(C)_\ell := \text{Div}^0(C) \otimes \mathbb{Z}_\ell \subset \widehat{\text{Div}}^0(C)_\ell$ and we have a diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & K^*/k^* \otimes \mathbb{Z}_\ell & \xrightarrow{\rho_{C, \ell}} & \text{Div}^0(C)_\ell & \xrightarrow{\varphi_\ell} & J\{\ell\} \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & \mathcal{T}_\ell(C) & \rightarrow & \hat{K}_\ell^* & \xrightarrow{\hat{\rho}_{C, \ell}} & \widehat{\text{Div}}^0(C)_\ell \xrightarrow{\hat{\varphi}_\ell} 0. \end{array} \quad (20)$$

Recall that, by Kummer theory, $\hat{K}_\ell^* = \text{Hom}(\mathcal{G}_\ell^a, \mathbb{Z}_\ell)$. Dualizing the exact sequence (11), we obtain the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}(\mathcal{G}_\ell^{un}, \mathbb{Z}_\ell) & \longrightarrow & \text{Hom}(\mathcal{G}_\ell^a, \mathbb{Z}_\ell) & \longrightarrow & \text{Hom}(\mathcal{G}_\ell^{ram}, \mathbb{Z}_\ell) \longrightarrow 0 \\ & & \parallel & & \parallel & & \parallel \\ 0 & \longrightarrow & \mathcal{T}_\ell(C) & \longrightarrow & \hat{K}_\ell^* & \longrightarrow & \widehat{\text{Div}}^0(C)_\ell \longrightarrow 0 \end{array}$$

The group \mathcal{G}_ℓ^{ram} has a distinguished basis consisting of $\delta_{\nu,\ell}$, with $\langle \delta_{\nu,\ell} \rangle = \mathcal{I}_{\nu,\ell}^a$, and subject to the condition

$$\sum_{\nu} \delta_{\nu,\ell} \in \Delta_\ell \subset \mathcal{M}(C(k), \mathbb{Z}_\ell).$$

This basis is unique, modulo simultaneous multiplication of all $\delta_{\nu,\ell}$ by an element in \mathbb{Z}_ℓ^* . Define $\mathcal{FS}(C)_\ell$ as the subgroup of elements in \hat{K}_ℓ^* with a finite support on δ_ν . We have an exact sequence

$$0 \rightarrow \mathcal{T}_\ell(C) \rightarrow \mathcal{FS}(C)_\ell \rightarrow \text{Div}^0(C)_\ell \rightarrow 0$$

and the dual sequence

$$0 \rightarrow \text{Hom}(\text{Div}^0(C)_\ell, \mathbb{Z}_\ell) \rightarrow \text{Hom}(\mathcal{FS}(C)_\ell, \mathbb{Z}_\ell) \rightarrow \text{Hom}(\mathcal{T}_\ell(C), \mathbb{Z}_\ell) \rightarrow 0. \quad (21)$$

The homomorphism

$$\begin{aligned} \mathcal{G}_\ell^a &\rightarrow \text{Hom}(\mathcal{FS}(C)_\ell, \mathbb{Z}_\ell) \\ \gamma &\mapsto (\gamma(f) = f(\gamma)), \end{aligned}$$

for $f \in \mathcal{FS}(C)_\ell \subset \hat{K}_\ell^*$, defines an isomorphism of exact sequences (11) and (21):

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathcal{G}_\ell^{ram} & \xrightarrow{\tau_\ell} & \mathcal{G}_\ell^a & \longrightarrow & \mathcal{G}_\ell^{un} \\ & & \parallel & & \parallel & & \parallel \\ 0 & \longrightarrow & \text{Hom}(\text{Div}^0(C)_\ell, \mathbb{Z}_\ell) & \longrightarrow & \text{Hom}(\mathcal{FS}(C)_\ell, \mathbb{Z}_\ell) & \longrightarrow & \text{Hom}(\mathcal{T}_\ell(C), \mathbb{Z}_\ell) \end{array}$$

Indeed, the restriction

$$\text{Hom}(\text{Div}^0(C)_\ell, \mathbb{Z}_\ell) \rightarrow \mathcal{M}(C(k), \mathbb{Z}_\ell) / \Delta_\ell$$

is an isomorphism (via Riesz duality). The map on quotient groups

$$\mathcal{G}_\ell^{un} \rightarrow \text{Hom}(\mathcal{T}_\ell(C), \mathbb{Z}_\ell)$$

is also an isomorphism (duality for finite-rank \mathbb{Z}_ℓ -modules). Since every element in $\mathcal{FS}(C)_\ell \subset \hat{K}_\ell^*$ defines a nontrivial functional on \mathcal{G}_ℓ^a , the map

$$\mathcal{G}_\ell^a \rightarrow \text{Hom}(\mathcal{FS}(C)_\ell, \mathbb{Z}_\ell)$$

is surjective.

We have a primitive embedding $K^*/k^* \otimes \mathbb{Z}_\ell \hookrightarrow \mathcal{FS}(C)_\ell$, with quotient

$$R := \mathcal{FS}(C)_\ell / (K^*/k^* \otimes \mathbb{Z}_\ell) \simeq \mathbb{Q}_\ell^{2g}.$$

Indeed, note that

$$\mathcal{FS}(C)_\ell / (K^*/k^* \otimes \mathbb{Z}_\ell + \mathcal{T}_\ell(C)) = J\{\ell\} \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}, \quad (22)$$

and that the primitive subgroup $K^*/k^* \otimes \mathbb{Z}_\ell \subset \mathcal{FS}(C)_\ell$ has trivial intersection with $\mathcal{T}_\ell(C)$. The quotient R is a torsion-free \mathbb{Z}_ℓ -module, generated by the image of an extension of $\mathcal{T}_\ell(C)$ by $J\{\ell\}$, with $\text{Hom}(R, \mathbb{Z}_\ell) = 0$ due to the restriction isomorphism. Hence $R \simeq \mathbb{Q}_\ell^{2g}$ and the image of $\mathcal{T}_\ell(C)$ in \mathbb{Q}_ℓ^{2g} coincides with \mathbb{Z}_ℓ^{2g} .

Lemma 8.6. Let $f \in \mathcal{FS}(C)_\ell$ be such that there exists a $\gamma \in \mathcal{G}_\ell^a$ with $\gamma(f) = 1$ (e.g., f is primitive in $K^*/k^* \otimes \mathbb{Z}_\ell$). Then $f \in (K^*/k^* \otimes \mathbb{Z}_\ell + \mathcal{T}_\ell(C))$.

Proof. By (22), $\mathcal{FS}(C)_\ell / (K^*/k^* \otimes \mathbb{Z}_\ell + \mathcal{T}_\ell(C))$ is a torsion group; and there is a minimal $n \in \mathbb{N}$ such that $\ell^n f \in (K^*/k^* \otimes \mathbb{Z}_\ell + \mathcal{T}_\ell(C))$. In particular, $\gamma(\ell^n f)$ is divisible by ℓ^n for all $\gamma \in \mathcal{G}_\ell^a$. Consider the projection

$$\hat{\rho}_{C,\ell} : \mathcal{FS}(C)_\ell \rightarrow \mathcal{FS}(C)_\ell / \mathcal{T}_\ell(C) = \text{Div}^0(C)_\ell$$

from Equation (20). Since

$$\mathcal{G}_\ell^a = \text{Hom}(\mathcal{FS}(C)_\ell, \mathbb{Z}_\ell) = \text{Hom}(K^*/k^*, \mathbb{Z}_\ell),$$

we have

$$\hat{\rho}_{C,\ell}(\ell^n f) = \hat{\rho}_{C,\ell}(\ell^n f') \quad \text{mod } \mathcal{T}_\ell(C),$$

for some $f' \in K^*/k^* \otimes \mathbb{Z}_\ell$. Since all elements in $\mathcal{FS}(C)_\ell / \mathcal{T}_\ell(C) = \text{Div}^0(C)_\ell$ are uniquely divisible we get $f - f' \in \mathcal{T}_\ell(C)$, i.e., $f \in f' + \mathcal{T}_\ell(C)$, as claimed. \square

Hence we obtain a well-defined homomorphism

$$\mathcal{FS}(C)_\ell / \mathcal{T}_\ell(C) \rightarrow J\{\ell\},$$

and a Galois-theoretic characterization of the homomorphism

$$\text{Div}^0(C)_\ell \rightarrow J\{\ell\}.$$

It remains to characterize the image of $C(k)$ in $J\{\ell\}$. Every $\delta_{\nu,\ell}$ defines a nontrivial functional on $\text{Div}^0(C)_\ell$ and thus a functional on $\mathcal{FS}(C)_\ell$. Fix a $\delta_{0,\ell} \in \mathcal{I}_{\nu_0,\ell}^a$ (and thus all other $\delta_{\nu,\ell}$). For $\nu \neq \nu_0$ define

$$c_\nu - c_0 \in \text{Div}^0(C)_\ell$$

by

$$\delta_{\nu,\ell}(c_\nu - c_0) = 1, \quad \delta_{0,\ell}(c_\nu - c_0) = -1 \quad \text{and} \quad \delta_{\nu',\ell} = 0 \quad \text{for all } \nu' \neq \nu, \nu_0.$$

Recall that

$$\mathcal{G}_\ell^a \subset \mathcal{M}(C(k), \mathbb{Q}_\ell) / \text{constant maps}$$

is the subspace of \mathbb{Z}_ℓ -valued functionals. The homomorphism $\mathbb{Q}_\ell \rightarrow \mathbb{Q}_\ell/\mathbb{Z}_\ell$ defines an embedding

$$\mathcal{G}_\ell^a/\mathcal{G}_\ell^{ram} = \mathcal{G}_\ell^{un} = \mathbb{Z}_\ell^{2g} \hookrightarrow \text{Hom}(\text{Div}(C), \mathbb{Q}_\ell/\mathbb{Z}_\ell)/\text{constant maps}.$$

Fixing topological generators $\gamma_1, \dots, \gamma_{2g}$ of \mathcal{G}_ℓ^{un} we get $2g$ maps on $C(k)$ with values in $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, well-defined modulo addition of a constant (corresponding to Δ_ℓ). This gives a well-defined vector $(\gamma_i(c - c_0)) \in (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$, and a map

$$\begin{aligned} C(k) &\rightarrow (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g} \\ c &\mapsto (\gamma_i(c - c_0)), \end{aligned}$$

which is unique, modulo translations. This defines ι_ℓ , modulo affine automorphisms of $J\{\ell\}$. \square

Proposition 8.5 implies that any isomorphism of pairs

$$(\mathcal{G}_{(p)}^a, \mathcal{I}^a) = (\tilde{\mathcal{G}}_{(p)}^a, \tilde{\mathcal{I}}^a)$$

induces a commutative diagram

$$\begin{array}{ccc} C(k) & \xrightarrow{\iota} & J(k)/J\{p\} \\ \downarrow & & \downarrow \\ \tilde{C}(k) & \xrightarrow{\tilde{\iota}} & \tilde{J}(k)/\tilde{J}\{p\} \end{array}$$

with the left vertical arrow a bijection of sets and the right vertical arrow an isomorphism of abelian groups, modulo affine automorphisms of $J(k), \tilde{J}(k)$, respectively. If $J\{p\} = 0$, the map ι is an embedding and we can apply Theorem 1.2 to conclude that the Galois isomorphism implies isogeny.

Assume $g(C) > 2$ and $p > 2$. Fix a point $c_0 \in J(k)$ and consider the diagram

$$\begin{array}{ccc} C^{(2)}(k) & \xrightarrow{\varphi} & J(k) \\ & & \downarrow \pi_p \\ & & J(k)/J\{p\} \end{array}$$

with $\varphi((c_1, c_2)) = c_1 + c_2$. Put

$$W_2 := \varphi(C^{(2)}) \subset J.$$

For $g(C) > 2$, the stabilizer of W_2 is trivial, i.e.,

$$W_b := \{w \in W_2(k) \mid w + b \in W_2(k), \quad b \in J(k) \setminus 0\},$$

is a proper subset of W_2 . For every subgroup $B \simeq \mathbb{Z}/p \subseteq J[p]$ (with $p \neq 2$) we put

$$H_B := \bigcap_{b \in B} W_b.$$

These loci play a role in the proof of Theorem 8.4; the following results describe their geometric properties.

Proposition 8.7. *Assume that $g(C) > 2$ and that for some $B \simeq \mathbb{Z}/p \subseteq J[p]$, the subvariety H_B contains a 1-dimensional component. Then H_B is an elliptic curve, $B \subset H_B(k) \subset J(k)$, and there is a degree-two map $C \rightarrow H_B$ inducing the embedding of $H_B \hookrightarrow J$.*

We subdivide the proof into a sequence of lemmas.

Lemma 8.8. Let $b = x - y$, for some $x, y \in C(k)$. Then

$$(C + y) \subseteq W_b := W_2 \cap (W_2 + b).$$

If $W_b \neq (C + y)$ then one of the following holds:

- (1) C is nonhyperelliptic, with a unique trigonal structure and

$$W_b = (C + y) \cup z, \quad z = z_1 + z_2,$$

- where $z_1 + z_2 + y$ is the unique fiber of the degree-three map $C \rightarrow \mathbb{P}^1$;
- (2) C is hyperelliptic and $W_b = (C + y) \cup (C + x^\sigma)$, where σ is the hyperelliptic involution;
- (3) $g(C) = 3$ and C is nonhyperelliptic, $W_b = (C + y) \cup (\kappa_C - C)$, where κ_C is the canonical class of C ;
- (4) H_B is zero-dimensional.

Proof. First of all, $(C + y) + (x - y) = (C + x) \subset W_2$ and the inclusion holds.

Assume that for some degree-2 cycle $z := z_1 + z_2 \notin (C + y)$ we have $\tilde{z} := \tilde{z}_1 + \tilde{z}_2 = z + x - y \in W_2$. If the degree-3 cycles (z_1, z_2, y) and $(\tilde{z}_1, \tilde{z}_2, x)$ on C are equal then $z_1 = y, \tilde{z}_1 = x$ (modulo relabeling) and $z \in (C + y)$, contradiction. If they are distinct then (z_1, z_2, y) is a g_1^3 -cycle.

If $z + x = \tilde{z} + y$ are nontrivial g_1^3 -cycles and C is nonhyperelliptic then $z + x$ defines a trigonal structure on C , which is unique for $g(C) > 3$. Hence z is the unique cycle with this property and we obtain (1).

If C is hyperelliptic then $W_b \supseteq (C + y) \cup (C + x^\sigma)$. Indeed,

$$C + x^\sigma + x - y = C + h - y = C + y^\sigma \subset W_2,$$

where $h = x + x^\sigma = y + y^\sigma$ is a hyperelliptic pencil.

Assume that $z \notin (C + y) \cup (C + x^\sigma)$ and $z + x = \tilde{z} + y$. Since $z \notin (C + y)$ this is not an identity of cycles on C . Any 3-gonal structure on a hyperelliptic curve C with $g(C) > 2$ is degenerate, i.e., $z + x = h + u$, and hence $z = u + x^\sigma \subset (C + x^\sigma)$, contradiction. This proves (2).

In case (3) the canonical map realizes C as a plane curve of degree 4; any trigonal structure on C is obtained as restriction of a projection $\mathbb{P}^2 \rightarrow \mathbb{P}^1$ from a point $u \in C$. If $z \notin (C + y)$ then $z + y = \tilde{z} + x$ implies $z + y + u = \tilde{z} + x + u + \kappa_C$, for $u \in C$ as above. Hence $z \in \kappa_C - (y + C)$. This proves (3).

To prove the last claim notice that $C \subset J$ is not invariant under any translation in J and that the same holds for all irreducible components of W_b listed in the lemma. Since B is a cyclic group of odd order and W_b consists of at most two components, the same holds for all W_b above. This completes the proof. \square

Lemma 8.9. Assume that $b \neq x - y$, for any $x, y \in C(k)$. Then

- (1) if C is nonhyperelliptic and $g(C) > 3$ then for any $z \neq \tilde{z} \in H_B$ the difference $z - \tilde{z} \neq \tilde{x} - \tilde{y}$, for $\tilde{x}, \tilde{y} \in C(k)$.
- (2) if C is hyperelliptic and $g(C) > 2$ then for any $z \neq \tilde{z} \in H_B - (h + B)$ the difference $z - \tilde{z} \neq \tilde{x} - \tilde{y}$, for $\tilde{x}, \tilde{y} \in C(k)$ (where $(h + B)$ is the B -orbit of the hyperelliptic pencil h , if it is contained in H_B).

Proof. Assume that for some $z \neq \tilde{z} \in H_B$ one has $z - \tilde{z} = \tilde{x} - \tilde{y}$, with $\tilde{x}, \tilde{y} \in C$. Same holds for pairs $(z + b), (\tilde{z} + b) \in H_B$ and $(z - b), (\tilde{z} - b) \in H_B$.

Step 1. We have $z + \tilde{y} = \tilde{z} + \tilde{x}$ and similarly for other pairs $(z + mb) + \tilde{y} = (\tilde{z} + mb) + \tilde{x}$, for $m = 1, \dots, p - 1$.

Step 2. Assume that $z + \tilde{y} = \tilde{z} + \tilde{x}$ identically on C . Then $(z_1, z_2, \tilde{y}) = (\tilde{z}_1, \tilde{z}_2, \tilde{x})$ implies that $z_1 = \tilde{x}, \tilde{z}_1 = \tilde{y}$ and $z = u + \tilde{x}$, for some $u \in C$. If $z + b \in (C + \tilde{x})$, i.e., $z + b = \tilde{u} + \tilde{x}$ for some $\tilde{u} \in C$, then $b = (z + b) - z = \tilde{u} - u$, for $u, \tilde{u} \in C$, contradicting the assumption on b . Thus at least two of the relations

$$z + \tilde{y} = \tilde{z} + x, \quad (z + b) + \tilde{y} = (\tilde{z} + b) + \tilde{x}, \quad (z - b) + \tilde{y} = (\tilde{z} - b) + \tilde{x}$$

are nontrivial. Since the cycles

$$z + \tilde{y}, \quad (z + b) + \tilde{y}, \quad (z - b) + \tilde{y}$$

are not equivalent there are at least two different trigonal structures on C . This implies (1).

Step 3. Assume that C is hyperelliptic. If $z \notin h + B$, $z \neq \tilde{z}$, and $z + y_1 = \tilde{z} + x_1$ is not an identity for cycles on C then $z + y_1 = \tilde{z} + x_1 = h + t$ (as in Lemma 8.8), $z = y_1^\sigma + t$ and $\tilde{z} = x_1^\sigma + t$, hence $y_1^\sigma = x_1^\sigma$ and $z = \tilde{z}$, contradiction.

As in Step 2, the relation $z + y_1 = \tilde{z} + x_1$ is identical only if $z \in C + x_1, \tilde{z}$, and hence the relation $(z + b) + y_1 = (\tilde{z} + b) + x_1$ is nontrivial. By the argument above, applied to $z + b$, we obtain $z + b = \tilde{z} + b$ and hence $z = \tilde{z}$, contradiction.

If similarly $(z + b) = (y_1^\sigma + t_1)$ then $(z + b) - z = b = t_1 - t$, contradicting the assumption on b . If $z + y_1 = h + y_1$ then $z = h$ and if $z + y_1 = h + x_1$ then $\tilde{z} = h$. This implies (2). \square

Lemma 8.10. Assume that H_B is one-dimensional and $z - \tilde{z} \neq x_1 - y_1$ for arbitrary $x_1, y_1 \in C$ and $z \neq \tilde{z}, z, \tilde{z} \in H_B \setminus S$, where $S \subset H_B(k)$ is a finite subset. Then

- (1) H_B contains only one irreducible one-dimensional component H_B^0 ;
- (2) there is a degree-two map $C \rightarrow H_B^0$ defining the embedding $H_B^0 \hookrightarrow W^2$;
- (3) $H_B^0 = H_B$ is an elliptic curve containing b .

Proof. Consider the proper preimage R of H_B in $C \times C$ under the degree-two map $C \times C \rightarrow W_2$. Thus $j' : R \rightarrow H_B$ is a degree-two map of algebraic schemes. Let $\pi_i : R \rightarrow C$, with $i = 1, 2$, be projections induced on R by the natural projections of $C \times C$ to C . By the assumption of the lemma, the preimage of $z = (z_1, z_2) \in H_B$ in R consists of

$$r_1(z) = (z_1, z_2), \quad r_2(z) = (z_2, z_1).$$

By assumption, for all but a finite number of $z \in H_B$ and any $r' \in R, r' \neq r_1(z)$, we have $\pi_1(r') \neq z_1$. The same argument holds for π_2 . Thus both maps $\pi_i : R \rightarrow C$ induce an isomorphism on the unique one-dimensional irreducible component of R . In particular, this component is isomorphic to C and the restriction of j' to C defines a degree-two map $j : C \rightarrow H_B^0$. The map j defines an embedding $H_B^0 \rightarrow H_B \subset W_2$. This proves (1) and (2).

The component H_B^0 is invariant under B since it is the unique irreducible component of H_B . Thus any cycle $z \in H_B^0$ is given as $(z_1, \tau(z_1))$, where τ is the involution on C defining j , i.e., $j : C \rightarrow C/\tau = H_B^0$ and $C/\tau = R$.

The map $j^* : \text{Pic}^0(H_B^0) \rightarrow \text{Pic}^0(C)$ has finite kernel since it is contained in $\text{Pic}^0(H_B^0)[2]$. Write $t_b(h)$ for the image of $h \in H_B^0$ under $b \in B$. Any

$$(h - t_b(h) - h' + t_b(h')), \quad \text{with } h, h' \in H_B^0,$$

is contained in the kernel of j^* since

$$j^*((h - t_b(h) - h' + t_b(h'))) = j^*(h) - (j^*(h) + b) - j^*(h') + j^*(h') + b = 0.$$

Thus $h + h' = t_b(h) + t_b(h')$ on H_B^0 , for any h, h' . In particular, H_B^0 has a family of hyperelliptic involutions. On the other hand, $H_B^0 \subset J$ is not rational, thus it is an elliptic curve. Since $j : C \rightarrow E$ is surjective, for any $z = (z_1, z_2) \in H_B \setminus E$ there is a $\tilde{z} \in E \subset H_B$ with $\tilde{z} = (\tilde{z}_1, \tilde{z}_2)$. This proves $H_B = E$ in case (1) (Lemma 8.9). In case (2), $\tau(h) = h$ and there is a hyperelliptic involution σ' on E such that j commutes with the hyperelliptic involution σ' on C . Hence h coincides with the preimage of a σ' -invariant point on E , $h + B \subset E$ and $H_B = E$ in case (2). \square

Applying Lemma 8.9 we prove Proposition 8.7, for all C , except for quartic curves in \mathbb{P}^2 , i.e., nonhyperelliptic curves of genus 3. We now treat this remaining case.

The canonical embedding realizes C as a plane quartic. Thus for any two-cycle $z = z_1 + z_2$, $z_i \in C(k)$ there is a uniquely defined two-cycle $\tilde{z} = \kappa_C - z$, where κ_C is the canonical class. Applying Lemma 8.8 we will assume that $mb \neq (x - y)$, for any $x, y \in C(k)$ and m -coprime to p , hence

$$b = (x_1 + x_2) - (y_1 + y_2), \quad x_i, y_i \in C(k)$$

(and similarly for mb, m -coprime to p). The cycle $z + b = \tilde{z}$ is equivalent to $z + (x_1 + x_2) = \tilde{z} + (y_1 + y_2)$, i.e.,

$$z + \tilde{z} = (y_1 + y_2) + (\tilde{x}_1 + \tilde{x}_2) = \kappa_C + b \in J(k).$$

Note that $\kappa_C + b \neq \kappa_C - b$, i.e., they define nonequivalent linear series. If H_B is nonzero then $\kappa_C + mb$, with m -coprime to p , $pb = 0$, defines $p - 1$ different g_1^4 -series on C .

Lemma 8.11. If $b \neq x - y$ then $\kappa_C + b$ does not degenerate, i.e., it defines a degree-4 map $\pi_b : C \rightarrow \mathbb{P}^1$.

Proof. The series is degenerate, i.e., defines a degree-three map $\theta_b : C \rightarrow \mathbb{P}^1$ if the lines in \mathbb{P}^2 defined by x_1, x_2 and y_1, y_2 intersect in $t \in C(k)$. In this case

$$x_1 + x_2 + x_3 + t = y_1 + y_2 + y_3 + t = \kappa_C$$

and hence

$$b = (x_1 + x_2) - (y_1 + y_2) = y_3 - x_3$$

contradicting the assumption on b .

Thus we can assume that $\theta_b : C \rightarrow \mathbb{P}^1$ has degree 4. Consider also θ_{-b} and the map

$$(\theta_b, \theta_{-b}) : C \rightarrow \mathbb{P}^1 \times \mathbb{P}^1.$$

Lemma 8.12. Assume that H_B has a one-dimensional component. Then

- (1) the map $(\theta_b, \theta_{-b}) : C \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$ is a degree-two map onto its image;
- (2) the image $E := (\theta_b, \theta_{-b})(C)$ is an elliptic curve;
- (3) the map $\sigma : E \rightarrow W_2$ defined by $\sigma(e) = (\theta_b, \theta_{-b})^{-1}(e) \in W^2$ identifies E with H_B .

Proof. By description, any two-cycle z in H_B is contained in a fiber of θ_b . The same holds for θ_{-b} . Note that $L_b \neq L_{-b}$ since $2b \neq 0$ (by the argument above). Thus any such z is contained in the fiber of (θ_b, θ_{-b}) and the map of C onto its image has degree at least 2. Note that the fibers of θ_b and θ_{-b} have at most a degree-2 cycle in common.

Assume on the contrary that for some $z + \tilde{z} = \kappa_C + b$ and $z_1 + \tilde{z}_1 = \kappa_C - b$ have a degree-3 cycle in the intersection. This means that

$$(z + \tilde{z}) - (z_1 + \tilde{z}_1) = \tilde{x} - \tilde{y} \quad \text{for some } \tilde{x}, \tilde{y} \in C(k).$$

Then

$$(\kappa_C + b) - (\kappa_C - b) = \kappa_C + 2b = (z + \tilde{z}) - (z_1 + \tilde{z}_1) = \tilde{x} - \tilde{y}$$

which contradicts the assumption on b . This proves (1).

Thus the image of C in $\mathbb{P}^1 \times \mathbb{P}^1$ is a curve of degree $(2, 2)$, hence it is either elliptic or rational. Since C is hyperelliptic, $E := (\theta_b, \theta_{-b})(C)$ is elliptic. Note that the fibers of map $(\theta_b, \theta_{-b}) : C \rightarrow E$ coincide with the cycles $z \in H_B$ and hence we obtain (3) \square

Thus Proposition 8.7 holds also for $g(C) = 3$, and we completed its proof. \square

Lemma 8.13. Assume that $J(k_0) \supseteq J[p]$. Let $z \in J(k) \setminus J(k_0)$ be such that $\pi_p(z) \in J(k_0)/(J(k_0) \cap J\{p\})$. Then there exists a subgroup $B \simeq \mathbb{Z}/p \subset J[p]$ such that the Galois orbit of z contains

$$\{z + b \mid b \in B\}.$$

Proof. Let w be the image of z in $W_2 = \varphi(C^{(2)}) \subset J$ and write $w = w_{(p)} + w_p$, where $w_{(p)}$ is of order prime to p and w_p is of p -power order. By assumption, $w_{(p)}$ is k_0 -rational.

Suppose that w is not k_0 -rational. Then w_p is not k_0 -rational. Since $w_p \in J\{p\}$ and $J[p] \subset J(k_0)$, we have $\text{Gal}(k_0(w_p)/k_0) \simeq \mathbb{Z}/p^m\mathbb{Z}$ for some $m \geq 1$. Take $\gamma \in \text{Gal}(k/k_0)$ whose image in $\text{Gal}(k_0(w_p)/k_0)$ is of order p . Then we can write $pu(\gamma - 1) = (\gamma^p - 1)$ on $J\{p\}$ (see proof of Lemma 5.1). Accordingly,

$$p(\gamma - 1)w_p = u^{-1}(\gamma^p - 1)w_p = 0.$$

Since $(\gamma - 1)w_p \neq 0$ by definition, this implies

$$(\gamma - 1)w = (\gamma - 1)w_p \in J[p] \setminus \{0\}.$$

In other words, there exists an $a \in J[p] \setminus \{0\}$, such that $(\gamma - 1)w = a$, or $w = \gamma w - a$. \square

Let k_0 be a sufficiently large finite extension of the ground field containing the field of definition of C and such that $c_0 \in C(k_0)$ and $J[p] \subset J(k_0)$. Let

$$\mathcal{K}(k_0) := \{k'_0/k_0 \mid J(k'_0) \cap J\{p\} = J(k_0) \cap J\{p\}\}$$

be the set of extensions of k_0 such that the p -component of $J(k)$ remains stable. Note that $\mathcal{K}(k_0)$ contains all finite extensions of k_0 of degree coprime to p . Put

$$\text{Mult}(J) := \{a \in \pi_p(W_2(k)) \mid \#\pi_p^{-1}(a) \geq 2\}.$$

and

$$H := \cup_{B \subset J[p], B \simeq \mathbb{Z}/p} H_B, \quad H_B := \cap_{b \in B} (W_2 + b).$$

Note that

$$\text{Mult}(J) = \text{Mult}(\tilde{J}),$$

under the identification of $J(k)/J\{p\} = \tilde{J}(k)/\tilde{J}\{p\}$ above.

Lemma 8.14. For all $k'_0 \in \mathcal{K}(k_0)$ the intersection

$$\text{Mult}(J) \cap J(k'_0) / (J(k'_0) \cap J\{p\})$$

is contained in the union of the following sets

$$\pi_p \left(\bigcup_{a \in J(k_0) \cap J\{p\}} C^{(2)}(k'_0) \cap (C^{(2)}(k'_0) + a) \right),$$

$$\pi_p (H(k) \cap (J(k'_0) + J\{p\})).$$

Proof. Let $z_1, z_2 \in W_2(k'_0)$ with $\pi_p(z_1) = \pi_p(z_2)$. Then $z_1 - z_2 \in J(k'_0) \cap J\{p\} = J(k_0) \cap J\{p\}$ and thus $\pi_p(z_1) = \pi_p(z_2)$ is in the first set. If $z \in W_2(k) \setminus W_2(k'_0)$ projects into $J(k'_0) / (J(k'_0) \cap J\{p\})$, then we apply Lemma 8.13. \square

Thus the intrinsically defined subset $\text{Mult}(J) \subset J(k) / J\{p\}$ (e.g., for $\mathfrak{g}(C) < 4$) may be a union of projections of an infinite number of algebraic curves in J . However, if we consider subfields k'_0 from $\mathcal{K}(k_0)$ then the number of such curves is bounded.

The intersection $\text{Mult}(J) \cap J(k'_0) / J\{p\}$ splits into two sets. The first consists of projections of k'_0 -points of a finite number of curves which are independent of $k'_0 \in \mathcal{K}(k_0)$. The number of such points is bounded by $c \cdot \#k'_0$, where c is independent of $k'_0 \in \mathcal{K}(k_0)$.

The second is contained in the projection of H , a finite union of curves defined by C . In general, it may contain projection of points from H which lie in much bigger fields, and the number of such points could be difficult to bound.

The next lemma shows that when all one-dimensional components of H are elliptic curves then it suffices to count only the projections of $H(k'_0)$, and hence a similar estimate works. By Proposition 8.7, all one-dimensional components of H , for $\mathfrak{g}(C) \geq 3$, are indeed elliptic curves; this yields the desired universal estimate.

Proposition 8.15. *Assume that $\mathfrak{g}(C) > 2$ and that for all finite subgroups $B \simeq \mathbb{Z}/p \subset J[p]$ any one-dimensional component of H_B is an elliptic curve. Then the isomorphism (12) implies an isogeny between J and \tilde{J} .*

Lemma 8.16. *Assume that for all $B \simeq \mathbb{Z}/p \subset J[p]$ all irreducible components of H_B are elliptic curves. Then there exists a constant $c > 0$ such that*

$$\#\pi_p(H_B(k)) \cap (J(k'_0) / J\{p\}) \leq c \#k'_0,$$

for all $k'_0 \in \mathcal{K}(k_0)$.

Proof. We can assume that $E \subset J$ and its translates $E + s, s \in J(k_0)$, are defined over k_0 . Decompose $E(k'_0) = E(k'_0) \cap E\{p\} \oplus E'$. The projection of the translates to $J(k) / J\{p\}$ coincides with the image of $E' + s$ and the intersection of $E(k'_0) + s$ with $E' \oplus J\{p\}$ is contained in $E' \oplus E\{p\}$. Hence the intersection of $\pi_p(E(k'_0))$ with $J(k'_0) / J\{p\}$ is equal to $\pi_p(E(k'_0))$, and thus bounded by $c \cdot q$, with $q = \#k'_0$. \square

We now apply the following inductive algorithm to subgroups $B_0 \subset J(k)/J\{p\}$, for $p > 2$.

$$B_{n+1} := \langle \frac{1}{2}B_n, c \rangle, \quad \exists c' \in \pi_p(C(k)) \text{ with } c + c' \in B_n, c + c' \notin \text{Mult}(J),$$

The union $\cup_n B_n \subset J(k)/J\{p\}$ is an infinite group containing the image of $J\{2\}$. If $B_0 \subseteq \tilde{B}_0$ then $B_n \subseteq \tilde{B}_n$ for all n .

Lemma 8.17. Assume that k_0 is sufficiently large such that:

- (1) $J[\ell] \subset J(k_0)$ for all primes $\ell \leq I$, for I from Lemma 5.4;
- (2) $J(k_0) \cap J\{p\}$ is relatively small.

Put $B_0 := J(k_0)/J\{p\}$. Then $B_n = (J(k_n)/J\{p\})$, for all $n \in \mathbb{N}$, where k_n is the unique extension of k_0 of degree 2^n .

The same holds for sufficiently large \tilde{k}'_0 such that in addition to the above conditions, $\tilde{J}(\tilde{k}'_0)/\tilde{J}\{p\}$ contains the image of $J(k'_0)/J\{p\}$.

Since the definition of B_{n+1} is the same for C and \tilde{C} we obtain that $J(k'_n)/J\{p\} \subset \tilde{J}(\tilde{k}'_n)/\tilde{J}\{p\}$, for all $n \in \mathbb{N}$. Thus the orders of $J(k'_n)$ divide the orders of $\tilde{J}(\tilde{k}'_n)$, for all $n \in \mathbb{N}$, modulo a constant term equal to $\#J(k'_0) \cap J\{p\} \leq q^g$. Applying [CZ02] and Theorem 7.10 we conclude that J and \tilde{J} are isogenous. This finishes the proof of Theorem 8.4.

Remark 8.18. Our analysis of the map $C \rightarrow J(k)/J\{p\}$ works similarly for a map into any quotient $J(k)/J\{m\}$, where m is an arbitrary odd number.

Remark 8.19. Let C be a curve of genus > 3 with a bielliptic structure $j : C \rightarrow E$, i.e., a degree-two map onto an elliptic curve. Then $E \subset W_2$ coincides with a component of H_B , for subgroup $B \simeq Z/p \subset E(k)$. By Corollary 7.3, if $(C, J) \rightarrow (\tilde{C}, \tilde{J})$ is an isomorphism of pairs and j a bielliptic structure then there is a commutative diagram

$$\begin{array}{ccc} (C, J) & \longrightarrow & (\tilde{C}, \tilde{J}) \\ \downarrow & & \downarrow \\ E & \longrightarrow & \tilde{E} \end{array}$$

Thus the groups of algebraic automorphisms generated by bielliptic reflections are isomorphic. Same holds for an isomorphism

$$(C, J(k)/J\{p\}) \rightarrow (\tilde{C}, \tilde{J}/J\{p\})$$

from Equation (12).

In particular, the Klein quartic curve C (the unique curve of genus 3 with bielliptic involutions generating $\text{PSL}_2(\mathbb{F}_7)$, the maximal group of automorphisms) is defined by the image of $C(k) \rightarrow J(k)/J\{p\}$ or $(\mathcal{G}_{(p)}^a, \mathcal{I})$ (for $p > 2$). In order to adjust the argument in Corollary 7.3 for the map $C(k) \rightarrow J(k)/J\{p\}$ we have

to notice only that the presence of an elliptic curve $E \subset W_2$ is detected by the infinity of the intersection of W_2 with $J\{S\}$, for any finite set of primes S (see [Box92]). Thus $W_2 \subset J$ contains an elliptic curve if and only if $\pi_p(W_2) \cap \pi_p(\bigoplus_{\ell_i \in S'} J(k)/J\{\ell_i\})$ is infinite for a finite set S' of primes $\ell_i \neq p$. Then W_2 has an infinite intersection with $\bigoplus_{\ell_i \in S'} J(k)/J\{\ell_i\} \oplus J\{p\}$.

Similar results hold for other special curves C with sufficiently many maps onto curves of small genus.

References

- [Abr94] D. ABRAMOVICH – “Subvarieties of semiabelian varieties”, *Compositio Math.* **90** (1994), no. 1, p. 37–52.
- [BF66] R. BRAUER and W. FEIT – “An analogue of Jordan’s theorem in characteristic p ”, *Ann. of Math. (2)* **84** (1966), p. 119–131.
- [Box92] J. BOXALL – “Autour d’un problème de Coleman”, *C. R. Acad. Sci. Paris Sér. I Math.* **315** (1992), no. 10, p. 1063–1066.
- [BT05] F. BOGOMOLOV and Y. TSCHINKEL – “Curves in abelian varieties over finite fields”, *Int. Math. Res. Not.* (2005), no. 4, p. 233–238.
- [BT08] —, “Reconstruction of function fields”, *Geom. Funct. Anal.* **18** (2008), no. 2, p. 400–462.
- [CZ02] P. CORVAJA and U. ZANNIER – “Finiteness of integral values for the ratio of two linear recurrences”, *Invent. Math.* **149** (2002), no. 2, p. 431–451.
- [Har95] D. HARBATER – “Fundamental groups and embedding problems in characteristic p ”, Recent developments in the inverse Galois problem (Seattle, WA, 1993), *Contemp. Math.*, vol. 186, Amer. Math. Soc., Providence, RI, 1995, p. 353–369.
- [How96] E. W. HOWE – “Constructing distinct curves with isomorphic Jacobians”, *J. Number Theory* **56** (1996), no. 2, p. 381–390.
- [Hru96] E. HRUSHOVSKI – “The Mordell-Lang conjecture for function fields”, *J. Amer. Math. Soc.* **9** (1996), no. 3, p. 667–690.
- [IKO86] T. IBUKIYAMA, T. KATSURA and F. OORT – “Supersingular curves of genus two and class numbers”, *Compositio Math.* **57** (1986), no. 2, p. 127–152.
- [Kat02] N. M. KATZ – *Twisted L-functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2002.
- [Pop95] F. POP – “Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar’s conjecture”, *Invent. Math.* **120** (1995), no. 3, p. 555–578.
- [PR04] R. PINK and D. ROESSLER – “On ψ -invariant subvarieties of semiabelian varieties and the Manin-Mumford conjecture”, *J. Algebraic Geom.* **13** (2004), no. 4, p. 771–798.
- [PS03] F. POP and M. SAÏDI – “On the specialization homomorphism of fundamental groups of curves in positive characteristic”, Galois groups and fundamental groups, *Math. Sci. Res. Inst. Publ.*, vol. 41, Cambridge Univ. Press, Cambridge, 2003, p. 107–118.
- [Ray02] M. RAYNAUD – “Sur le groupe fondamental d’une courbe complète en caractéristique $p > 0$ ”, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), *Proc. Sympos. Pure Math.*, vol. 70, Amer. Math. Soc., Providence, RI, 2002, p. 335–351.
- [Tam04] A. TAMAGAWA – “Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups”, *J. Algebraic Geom.* **13** (2004), no. 4, p. 675–724.
- [Tat66] J. TATE – “Endomorphisms of abelian varieties over finite fields”, *Invent. Math.* **2** (1966), p. 134–144.
- [Wei84] B. WEISFEILER – “Post-classification version of Jordan’s theorem on finite linear groups”, *Proc. Nat. Acad. Sci. U.S.A.* **81** (1984), no. 16, Phys. Sci., p. 5278–5279.
- [Zar08] Y. ZARHIN – “Homomorphisms of abelian varieties over finite fields”, Higher-dimensional geometry over finite fields, IOS Press, Amsterdam, 2008, p. 315–343.